Transfer of Funds Regulation
Draft Compromises - V4 - 25 March 2022

COMPROMISE A - Article 1 and Article 2

covers AMs 79-80, 335-341

Article 1

Subject matter

This Regulation lays down rules on the information on payers and payees, accompanying transfers of funds, in any currency, and the information on originators and beneficiaries, accompanying transfers of crypto-assets, for the purposes of preventing, detecting and investigating money laundering and terrorist financing***, and facilitating ~~ensuring~~ compliance with restrictive measures*** **[AM141]**, where at least one of the payment or crypto-asset service providers involved in the transfer of funds or crypto-assets is established in the Union.

Article 2

Scope

1. This Regulation shall apply to transfers of funds, in any currency, or crypto-assets, which are sent or received by a payment service provider , a ~~crypto-asset service provider~~ provider of crypto-asset transfers, or an intermediary payment service provider established in the Union.

2. This Regulation shall not apply to the services listed in ~~points (a) to (m) and (o) of~~ Article 3, ***points (a) to (m) and (o)*** of Directive (EU) 2015/2366.

2a (new) This Regulation shall also apply to transfers of crypto-assets executed by means of kiosks connected to a distributed ledger network known as crypto-asset automated teller machines ("crypto-ATMs"). **[AM23, AM146]**

3. This Regulation shall not apply to transfers of funds ***or transfers involving crypto-assets*** **[AM24]** carried out ***by actors regulated under Directive 2015/2366*** **[AM149]** using a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, where the following conditions are met:

(a) that card, instrument or device is used exclusively to pay for goods or services; and

(b) the number of that card, instrument or device accompanies all transfers flowing from the transaction.

However, this Regulation shall apply when a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, is used in order to effect a person-to-person transfer of funds or crypto-assets.

4. This Regulation shall not apply to persons that have no activity other than to convert paper documents into electronic data and that do so pursuant to a contract with a payment service provider, or to persons that have no activity other than to provide payment service providers with messaging or other support systems for transmitting funds or with clearing and settlement systems.

This Regulation shall not apply to providers of ancillary infrastructure allowing another entity to provide services for the transfer of crypto-assets. **[AM157]**

This Regulation shall not apply to transfers of funds ~~and crypto-assets~~ **[AM25],** if any of the following conditions is fulfilled:

(a) they involve the payer withdrawing cash from the payer's own payment account;

(b) they constitute transfers of funds ~~or crypto-assets~~ **[AM26, AM152]** to a public authority as payment for taxes, fines or other levies within a Member State;

(c) both the payer and the payee are payment service providers ~~or both the originator and the beneficiary are crypto-asset service providers~~ **[AM27],** acting on their own behalf;

(d) they are carried out through cheque images exchanges, including truncated cheques.

This Regulation shall not apply to transfers of crypto-assets if any of the following conditions is fulfilled:

(a) both the originator and the beneficiary are ~~crypto-asset service provider~~ provider of crypto-asset transfers acting on their own behalf;

(b) the transfers constitute person-to-person transfers of crypto-assets as defined in Article 3(14) [AM154, 155] carried out without the involvement of a ~~crypto-asset service provider~~provider of crypto-asset transfers or obliged entity. **[AM28].**

Electronic money tokens, as defined in Article 3(1), point 4 of Regulation [*please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final*] shall be treated as crypto-assets under this Regulation.

~~This Regulation shall not apply to person-to-person transfer of crypto-assets.~~ **[AM28].**

---

5. A Member State may decide not to apply this Regulation to transfers of funds ~~or transfers of crypto-assets~~ within its territory to a payee's payment account ~~or a beneficiary's account~~ permitting payment exclusively for the provision of goods or services where all of the following conditions are met:

(a) the payment service provider ~~or the crypto-asset service provider~~ of the payee ~~or the beneficiary~~ is subject to ***Directive (EU) 2015/849*** ~~Directive (EU) 2015/849 [*please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*];~~

(b) the payment service provider of the payee ~~or the crypto-asset service provider of the beneficiary~~ is able to trace back, through the payee, by means of a unique transaction identifier, the transfer of funds ~~or, for transfers of crypto-assets,~~

~~through the beneficiary, by means allowing to identify individually the transfers of crypto-assets on the distributed ledger,~~ from the person who has an agreement with the payee ~~or the beneficiary~~ for the provision of goods or services;

(c) the amount of the transfer of funds ~~or crypto-assets~~ does not exceed EUR 1000

[AM 158, 159, 160, 161, 162, 163, 164, 165, 166, 169, 170].

COMPROMISE B - Article 3

covers AMs 30-34; 172, 182

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'terrorist financing' means terrorist financing as defined in Article ***1(5) of Directive (EU) 2015/849*** **[AM172];** ~~2(2)1(5) of Directive (EU) 2015/849 [*please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*];~~

(2) 'money laundering' means the money laundering activities referred to in Article ***1(3) and (4) of*** ~~2(1)1(3) and (4) of Directive (EU) 2015/849~~ [~~*please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*~~]; **[AM173]**

(3) 'payer' means a person that holds a payment account and allows a transfer of funds from that payment account, or, where there is no payment account, that gives a transfer of funds order;

(4) 'payee' means a person that is the intended recipient of the transfer of funds;

(5) 'payment service provider' means the categories of payment service provider referred to in Article 1(1) of Directive (EU) 2015/2366~~2007/64/EC~~, natural or legal persons benefiting from a waiver pursuant to Article 32~~26~~ thereof and legal persons benefiting from a waiver pursuant to Article 9 of Directive 2009/110/EC of the European Parliament and of the Council[1], providing transfer of funds services;

(6) 'intermediary payment service provider' means a payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a transfer of funds on behalf of the payment service provider of the payer or of the payee or of another intermediary payment service provider;

[1] 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).

(7) ‘payment account’ means a payment account as defined in Article 4, point (12), of Directive (EU) 2015/2366;

(8) ‘funds’ means funds as defined in Article 4, point (25), of Directive (EU) 2015/2366;

(9) ‘transfer of funds’ means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including:

(a) a credit transfer as defined in Article 2, point (1), of Regulation (EU) No 260/2012;

(b) a direct debit as defined in Article 2, point (2), of Regulation (EU) No 260/2012;

(c) a money remittance as defined in Article 4, point (22), of Directive (EU) 2015/2366, whether national or cross border;

(d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics;

---

(10) ‘transfer of crypto-assets’ means any ***transfer of crypto-assets from one wallet address or crypto-asset account to another wallet address or crypto-asset account,*** carried out ***or received on behalf of a natural or legal person by at least*** ~~***one***~~ ***a*** ~~crypto-asset service provider~~provider of crypto-asset transfers ***or other obliged entity, acting on behalf of either the originator or the*** beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator and that of the beneficiary are one and the same. **[AM30, AM174, 176],**

---

(11) ‘batch file transfer’ means a bundle of several individual transfers of funds or crypto-assets put together for transmission;

(12) ‘unique transaction identifier’ means a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, ***or determined by a*** ~~***crypto-asset service provider***~~***provider of crypto-asset transfers,*** which permits the traceability of the transaction back to the payer and the payee ***or the traceability of transfer of crypto-assets back to the originator and the beneficiary***; [AM31

(13) ‘person-to-person transfer of funds’ means a transaction between natural persons acting, as consumers, for purposes other than trade, business or profession;

---

(14) ‘person-to-person transfer of crypto-assets’ means a transaction between natural persons acting, as consumers, for purposes other than trade, business or

profession, without the use or involvement of a ~~crypto-asset service provider~~provider of crypto-asset transfers or other obliged entity;

(15) 'crypto-asset'means ***a digital representation of a value or a right that uses cryptography for security and is in the form of a coin or a token or any other digital medium, which may be transferred and stored electronically, using distributed ledger technology or similar technology***~~.a crypto-asset as defined in Article 3(1), point 2 of Regulation [*please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 – COM/2020/593 final*]~~ except when falling under the categories listed in Article 2(2) of that Regulation or otherwise qualifying as funds. **[AM179]**

(16) '~~crypto-asset service provider~~provider of crypto-asset transfers ***of crypto-asset transfers***'means ***any natural or legal person whose occupation or business includes is the provision of services relating to the transfer of crypto-assets on behalf of another natural or legal person*** ~~– a crypto-asset service provider as defined in Article 3(1), point (8) of [*please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 – COM/2020/593 final*] where performing one or more crypto-asset services as defined in Article 3(1) point (9) of [*please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 – COM/2020/593 final*];~~**. [AM180]**

(16 a)'intermediary ~~crypto-asset service provider~~provider of crypto-asset transfers' means a ~~crypto-asset service provider~~provider of crypto-asset transfers or other obliged entity that is not the ~~crypto-asset service provider~~provider of the originator or of the beneficiary and that receives and transmits a transfer of crypto-assets on behalf of the ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator or of the beneficiary or of another intermediary ~~crypto-asset service provider~~provider of crypto-asset transfers; **[AM181]**

(17) 'wallet address' means ~~an account number which custody is ensured by a crypto-asset service provider or a~~ an alphanumeric code ***that identifies an address that holds crypto-assets on a distributed ledger or on similar technology*** ~~for a wallet on a blockchain~~; **[AM32]**

(18) '***crypto-asset*** account number' means ~~the number of~~ an account ***held with or managed by*** ~~to hold crypto-assets which custody is ensured~~ by a ~~crypto-asset service provider~~provider of crypto-asset transfers ***for crypto-assets and which is used for the execution of transfers of crypto-assets***; **[AM34]**

(18 a)'unhosted wallet' means a crypto-asset wallet address that is not held or managed by a ~~crypto-asset service provider~~provider of crypto-asset transfers; **[AM32, AM182]**

(19) 'originator' means a person that holds an account with a ~~crypto-asset service provider~~provider of crypto-asset transfers and allows a transfer of crypto-assets from that account, or, where there is no account, that gives a transfer of crypto-assets order;

(20) 'beneficiary' means a person that is the intended recipient of the transfer of crypto-assets;

(21) 'legal entity identifier' (LEI) means a unique alphanumeric reference code based on the ISO 17442 standard assigned to a legal entity.

COMPROMISE C - Articles 4-13

covers AMs 35-41; 183-213

CHAPTER II

OBLIGATIONS ON PAYMENT SERVICE PROVIDERS

SECTION 1

OBLIGATIONS ON THE PAYMENT SERVICE PROVIDER OF THE PAYER

Article 4

Information accompanying transfers of funds

1. The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payer:

(a) the name of the payer;

(b) the payer's payment account number;

(c) the payer's address, ***country,*** official personal document number, customer identification number or date and place of birth; **[AM183]**

(d) subject to the existence of the necessary field in the relevant payments message format, and where provided by the payer to the payer's Payment service provider, the current Legal Entity Identifier of the payer ***or, in its absence, any official equivalent identifier available***. **[AM184]**

---

2. The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payee:

(a) the name of the payee;

(b) the payee's payment account number;

(c) subject to the existence of the necessary field in the relevant payments message format, and where provided by the payer to the payer's Payment service provider, the current Legal Entity Identifier of the payee ***or, in its absence, any official equivalent identifier available***. **[AM185]**

3. By way of derogation from point (b) of paragraph 1 and point (b) of paragraph 2, in the case of a transfer not made from or to a payment account, the payment service provider of

the payer shall ensure that the transfer of funds is accompanied by a unique transaction identifier rather than the payment account number(s).

4. Before transferring funds, the payment service provider of the payer shall verify the accuracy of the information referred to in paragraph 1 and, where applicable, in paragraph 3, on the basis of documents, data or information obtained from a reliable and independent source.

5. Verification as referred to in paragraph 4 shall be deemed to have taken place where:

(a) a payer's identity has been verified in accordance with ***Article 13 of Directive (EU) 2015/849*** ~~*Artiele* 13 of Directive (EU) 2015/849~~ Articles 16, 37 and 18(3) of *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]* and the information obtained pursuant to that verification has been stored in accordance with Article ~~5640~~ ***40 of*** of that ***Directive*** ~~RegulationDirective~~; or **[AM35, AM186]**

(b) Article ***14(5) of Directive (EU) 2015/849*** ~~21(2) and (3)14(5) of Directive (EU) 2015/849 [*please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*]~~ applies to the payer. **[AM36, AM187]**

6. Without prejudice to the derogations provided for in Articles 5 and 6, the payment service provider of the payer shall not execute any transfer of funds before ensuring full compliance with this Article.

Article 5

Transfers of funds within the Union

1. By way of derogation from Article 4(1) and (2), where all payment service providers involved in the payment chain are established in the Union, transfers of funds shall be accompanied by at least the payment account number of both the payer and the payee or, where Article 4(3) applies, the unique transaction identifier, without prejudice to the information requirements laid down in Regulation (EU) No 260/2012, where applicable.

2. Notwithstanding paragraph 1, the payment service provider of the payer shall, within three working days of receiving a request for information from the payment service provider of the payee or from the intermediary payment service provider, make available the following:

(a) for transfers of funds exceeding EUR 1000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, the information on the payer or the payee in accordance with Article 4;

(b) for transfers of funds not exceeding EUR 1000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1000, at least:

(i) the names of the payer and of the payee; and

(ii) the payment account numbers of the payer and of the payee or, where Article 4(3) applies, the unique transaction identifier.

3. By way of derogation from Article 4(4), in the case of transfers of funds referred to in paragraph 2, point (b), of this Article, the payment service provider of the payer need not verify the information on the payer unless the payment service provider of the payer:

(a) has received the funds to be transferred in cash or in anonymous electronic money; or

(b) has reasonable grounds for suspecting money laundering or terrorist financing.

Article 6

Transfers of funds to outside the Union

1. In the case of a batch file transfer from a single payer where the payment service providers of the payees are established outside the Union, Article 4(1) shall not apply to the individual transfers bundled together therein, provided that the batch file contains the information referred to in Article 4(1), (2) and (3), that that information has been verified in accordance with Article 4(4) and (5), and that the individual transfers carry the payment account number of the payer or, where Article 4(3) applies, the unique transaction identifier.

2. By way of derogation from Article 4(1), and, where applicable, without prejudice to the information required in accordance with Regulation (EU) No 260/2012, where the payment service provider of the payee is established outside the Union, transfers of funds not exceeding EUR 1000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1000, shall be accompanied by at least:

(a) the names of the payer and of the payee; and

(b) the payment account numbers of the payer and of the payee or, where Article 4(3) applies, the unique transaction identifier.

By way of derogation from Article 4(4), the payment service provider of the payer need not verify the information on the payer referred to in this paragraph unless the payment service provider of the payer:

(a) has received the funds to be transferred in cash or in anonymous electronic money; or

(b) has reasonable grounds for suspecting money laundering or terrorist financing.

SECTION 2

OBLIGATIONS ON THE PAYMENT SERVICE PROVIDER OF THE PAYEE

Article 7

Detection of missing information on the payer or the payee

1. The payment service provider of the payee shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.

2. The payment service provider of the payee shall implement effective procedures, including, where appropriate, monitoring after or during the transfers, in order to detect whether the following information on the payer or the payee is missing:

(a) for transfers of funds where the payment service provider of the payer is established in the Union, the information referred to in Article 5;

(b) for transfers of funds where the payment service provider of the payer is established outside the Union, the information referred to in Article 4(1), points (a), (b) and (c), and Article 4(2), points (a) and (b);

(c) for batch file transfers where the payment service provider of the payer is established outside the Union, the information referred to in Article 4(1), points (a), (b) and (c), and Article 4(2), points (a) and (b), in respect of that batch file transfer.

3. In the case of transfers of funds exceeding EUR 1000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, before crediting the payee's payment account or making the funds available to the payee, the payment service provider of the payee shall verify the accuracy of the information on the payee referred to in paragraph 2 of this Article on the basis of documents, data or information obtained from a reliable and independent source, without prejudice to the requirements laid down in Articles 83 and 84 of Directive (EU) 2015/2366.

4. In the case of transfers of funds not exceeding EUR 1000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1000, the payment service provider of the payee need not verify the accuracy of the information on the payee, unless the payment service provider of the payee:

(a) effects the pay-out of the funds in cash or in anonymous electronic money; or

(b) has reasonable grounds for suspecting money laundering or terrorist financing.

5. Verification as referred to in paragraphs 3 and 4 shall be deemed to have taken place where:

(a) a payee's identity has been verified in accordance with ***Article 13 of Directive (EU) 2015/849*** ~~Article 13 of Directive (EU) 2015/849 Articles 16, 37 and 18(3) of *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~ and the information obtained pursuant to that verification has been stored in accordance with Article ***40*** ~~5640~~ of that ***Directive*** ~~RegulationDirective~~; or **[AM37, AM205]**

(b) Article ***14(5) of Directive (EU) 2015/849*** ~~21(2) and (3)14(5) of Directive (EU) 2015/849 [please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]~~ applies to the payee. **[AM38, AM206]**

Article 8

Transfers of funds with missing or incomplete information on the payer or the payee

1. The payment service provider of the payee shall implement effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in Article ***13 of Directive (EU) 2015/849*** ~~1613 of Directive (EU) 2015/849 [*please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*]~~, for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action. **[AM39, AM207]**

Where the payment service provider of the payee becomes aware, when receiving transfers of funds, that the information referred to in Article 4(1), points (a), (b) and (c), Article 4(2), points (a) and (b), Article 5(1) or Article 6 is missing or incomplete or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7(1), the payment service provider of the payee shall reject the transfer or ask for the required information on the payer and the payee before or after crediting the payee's payment account or making the funds available to the payee, on a risk-sensitive basis.

2. Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the payment service provider of the payee shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider, or restricting or terminating its business relationship with that payment service provider.

The payment service provider of the payee shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

Article 9

Assessment and reporting

The payment service provider of the payee shall take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported to the Financial Intelligence Unit (FIU) in accordance with ***Directive (EU) 2015/849*** ~~Directive (EU) 2015/849~~ [~~*please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*~~]. **[AM40, AM209]**

SECTION 3

OBLIGATIONS ON INTERMEDIARY PAYMENT SERVICE PROVIDERS

Article 10

Retention of information on the payer and the payee with the transfer

Intermediary payment service providers shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer.

Article 11

Detection of missing information on the payer or the payee

1. The intermediary payment service provider shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.

2. The intermediary payment service provider shall implement effective procedures, including, where appropriate, *ex-post* monitoring or real-time monitoring, in order to detect whether the following information on the payer or the payee is missing:

(a) for transfers of funds where the payment service providers of the payer and the payee are established in the Union, the information referred to in Article 5;

(b) for transfers of funds where the payment service provider of the payer or of the payee is established outside the Union, the information referred to in Article 4(1), points (a), (b) and (c), and Article 4(2), points (a) and (b);

(c) for batch file transfers where the payment service provider of the payer or of the payee is established outside the Union, the information referred to in Article 4(1) and (2) in respect of that batch file transfer.

Article 12

Transfers of funds with missing information on the payer or the payee

1. The intermediary payment service provider shall establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow up action.
Where the intermediary payment service provider becomes aware, when receiving transfers of funds, that the information referred to in Article 4(1), points (a), (b) and (c), Article 4, points (2)(a) and (b), Article 5(1) or Article 6 is missing or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7(1) it shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the transfer of funds, on a risk-sensitive basis.
2. Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the intermediary payment service provider shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider, or restricting or terminating its business relationship with that payment service provider.
The intermediary payment service provider shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

Article 13

Assessment and reporting

The intermediary payment service provider shall take into account missing information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious, and whether it is to be reported to the FIU in accordance with ***Directive (EU) 2015/849*** ~~Directive (EU) 2015/849~~ [~~*please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*~~]. **[AM41, AM213]**

COMPROMISE D - Article 14 and 15

covers AMs 42-57, 214-240, 242-261

CHAPTER III

OBLIGATIONS ON ~~CRYPTO-ASSET SERVICE PROVIDER~~PROVIDER OF CRYPTO-ASSET TRANSFERSS

SECTION 1

OBLIGATIONS ON THE ~~CRYPTO-ASSET SERVICE PROVIDER~~PROVIDER OF CRYPTO-ASSET TRANSFERS OF THE ORIGINATOR

Article 14

Information accompanying transfers of crypto-assets

1. The ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator shall ensure that transfers of crypto-assets are accompanied by the following information on the originator: [AM42, AM214]

(a) the name of the originator;

(b) ***the originator's wallet address, where a transfer of crypto-assets is registered on a network using distributed ledger technology or similar technology and the crypto-asset*** account number of the originator, where an account is used to process the transaction; **[AM43, 216, 217, 218]**

(b a) the originator's crypto-asset account number, where a transfer of crypto-assets is not registered on a network using distributed ledger technology or similar technology; **[AM219, 220]**

(c) the originator's address, ***country,*** official personal document number, customer identification number or date and place of birth. **[AM221, 222]**

(c a) subject to the existence of the necessary field in the relevant message format, and where provided by the originator to the originator's ~~crypto-asset service provider~~provider of crypto-asset transfers, the current LEI of the originator. **[AM223, 224]**

2. The ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator shall ensure that transfers of crypto-assets are accompanied by the following information on the beneficiary: **[AM46]**

(a) the name of the beneficiary;

(b) the beneficiary's ***wallet address, where a transfer of crypto-assets is registered on a network using distributed ledger technology or similar technology and the beneficiary's crypto-asset*** account number, where such an account exists and is used to process the transaction; **[AM47, 226, 227, 218]**

(b a) the beneficiary's crypto-asset account number, where a transfer of crypto-assets is not registered on a network using distributed ledger technology or similar technology; **226]**

***(bb) subject to the existence of the necessary field in the relevant message format, and where provided by the beneficiary to the crypto- asset service provider of the beneficiary ~~or other obliged entity~~, the current LEI of the beneficiary or any other available equivalent official identifier.* [AM49, 226]**

3. By way of derogation from paragraph 1, point (b), and paragraph 2, point (b), in the case of a transfer not made from or to an account, the ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator shall ensure that the transfer of crypto-assets ***is accompanied by a unique transaction identifier*** **[AM44]** ~~can be individually identified~~ and record the originator and beneficiary address identifiers on the distributed ledger. ***For this purpose, ~~crypto-asset service provider~~providers of crypto-asset transfers shall rely on suitable tools, including innovative technological solutions, to ensure that the transfer of crypto-assets can be individually identified.***

4. The information referred to in paragraphs 1 and 2 ***shall be submitted previously, simultaneously or concurrently with the transfer of crypto-assets and in a secure manner and in line with the provisions and obligations of Regulation (EU) 2016/679.~~, provided that either of the following applies:~~***

~~(a) the crypto-asset service provider of the beneficiary is a regulated entity established within the Union;~~

~~(b) the crypto-asset service provider of the beneficiary is established in a third country and is able to receive and retain the information required under this Regulation and applies secure measures and adequate safeguards for protecting the confidentiality of personal ensuring data protection.~~

The information referred to in paragraph 1, points (a) and (c), and paragraph 2, point (a), shall not be attached directly to, or be included in, the transfer of crypto-assets. **[AM51, 235, 237]**

4a. Where the ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator knows, suspects or has reasonable grounds to suspect that the ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary does not apply appropriate measures in line with Regulation (EU) 2016/679 to protect personal data ~~secure measures and adequate safeguards for protecting the confidentiality of personal ensuring data protection~~, the ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator shall proceed with the execution of the transfer without transmitting the information referred to in paragraph 1 points (a) and (c) and paragraph 2 point (a).

Such information shall however be retained pursuant to Article 21 of this Regulation and made available to competent authorities upon request.

***~~Crypto-asset service provider~~Providers of crypto-asset transfers shall establish and maintain alternative procedures consistent with the objectives of this Regulation, including the possibility of not sending personally identifiable information. Those procedures shall be subject to appropriate review by competent authorities.* [AM238]**

4b. EBA shall issue guidelines in accordance with Article 30 to specify the criteria for assessing whether the provider of the originator is able to protect personally identifiable information and the conditions for establishing alternative procedures to ensure the traceability of transfers, where the submission of information to the provider of the beneficiary shall be avoided. **[AM238]**

5. Before transferring crypto-assets, the ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator shall verify the accuracy of the information referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source.

5a. Before transferring crypto-assets, the ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator shall screen the information referred to paragraph 2 to verify that the beneficiary of the transfer is not a designated individual, entity or group subject to targeted restrictive measures or determine if there are any other money laundering or terrorism financing risks **[AM248]**

5b. In the case of a transfer of crypto-assets made to an unhosted wallet, the ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator shall collect and retain information referred to paragraph 1 and 2, including from its customer, verify this information in accordance with paragraph 5, and ensure that the transfer of crypto-assets can be individually identified. For transfers to unhosted crypto-wallets which are already verified and have a known beneficiary, crypto-asset service providers shall not be required to verify information of the originator accompanying each transfer of crypto-assets. Such information shall be made available to competent authorities upon request in accordance with article 33 of Directive (EU) 2015/849. **[AM52, 240]**

Providers of crypto-asset transfers shall adopt effective measures to ensure that the verification of the ownership information in relation to unhosted wallets does not cause undue delay to the execution of the intended transfers.

6. Verification as referred to in paragraph 5 shall be deemed to have taken place where

(a) the identity of the originator has been verified in accordance with Article ***13 of Directive (EU) 2015/849*** ~~16, 18(3) and 37 of Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~ [and the information obtained pursuant to that verification has been stored in accordance with Article ***40 of that Directive*** ~~56 of Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~ or

(b) Article ***14(5) of Directive (EU) 2015/849*** ~~21(2) and (3) of Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~ applies to the originator. **[AM246]**

6 a. ~~Crypto-asset service provider~~Providers of crypto-asset transfers may rely on other ~~crypto-asset service provider~~providers of crypto-asset transfers, whether situated in a

Member State or in a third country, to screen the information on the beneficiary of a transfer to ensure compliance with this Regulation and any restrictive measures, provided that the applicable conditions laid down in Section IV of Directive (EU) 2015/849 are respected. **[AM250]**

7. ~~Without prejudice to the derogation provided for in Article 15(2),~~ The ~~crypto-asset service provider~~provider of crypto-asset transfers of the originator shall not execute any transfer of crypto-assets before ensuring full compliance with this Article.

Article 15

Transfers of crypto-assets

1. In the case of a batch file transfer from a single originator, Article 14(1) shall not apply to the individual transfers bundled together therein, provided that the batch file contains the information referred to in Article 14(1), (2) and (3), that that information has been verified in accordance with Article 14(5) and (6), and that the individual transfers ***are accompanied by the wallet address and the crypto-asset*** account number of the originator, ***where an account is used to process the transaction,*** or, where Article 14(3) applies the individual identification of the transfer. **[AM253]**

~~**2. By way of derogation from Article 14(1), transfers of crypto-assets not exceeding EUR 1 000 that do not appear to be linked to other transfers of crypto-assets which, together with the transfer in question, exceed EUR 1 000, shall be accompanied by at least the following information:**~~

~~**(a) the names of the originator and of the beneficiary;**~~

~~**(b) the account number of the originator and of the beneficiary or, where Article 14(3) applies, the insurance that the crypto-asset transaction can be individually identified;**~~

~~**By way of derogation from Article 14(5), the crypto-assets service provider of the originator shall only verify the information on the originator referred to in this paragraph, first subparagraph, points (a) and (b), in the following cases:**~~

~~**(a) the crypto-assets service provider of the originator has received the crypto-assets to be transferred in exchange of cash or anonymous electronic money;**~~

~~**(b) the crypto-assets service provider of the originator has reasonable grounds for suspecting money laundering or terrorist financing.** **AM254, 255, 256]**~~

COMPROMISE E - Articles 16-18

covers AMs 58, 66; 262-297

SECTION 2

Obligations on the ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary

Article 16

Detection of missing information on the originator or the beneficiary

1. The ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary shall implement effective procedures, including, where appropriate, monitoring after or during the transfers, in order to detect whether the information referred to in Article 14(1) and (2), on the originator or the beneficiary is included in, or follows, the transfer of crypto-assets or batch file transfer.

2. ~~In the case of transfers of crypto-assets exceeding EUR 1 000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, b~~ ***B***efore making the crypto-assets available to the beneficiary, the ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary shall verify the accuracy of the information on the beneficiary referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source, without prejudice to the requirements laid down in Articles 83 and 84 of Directive (EU) 2015/2366. [**266, 267]**

2a. Before making the crypto-assets available to the beneficiary, the ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary shall screen the information referred to in paragraph 2 to verify that the originator of the transfer is not an individual, entity or group subject to targeted restrictive measures or determine if there are any other money laundering or terrorism financing risks. **[AM285]**

~~3. In the case of transfers of crypto-assets not exceeding EUR 1 000 that do not appear to be linked to other transfers of crypto-asset which, together with the transfer in question, exceed EUR 1 000, the crypto-asset service provider of the beneficiary shall only verify the accuracy of the information on the beneficiary in the following cases:~~

~~(a) where the crypto-asset service provider of the beneficiary effects the pay-out of the crypto-assets in cash or anonymous electronic money;~~

~~(b) where the crypto-asset service provider of the beneficiary has reasonable grounds for suspecting money laundering or terrorist financing.~~ **[AM61, 273, 274]**

4. Verification as referred to in paragraphs 2 and 3 shall be deemed to have taken place where one of the following applies:

(a) the identity of the crypto-assets transfer beneficiary has been verified in accordance with ***Article 13 of Directive (EU) 2015/849*** ~~[replace with right reference in AMLR to replace Articles 16, 18(3) and 37 of Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~ and the information obtained pursuant to that verification has been stored in accordance with Article ***40 of that Directive*** ~~56 of Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~; **[AM280, 281]**

(b) Article ***14(5) of Directive (EU) 2015/849*** ~~21(2) and (3) of Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~ applies to the crypto-assets transfer beneficiary. **[AM280, 283]**

4 a. In the case of a transfer of crypto-assets from an unhosted wallet, the ~~***crypto-asset service provider***~~***provider of crypto-asset transfers*** ***of*** ***crypto-asset transfers of*** ***the beneficiary shall collect and retain the information referred to in Article 14(1) and (2) from its customer, verify this information in accordance with paragraph 2 and ensure that the transfer of crypto-assets can be individually identified. For transfers from unhosted crypto-wallets which are already verified and have a known originator, crypto-asset service providers should not be required to verify information of the originator accompanying each transfer of crypto-assets.***

~~***The crypto-asset service provider shall maintain a record of all transfers of crypto-assets from unhosted wallets and make such information available to competent authorities.***~~ **[263, 264, 265]**

~~***In the case of a transfer of crypto-assets from an unhosted wallet, the crypto-asset service provider of the beneficiary shall obtain and retain the information referred to in Article 14(1) and (2) from its customer.***~~

~~***The crypto-asset service provider***~~ ***The provider of crypto-asset transfers shall maintain a record of all transfers of crypto-assets from unhosted wallets and notify competent authority of any customer having received EUR 1 000 or more from unhosted wallets. [AM 264].***

Providers of crypto-asset transfers shall adopt effective measures to ensure that the intended transfers are not unduly delayed by the verification procedures of the ownership information in relation to unhosted wallets and reporting procedures. -

Article 17

Transfers of crypto-assets with missing or incomplete information on the originator or the beneficiary

1. The ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary shall implement effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in ***Article 13 of Directive (EU) 2015/849*****, [AM289],** ~~Articles 16, 18(3) and 37 of Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~, ***including procedures to detect the origin or destination of the transferred crypto-assets***, for determining whether to execute or reject a transfer of crypto-assets lacking the required complete originator and beneficiary information ***or a transfer that is detected as suspicious*** **[AM64]** and for taking the appropriate follow-up action.

Where the ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary becomes aware, ***before making the*** ~~when receiving~~ transfers of crypto-assets ***available to the beneficiary***, that the information referred to in Article 14(1) or (2) or Article 15 is missing or

incomplete, ***or a transfer that is suspicious,*** the ~~crypto-asset service provider~~provider of crypto-asset transfers shall ***on a risk-sensitive basis:***

a) immediately **[AM290]** reject the transfer or ***return the transferred crypto-assets to the originator's crypto-asset account or wallet address; or***

b) ask for the required information on the originator and the beneficiary ***on the shortest term possible*** before ~~**or after**~~ making the crypto-assets available to the beneficiary~~, on a risk-sensitive basis~~ **[AM291, 292];**

c) report to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions and hold the transferred crypto-assets without making them available to the beneficiary, pending review by the competent authority, that must provide specific instructions on the shortest term possible . **[AM288, 293]**

2. Where a ~~crypto-asset service provider~~provider of crypto-asset transfers repeatedly fails to provide the required information on the originator or the beneficiary, the ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary shall take steps, which may initially include the issuing of warnings and setting of deadlines, and return the transferred crypto-assets to the originator's account or address. ~~Alternatively, the crypto-asset service provider of the beneficiary may hold the transferred crypto-assets without making them available to the beneficiary, pending review by the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.~~

The ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

The ~~crypto-asset service provider~~provider of crypto-asset transfers ~~or obliged entity~~ shall also determine on a risk sensitive basis whether to reject any future transfers of crypto-assets from or to, restrict or terminate its business relationship with, that ~~crypto-asset service provider~~provider of crypto-asset transfers. **[AM66]**

Article 18

Assessment and reporting

The ~~crypto-asset service provider~~provider of crypto-asset transfers of the beneficiary shall take into account missing or incomplete information on the originator or the beneficiary when assessing whether a transfer of crypto-assets, or any related transaction, is suspicious and whether it is to be reported to the FIU in accordance with ***Directive (EU) 2015/849*** ~~Regulation [*please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*].~~ [AM67,298]

COMPROMISE F - Article 18a

covers AMs 304-308

Article 18 a

By 12 months after the entry into force of this Regulation, the EBA shall issue guidelines to specify how the relevant obligations imposed on providers of crypto-assets transfers also apply to intermediary providers of crypto-assets transfers, taking into account international standards.

~~***SECTION 2 A*** [**AM 304-308**]~~

~~***OBLIGATIONS ON INTERMEDIARY CRYPTO-ASSET SERVICE PROVIDERS***~~

~~***Article 18 a (new)***~~

~~***Retention of information on the originator and the beneficiary with the transfer***~~

~~***Intermediary crypto-asset service providers shall ensure that all the information received on the originator and the beneficiary that accompanies a transfer of funds is transmitted with the transfer and that records of such information are retained and made available on request to the competent authorities.***~~

~~***Article 18 b***~~

~~***Detection of missing information on the originator or the beneficiary***~~

~~***1. The intermediary crypto-asset service providershall implement effective procedures, including, where appropriate, monitoring after or during the transfers, to detect whether the information referred to in Article 14(1) points (a), (b) and (c) and Article 14 (2) points (a), (b) and (ba) on the originator or the beneficiary is submitted previously, simultaneously or concurrently with with the transfer of crypto-assets or batch file transfer, including where the transfer is made from an unhosted wallet.***~~

~~***2. Before making the crypto-assets available to the beneficiary, the intermediary crypto-asset service providerof the beneficiary shall verify the accuracy of the information on the beneficiary referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source, without prejudice to the requirements laid down in Articles 83 and 84 of Directive (EU) 2015/2366.***~~

~~***Article 18 c***~~

~~***Transfers of crypto-assets with missing information on the originator or the beneficiary***~~

~~***1. The intermediary crypto-asset service providershall implement effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in Article 13 of Directive (EU) 2015/849, or determining whether to execute, reject or suspend a transfer of crypto-asset lacking the required complete originator and beneficiary information or a***~~

~~*transfer that is detected as suspicious* [AM64] *and for taking the appropriate follow up action.*~~

~~*Where the intermediary crypto-asset service provider becomes aware, when receiving transfers of crypto-assets, that the information referred to in Article 14(1), points (a), (b) and (c), Article 14, points (2)(a) and (b), or Article 15 is missing or incomplete, the intermediary crypto-asset service providershall reject the transfer or ask for the required information on the originator and the beneficiary before or after making the crypto-assets available to the beneficiary, on a risk-sensitive basis.*~~

~~*Alternatively, the intermediary crypto-asset service providerof the beneficiary may hold the transferred crypto-assets without making them available to the beneficiary, until such information has been obtained.*~~

~~*2. Where a crypto-asset service providerrepeatedly fails to provide the required information on the originator or the beneficiary, the intermediary crypto-asset service providershall take steps, which may initially include the issuing of warnings and setting of deadlines, and return the transferred crypto-assets to the originator's crypto-asset account or wallet address.*~~

~~*The intermediary crypto-asset service of the beneficiary shall also determine whether to reject any future transfers of crypto-assets from, restrict or terminate its business relationship with, that crypto-asset service provider.*~~

~~*The intermediary crypto-asset service providershall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.*~~

~~*Article 18 d*~~

~~*Assessment and reporting*~~

~~*The intermediary crypto-asset service providershall take into account missing information on the originator or the beneficiary as a factor when assessing whether a transfer of crypto-asset, or any related transaction, is suspicious, and whether it is to be reported to the FIU in accordance with Directive (EU) 2015/849.*~~

COMPROMISE G - Article 18aa-~~18ae~~ 18ad *(new)*

covers AMs 68, 299-301

REVISED TEXT (CLEAN VERSION)

CHAPTER IVA (NEW)

MITIGATION MEASURES FOR TRANSFERS OF CRYPTO-ASSETS

Article 18aa (new)

Prohibition of transfers with non-compliant providers

1. ~~Crypto-asset service provider~~Provider of crypto-asset transfers and intermediary ~~crypto-asset service provider~~provider of crypto-asset transfers shall not facilitate any transfer of crypto-assets to or from non-compliant ~~crypto-asset service provider~~provider of crypto-asset transfers.

The following services shall be deemed as non-compliant ~~crypto-asset service provider~~provider of crypto-asset transfers:

a) ~~crypto-asset service provider~~provider of crypto-asset transfers that are not established or do not have any central contact point or substantive management presence in any jurisdiction and which are unaffiliated with a regulated entity;

b) ~~crypto-asset service provider~~provider of crypto-asset transfers operating in the Union without authorisation under Regulation [Regulation on Markets in Crypto-assets].

The condition referred to in point (b) shall apply from [please insert date of application of proposal for a Regulation on Markets in Crypto-assets], without prejudice to any transitional measures set out in that Regulation, as applicable.

Article 18ab (new)

Specific enhanced due diligence measures for counterparty providers

With respect to counterparty relationships involving the execution of transfers with non-EU counterparty provider of crypto-assets transfers, without prejudice to the customer due diligence measures laid down in Directive (EU) 2015/849, providers of crypto-asset trasfers shall be required, when entering into a relationship with a counterparty provider, to:

(a) gather sufficient information about the counterparty to understand fully the nature of the counterparty's business and to determine from publicly available information the reputation of the counterparty and the quality of supervision;

(b) assess the counterparty's AML/CFT controls;

(c) assess the ability of the counterparty to apply secure measures and adequate safeguards for protecting the confidentiality of personal data;

d) obtain approval from senior management before establishing new relationship with a counterparty provider of crypto-asset transfers.

Article 18ac (new)

Specific high-risk factors in relation to transfers of crypto-assets

1. Providers of crypto-assets transfers shall refrain from executing or facilitating transfers associated with high risk of money-laundering, terrorist financing and other criminal activities.

2. Without prejudice to Article 18 ac and the cases of higher risk referred to in Directive (EU) 2015/849, providers of crypto-assets transfers shall implement effective measures to detect whether a transfer of crypto-assets is to be considered high-risk, taking into account at least the following high risk factors:

(1) geographical risk factors:

a) ~~crypto-asset service provider~~provider of crypto-asset transfers registered or domiciled in a country included in the EU AML/CFT list of high risk third countries or in in a third country subject to restrictive measures , or in Annex I or Annex II of the EU list of non-cooperative jurisdictions for tax purposes **[AM131]***;*

(2) counterparty risk factor:

a) providers of crypto-asset transfers ~~crypto-asset service provider~~provider of crypto-asset transfers identified as not applying adequate customer identification and verification procedures;

b) providers of crypto-asset transfers ~~crypto-asset service provider~~provider of crypto-asset transfers identified as not applying secure measures and adequate safeguards for protecting the confidentiality of personal data;

c) providers of crypto-asset transfers ~~crypto-asset service provider~~provider of crypto-asset transfers identified as having links to money laundering, terrorist financing and other illegal activities;

(3) wallet, services risk factor:

a) privacy wallets, mixers or tumblers, or other anonymising services for transfers of crypto-assets; **[302]**

b) crypto-asset wallet addresses, including unhosted wallets, identified as being linked to money laundering, terrorist financing **[AM241]**

3. The provider of crypto-asset transfers ~~crypto-asset service provider~~provider of crypto-asset transfers shall also determine on a risk sensitive basis whether to reject any future transfers of crypto-assets from or to, restrict or terminate its business relationship with, that provider of crypto-asset transfers.

4. Notwithstanding paragraph 1, with respect to privacy wallets, mixers or tumblers, or other anonymising services for transfers of crypto-assets, the provider of the crypto-asset transfer shall obtain additional information on the purpose of the intended transfer and a

justification for legitimate use, before deciding whether to reject or suspend a transfer, and shall report its decision to the competent authority. **[AM68, AM299, 300, 301]**

Article 18 ad (new)

Public register on non-compliant or high-risk providers of crypto-asset transfers ~~crypto-asset service providers~~ and high-risk wallet addresses

1. In order to facilitate compliance with Article aa (new) and Article ab (new), the EBA shall set up and maintain an non-exhaustive public register to enable centralised access to the following information:

a) non-compliant providers of crypto-asset transfers ~~crypto-asset service provider~~operating within and outside the Union as referred to in Article 18 aa (new); and

b) high-risk providers of crypto asset services;

c) high-risk wallet addresses **[AM 241].**

2. The EBA shall regularly review the public register taking into account any changes of circumstances concerning the providers, services and wallet addresses included in the register or any information that is brought to its attention. **[AM70]**

3. The information contained in the EBA public register shall be available in machine-readable format and allow the extraction of data by ~~crypto-asset service provider~~provider of crypto-asset transfers.

4. Where a provider of crypto-asset transfers ~~crypto-asset service providers~~ becomes aware that a counterparty provider or another provider of crypto-asset transfers ~~crypto-asset service provider~~ operating within or outside the Union might be a non-compliant providers of crypto-asset transfers ~~crypto-asset service provider~~ in accordance with Article 18 aa (new) or that provider ~~crypto-asset service~~ or wallet address might be deemed high-risk in accordance with Article 18 ab (new), it shall promptly report this information to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.

5. Where a competent authority following an evaluation, concludes that a provider of crypto-asset transfers ~~crypto-asset service provider~~provider of crypto-asset transfers operating within or outside the Union is to considered a non-compliant provider of crypto-asset transfers ~~crypto-asset service provider~~ in accordance with Article 18 aa (new) or that a crypto-asset service or wallet address is to be considered high-risk in accordance with Article 18 ab (new), it shall promptly inform EBA that shall include that information in the register.

The EBA may also carry out an analysis for the purpose of identifying non-compliant providers of crypto-asset transfers ~~crypto-asset service providers~~ or high-risk crypto-asset service or high-risk wallet address to be included in the register on its own initiative.

6. Providers of providers of crypto-asset transfers ~~crypto-asset transfers~~ shall not rely exclusively on the central register to fulfil their enhanced due diligence requirements in accordance with Chapter.

[AM302]

COMPROMISE H - Article 19- 21 a (new)

covers AMs 68, 299-301

CHAPTER IV

INFORMATION, DATA PROTECTION AND RECORD-RETENTION

Article 19

Provision of information

Payment service providers and ***providers of crypto-asset transfers*** ~~crypto-asset service providers~~ shall respond fully and without delay, including by means of a central contact point in accordance with Article ***45(9) of Directive (EU) 2015/849*** **[AM 69, 309]** ~~5(1) of [*please insert reference – proposal for a directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*]~~, where such a contact point has been appointed, and in accordance with the procedural requirements laid down in the national law of the Member State in which they are established, to enquiries exclusively from the authorities responsible for preventing and combating money laundering or terrorist financing of that Member State concerning the information required under this Regulation.

Article 20

Data protection

1. The processing of personal data under this Regulation is subject to Regulation (EU) 2016/679. Personal data that is processed pursuant to this Regulation by the Commission or EBA is subject to Regulation (EU) 2018/1725.

2. Personal data shall be processed by payment service providers and ***providers of crypto-asset transfers***~~crypto-asset service providers~~ on the basis of this Regulation only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Regulation for commercial purposes shall be prohibited.

3. Payment service providers and ***providers of crypto-asset transfers*** ~~crypto-asset service providers~~ shall provide new clients with the information required pursuant to Article 13 of Regulation (EU) 2016/679 before establishing a business relationship or carrying out an occasional transaction. That information shall ***be accessible, clear and transparent including [310]***~~,~~ in particular, include a general notice concerning the legal obligations of payment service providers and ~~crypto-asset service provider~~provider of crypto-asset transfers under this Regulation when processing personal data for the purposes of the prevention of money laundering and terrorist financing.

4. Payment and ~~crypto-asset service provider~~ crypto-asset transfers providers shall ensure that the confidentiality of the data processed is respected.

Article 21

Record retention

1. Information on the payer and the payee, or, for transfers of crypto-assets, on the originator and beneficiary, shall not be retained for longer than strictly necessary. Payment service providers of the payer and of the payee shall retain records of the information referred to in Articles 4 to 7 and ~~crypto-asset service provider~~ providers of crypto-asset transfers of the originator and beneficiary shall retain records of the information referred to in Articles 14 to 16, for a period of ~~five~~ ***~~ten~~ five*** years. ***[AM331]***

2. Upon expiry of the retention period referred to in paragraph 1, payment service providers and ~~crypto-asset service provider~~providers of crypto-asset transfers shall ensure that the personal data is ***permanently*** deleted **[AM312].**~~.~~

3. Where ~~on [the date of application of this Regulation],~~ legal proceedings concerned with the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing are pending in a Member State, and a payment service provider holds information or documents relating to those pending proceedings, the payment service provider may retain that information or those documents in accordance with national law for a further period of five years ~~from [the date of application of this Regulation].~~

~~Member States may, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings, allow or require the retention of such information or documents for a further period of five years where the necessity and proportionality of such further retention has been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing.~~
[AM311]

Article 21 a
Cooperation among competent authorities

The exchange of information among national competent authorities and with relevant third country authorities under this Regulation shall be subject to the provisions laid down in Directive (EU) 2015/849.

[AM313]

COMPROMISE I - Article 22-27

covers AMs 70-76; 314-325

AM 326 covered under COMP X (final provisions)

CHAPTER V

SANCTIONS AND MONITORING

Article 22

Administrative sanctions and measures

1. Without prejudice to the right to provide for and impose criminal sanctions, Member States shall lay down the rules on administrative sanctions and measures applicable to breaches of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The sanctions and measures provided for shall be effective, proportionate and dissuasive and shall be consistent with those laid down in accordance with Chapter IV, Section 4, of ***Directive (EU) 2015/849*** **[AM70, AM314]** ~~[*please insert reference – proposal for a directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*]~~.
Member States may decide not to lay down rules on administrative sanctions or measures for breach of the provisions of this Regulation which are subject to criminal sanctions in their national law. In that case, Member States shall communicate to the Commission the relevant criminal law provisions.
2. Member States shall ensure that where obligations apply to payment service~~s~~ providers and ~~crypto-asset service provider~~providers of crypto-asset transfers, in the event of a breach of provisions of this Regulation, sanctions or measures can, subject to national law, be applied to the members of the management body and to any other natural person who, under national law, is responsible for the breach.

3. Member States shall notify the rules referred to in paragraph 1 to the Commission and to the Joint Committee of the ESAs. Member States shall notify the Commission and EBA without undue delay of any subsequent amendments thereto.

4. In accordance with Article ***58(4) of Directive (EU) 2015/849*** **[AM71, 315]** ~~3958(4) of Directive (EU) 2015/849 [*please insert reference – proposal for a directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*],~~ competent authorities shall have ***appropriate resources and*** **[AM316]** all the supervisory and investigatory powers that are necessary for the exercise of their functions. In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.
5. Member States shall ensure that legal persons can be held liable for the breaches referred to in Article 23 committed for their benefit by any person acting individually or as part of an organ of that legal person, and having a leading position within the legal person based on any of the following:

(a) power to represent the legal person;

(b) authority to take decisions on behalf of the legal person; or

(c) authority to exercise control within the legal person.

6. Member States shall also ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 5 has made it possible to commit

one of the breaches referred to in Article 23 for the benefit of that legal person by a person under its authority.

7. Competent authorities shall exercise their powers to impose administrative sanctions and measures in accordance with this Regulation in any of the following ways:

(a) directly;

(b) in collaboration with other authorities;

(c) under their responsibility by delegation to such other authorities;

(d) by application to the competent judicial authorities.

In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely in order to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.

Article 23

Specific provisions

Member States shall ensure that their administrative sanctions and measures include at least those laid down by ***Article 59(2) and (3) of Directive (EU) 2015/849*** ~~Articles 40(2), 40(3) and 41(1)59(2) and (3)~~ of ~~Directive (EU) 2015/849~~ ~~*[please insert reference – proposal for a directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~ in the event of the following breaches of this Regulation **[AM320]**:

(a) repeated or systematic failure by a payment service provider to include the required information on the payer or the payee, in breach of Article 4, 5 or 6 or by a ~~crypto-asset service provider~~provider of crypto-asset transfers to include the required information on the originator and beneficiary, in breach of Articles 14 and 15;

(b) repeated, systematic or serious failure by a payment service provider or ~~crypto-asset service provider~~provider of crypto-asset transfers to retain records, in breach of Article 21;

(c) failure by a payment service provider to implement effective risk-based procedures, in breach of Articles 8 or 12 or by a ~~crypto-asset service provider~~provider of crypto-asset transfers to implement effective risk-based procedures, in breach of Article 17;

(d) serious failure by an intermediary payment service provider to comply with Article 11 or 12.

(da) failure to comply with the prohibition to facilitate transfers to non-compliant ~~crypto-asset service provider~~providers of crypto-asset transfers, in breach of Article 18aa (new). **[AM318]**

Article 24

Publication of sanctions and measures

In accordance with Article ***60(1), (2) and (3) of Directive (EU) 2015/849*** **[AM73, AM320]** ~~42 of *[please insert reference – proposal for a directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~, the competent authorities shall publish administrative sanctions and measures imposed in the cases referred to in Articles 22 and 23 of this Regulation without undue delay, including information on the type and nature of the breach and the identity of the persons responsible for it, if necessary and proportionate after a case-by-case evaluation.

Article 25

Application of sanctions and measures by the competent authorities

1. When determining the type of administrative sanctions or measures and the level of administrative pecuniary sanctions, the competent authorities shall take into account all relevant circumstances, including those listed in Article ***60(4) of Directive (EU) 2015/849*** **[AM74, AM321].**

2. As regards administrative sanctions and measures imposed in accordance with this Regulation, ***Article 62 of Directive (EU) 2015/849*** ~~Articles 6(6) and 44 [...] of [...]Directive (EU) [*please insert reference – proposal for a directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*]~~ shall apply **[AM75, AM322]**.

Article 26

Reporting of breaches

1. Member States shall establish effective mechanisms to encourage the reporting to competent authorities of breaches of this Regulation.

Those mechanisms shall include at least those referred to in Article ***61(2) of Directive (EU) 2015/849*** ~~43of [*please insert reference – proposal for a directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*]~~. **[AM76, AM324]**

2. Payment service providers and ~~crypto-asset service provider~~providers of crypto-asset transfers, in cooperation with the competent authorities, shall establish appropriate internal procedures for their employees, or persons in a comparable position, to report breaches internally through a secure, independent, specific and anonymous channel, proportionate to the nature and size of the payment service provider or the ~~crypto-asset service provider~~provider of crypto-asset transfers concerned.

Article 27

Monitoring

1. Member States shall require competent authorities to monitor effectively and to take the measures necessary to ensure compliance with this Regulation and encourage, through effective mechanisms, the reporting of breaches of the provisions of this Regulation to competent authorities.

2. Two years after the entry into force of this Regulation and every three years thereafter the Commission shall submit a report to the European Parliament and to the Council on the application of Chapter ~~I~~V, with particular regard to cross-border cases.

COMPROMISE J - Article 28-30

covers AMs 77, 327-330

CHAPTER VI

IMPLEMENTING POWERS

Article 28

Committee procedure

1. The Commission shall be assisted by the Committee on the Prevention of Money Laundering and Terrorist Financing. That Committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VII

DEROGATIONS

Article 29

Agreements with countries and territories which do not form part of the territory of the Union

1. The Commission may authorise any Member State to conclude an agreement with a third country or with a territory outside the territorial scope of the TEU and the TFEU as referred to in Article 355 TFEU (the 'country or territory concerned'), which contains derogations from this Regulation, in order to allow transfers of funds between that country or territory and the Member State concerned to be treated as transfers of funds within that Member State.
Such agreements may be authorised only where all of the following conditions are met:

(a) the country or territory concerned shares a monetary union with the Member State concerned, forms part of the currency area of that Member State or has signed a monetary convention with the Union represented by a Member State;

(b) payment service providers in the country or territory concerned participate directly or indirectly in payment and settlement systems in that Member State;

(c) the country or territory concerned requires payment service providers under its jurisdiction to apply the same rules as those established under this Regulation.

2. A Member State wishing to conclude an agreement as referred to in paragraph 1 shall submit a request to the Commission and provide it with all the information necessary for the appraisal of the request.
3. Upon receipt by the Commission of such a request, transfers of funds between that Member State and the country or territory concerned shall be provisionally treated as

transfers of funds within that Member State until a decision is reached in accordance with this Article.

4. If, within two months of receipt of the request, the Commission considers that it does not have all the information necessary for the appraisal of the request, it shall contact the Member State concerned and specify the additional information required.

5. Within one month of receipt of all the information that it considers to be necessary for the appraisal of the request, the Commission shall notify the requesting Member State accordingly and shall transmit copies of the request to the other Member States.

6. Within three months of the notification referred to in paragraph 5 of this Article, the Commission shall decide, whether to authorise the Member State concerned to conclude the agreement that is the subject of the request. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 28(2).

The Commission shall, in any event, adopt a decision as referred to in the first subparagraph within 18 months of receipt of the request.

Article 30

Guidelines

The ESAs shall issue guidelines addressed to the competent authorities, payment service providers ***and*** ~~***crypto asset service***~~ ***providers*** ***of crypto asset transfers*** in accordance with Article 16 of Regulation (EU) No 1093/2010 on measures to be taken in accordance with this Regulation, in particular as regards the implementation of Articles 7, 8, 11 and 12 ***and Articles 14, 16, 17,*** ~~***18-b (new) and 18-c (new)***~~ thereof. From 1 January 2020, EBA shall, where appropriate, issue such guidelines **[AM77, AM 329, AM330]**

The EBA shall issue guidelines specifying technical aspects of the application of this Regulation to direct debits as well as the measures to be taken by payment initiation service providers under this Regulation, taking into account their limited role in the payment transaction. **[AM 329, AM330]**

COMPROMISE K - Article 30a

covers AMs 78, 331-334

Article 30 a

Review Clause

1. By 12 months after the entry into force of Regulation [please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849] the Commission shall review this Regulation and shall, if appropriate, propose amendments in order to ensure alignment with that Regulation and ensure a consistent approach **[AM326, 335].**

2. By 12 months after the entry into application of this Regulation, the Commission shall assess the need of additional specific measures to mitigate the risks posed by transfers from or to unhosted wallets, including an analysis of the ~~***feasibility***~~ ***effectiveness and***

proportionality of ~~introducing~~ mechanisms to obtain and verify the accuracy of the information concerning the ownership of unhosted wallets and the need of applying restrictions on transfers from/to unhosted wallets **[AM78, AM266, 271, 303]** *and present, if appropriate, amendments to this Regulation.*

~~2~~3. By ... [please insert ~~2~~ 3 **[AM 332]** *years from the date of entry into force of this Regulation], the Commission shall submit to the European Parliament and to the Council a report on the application and enforcement of this Regulation accompanied, if appropriate, by a legislative proposal.*

That report shall include the following elements:

(a) an assessment of the effectiveness of the measures provided for in this Regulation and the compliance by payment service providers and ~~crypto-asset service provider~~providesr of crypto-asset transfers **[AM 78];**

(aa), ~~in particular as regards~~ an assessment of the development of technological solutions for complying with their obligations, including the latest developments in crypto-asset industry-led standard settings initiatives that mirror existing messaging and reporting data standards and the use of blockchain analysis for identifying the origin and destination of transfers in crypto-assets and know your transaction (KYT) assessment; **[AM78, AM331, 332]**

ab) an assessment of the effectiveness and suitability of the de minimis thresholds related to transfers of funds, in particular with respect to the scope of application and the set of information accompanying transfers, and an assessment of the need of lowering or removing such threshold relateds to transfer of funds **[AM333];**

ac) assessment of the costs and benefits of introducing de minimis thresholds related to the set of information accompanying transfers of crypto-assets, including an assessment of the related money laundering and terrorist financing risks; **[AM334]**

(b) an assessment of the effectiveness of international cooperation and information exchange between competent authorities and FIUs; **[AM78, AM332]**

(c) the impact of the measures provided for in this Regulation on data protection and fundamental rights; **[AM332, 334]**

(d) an assessment as regards to the application of sanctions, in particular whether they are effective, proportionate and dissuasive, and the need to further harmonise the administrative sanctions laid down in Chapter V for infringements of the requirements established in this Regulation;

~~*(e) an analysis of the need of specific measures to mitigate the risks posed by transfers from or to unhosted wallets, including an analysis of the feasibility and proportionality of mechanisms to obtain and verify the accuracy of the information concerning the ownership of unhosted wallet and an assessment the impact of restrictions on transfers from/to unhosted wallets* **[AM78, AM266, 271, 303];**~~

(f) an analysis of the trends in the use of unhosted wallets to perform transfers without the involvement of a third party, together with an assessment of the related money laundering and terrorist financing risks and an evaluation of the need, effectiveness and enforceability of additional mitigation measures, including specific obligations on providers of hardware and software wallets and limitations, control or prohibition of transfers involving unhosted wallets;

(g) an assessment on the systematic coherence of this Regulation with the European legislation on Anti-Money Laundering and Countering Terrorist Financing (AML/CFT).

The Report shall take into account the developments as well as relevant evaluations, assessments or reports drawn up by international organisations and standard setters in the field of preventing money laundering and combating terrorist financing, law enforcement authorities and intelligence agencies and any information provided by crypto-assets service providers or reliable sources. **[AM78, 331, 332]**

COMPROMISE L - Article 30b (new) - Article 32

covers AMs 79-80, 335-341

CHAPTER VIII

FINAL PROVISIONS

Article 30 b (new) **[AM79, 337]**
Amendments to Directive (EU) 2015/849

1. Directive (EU) 2015/849 is amended as follows:

(1) Article 2(1), point 3, is amended as follows:

(a) point (g) is replaced by the following:

'(g) ~~crypto-asset service provider~~providers of crypto-asset transfers;';

(b) point (h) is deleted;

(2) Article 3 is amended as follows:

(a) point 18 is replaced by the following:

''(18) 'crypto-asset' means a crypto-asset as defined in Article 3(1), point (2), of Regulation [please insert reference –proposal for a Regulation on Markets in Crypto-assets, and amending Directive(EU) 2019/1937 - COM/2020/593 final] except when falling under the categories listed in Article 2(2) and (2a) of that Regulation or otherwise qualifying as funds;';

(b) point 19 is replaced by the following:

''(19) '~~crypto-asset service provider~~provider of crypto-asset transfers' means a crypto-assets service provider as defined in Article 3(1), point (8), of Regulation [Regulation on Markets in Crypto-assets] where performing one or more crypto-asset services as defined in Article 3(1), point (9), of that Regulation, with the exception of providing advice on crypto-assets as defined in point (9)(h) of that Article.

2. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with the previous paragraph by... [please insert reference to the date of application of proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final]. They shall immediately communicate the text of those provisions to the Commission.

Article 30c (new) **[AM338]**

Transitional arrangements

1. Member States shall ensure that payment service providers, ~~crypto-asset service provider~~providers of crypto-asset transfers, and intermediary payment service providers as well as intermediary ~~crypto-asset service provider~~providers of crypto-asset transfers are licensed or registered, subject to adequate supervision in accordance with Article 47 of Directive 2015/849.
2. Member States shall require competent authorities to ensure that the persons who hold a management function in the entities referred to in paragraph 1, or are the beneficial owners of such entities, are fit and proper persons.

~~2~~3. The ~~ESAs~~ EBA shall be responsible for providing guidance and to assist the relevant supervisors until the date on which the Anti-Money Laundering Authority becomes operational, in accordance with [please insert reference to the date of application of proposal for a AML Authority Regulation].

~~3~~4. For the purposes of paragraph 2, and in order to facilitate and promote effective cooperation, and in particular the exchange of information, the EBA ~~ESAs~~ shall issue guidelines, addressed to competent authorities, on the characteristics of a risk-based approach to supervision and the steps to be taken when conducting supervision on a risk-based basis.
Within 3 months of the entry into force of this Regulation, the EBA ~~ESAs~~ shall issue such guidelines, taking into account relevant information on the risks associated with customers, products and services offered by ~~these~~ providers of crypto-assets transfers~~entities~~, as well as geographical risk factors.

By [please insert reference to the date of application of proposal for an AML Authority Regulation] the responsibilities attributed to the EBA shall be taken over by AMLA, without prejudice to any additional competences attributed under that Regulation.

Article 30d (new)

Alignment with Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets]

The Commission is empowered to adopt delegated acts within 3 months after the adoption of Regulation [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final] in order to update and align the definitions contained in article 3, paragraph 1, points 10, 13, 14, and 15 ~~and 16~~ of this Regulation with the relevant definitions contained in that Regulation, where necessary. ~~in case there are any discrepancies.~~
~~By means of delegated acts, the Commission shall update and align this Regulation following the entry into force of Regulation [please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849].~~

[AM326, 335]

Article 31

Repeal

Regulation (EU) 2015/847 is repealed.
References to the repealed Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table in Annex II.

Article 32

Entry into force

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

By [please insert 96 ~~6~~ months after entry into force of this Regulation] providers of services relating to transfers of crypto-assets that are obliged entities under Directive (EU) 2015/849 shall adopt a rollout plan to carry out the phase-in implementation of this Regulation in accordance with guidelines issued by the EBA, in order to ensure full compliance with the obligations of this Regulation by [please insert 18 ~~12~~ months after entry into force of this Regulation].

By [please insert 3 months after entry into force of the proposal] EBA shall adopt guidelines to specify the conditions to facilitate the phased-in implementation of this Regulation. **[AM339]**

~~4. Where, due to the lack of technological capability, a crypto-asset service provider is unable to comply with the requirements laid down under this Regulation, it may request the competent authority to grant an additional transitional period to comply with those requirements, provided that such request is duly justified.~~

~~5. The competent authority, after consultation of the EBA, may grant a transitional period up to 6 months, on a case-by-case basis, where duly justified by the lack of technological capability and the scale of operations of the provider, and may require compensatory measures to restrict certain transfers of crypto-assets.~~ **~~[AM336]~~**

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

Transfer of Funds Regulation

Draft Compromise on Recitals - V2 - 25 March 2022

Compromise V

AMs 1-22; 81-140

Whereas:

(1) Regulation (EU) 2015/847 of the European Parliament and of the Council[1] has been substantially amended[2]. Since further amendments are to be made, that Regulation should be recast in the interests of clarity.

(2) Regulation (EU) 2015/847 was adopted to ensure that the Financial Action Task Force (FATF) requirements on wire transfers services providers, and in particular the obligation on payment service providers to accompany transfers of funds with information on the payer and the payee, were applied uniformly throughout the Union. The latest changes introduced in June 2019 in the FATF standards on new technologies, aiming at regulating so called virtual assets and virtual asset service providers, have provided new and similar obligations for virtual asset service providers, with the purpose to facilitate the traceability of transfers of virtual assets. Thus, under those new requirements, virtual asset transfer service providers must accompany transfers of virtual assets with information on their originators and beneficiaries, that they must obtain, hold, share with counterpart at the other hand of the virtual assets transfer and make available on request to ~~appropriate~~ ***competent*** authorities.

(3) Given that Regulation (EU) 2015/847 currently only applies to transfer of funds, in the meaning of banknotes and coins, scriptural money and electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC, it is appropriate to extend the scope in order to also cover transfer of virtual assets.

(4) Flows of illicit money through transfers of funds and crypto-assets can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development. Money laundering, terrorist financing and organised crime remain significant problems which should be addressed at Union level. The soundness, integrity and stability of the system of transfers of funds and crypto-assets as well as and confidence in the financial system as a whole , could be seriously jeopardised by the efforts of criminals and their associates to disguise the origin of criminal proceeds or to transfer funds or crypto-assets for criminal activities or terrorist purposes.

(5) In order to facilitate their criminal activities, money launderers and financers of terrorism are likely to take advantage of the freedom of capital movements within the Union's integrated financial area unless certain coordinating measures are adopted at Union level. International cooperation within the framework of ~~the Financial Action Task Force (~~FATF~~)~~ and the global implementation of its recommendations aim to

---

[1] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (OJ L 141, 5.6.2015, p. 1).

[2] See Annex I.

prevent money laundering and terrorist financing while transferring funds or crypto-assets .

(6) By reason of the scale of the action to be undertaken, the Union should ensure that the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by FATF on 16 February 2012 and then on 21 June 2019 (~~the~~ 'revised FATF Recommendations~~'~~), and, in particular, FATF Recommendation 15 on new technologies (FATF Recommendation 15), FATF Recommendation 16 on wire transfers (~~the~~ 'FATF Recommendation 16') and the revised interpretative notes on those Recommendations ~~note for its implementation~~, are ~~implemented~~ applied uniformly throughout the Union and that, in particular, there is no discrimination or discrepancy between, on the one hand, national payments or transfers of crypto-assets within a Member State and, on the other, cross-border payments or transfers of crypto-assets between Member States. Uncoordinated action by Member States acting alone in the field of cross-border transfers of funds and crypto-assets could have a significant impact on the smooth functioning of payment systems and crypto-asset transfer services at Union level and could therefore damage the internal market in the field of financial services.

(7) In order to foster a coherent approach in the international context and to increase the effectiveness of the fight against money laundering and terrorist financing, further Union action should take account of developments at international level, ~~namely~~ in particular the revised FATF Recommendations.

(7a) The global reach, the speed at which transactions can be carried out and the possible anonymity offered by crypto-asset transactions make crypto-assets particularly suitable for criminals seeking to carry out illicit transfers across jurisdictions and operate beyond national borders. In order to effectively address the risks posed by the misuse of crypto-assets for money laundering and terrorist financing purposes, the Union should aim to advance the implementation at global level of the standards established under this Regulation and also to develop the international and cross-jurisdictional dimension of the regulation and supervision of transfers of crypto-assets in relation to money laundering and terrorist financing.

(8) Directive (EU) 2018/843 of the European Parliament and of the Council[3] introduced a definition of virtual currencies and recognised providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers among the entities submitted to anti-money laundering and countering terrorism financing requirements in the Union legal framework. The latest international developments, notably within the FATF, now implies the need to regulate additional categories of virtual asset service providers not yet covered as well as to broaden the current definition of virtual currency.

(9) It is to be noted that the definition of crypto-assets in Regulation[4] [please insert reference – proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937-COM/2020/593 final] corresponds to the definition of virtual assets set out in the recommendations of FATF, and the list of crypto-asset services and crypto-asset service providers covered in that Regulation also encompass the virtual asset services providers identified as such by FATF and considered as likely to raise money-laundering concerns. In order to ensure the coherency of the

---

[3] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156, 19.6.2018, p. 43).

[4] References to MiCA to be added once the text adopted

Union legal framework, this proposal should refer to those definitions of crypto-assets and crypto-asset service providers.

(10) The implementation and enforcement of this Regulation~~, including FATF Recommendation 16,~~ represent relevant and effective means of preventing and combating money-laundering and terrorist financing.

(11) This Regulation is not intended to impose unnecessary burdens or costs on payment service providers , crypto-asset service providers or on persons who use their services. In this regard, the preventive approach should be targeted and proportionate and should be in full compliance with the free movement of capital, which is guaranteed throughout the Union.

(12) In the Union's Revised Strategy on Terrorist Financing of 17 July 2008 (the 'Revised Strategy'), it was pointed out that efforts must be maintained to prevent terrorist financing and to control the use by suspected terrorists of their own financial resources. It is recognised that FATF is constantly seeking to improve its Recommendations and is working towards a common understanding of how they should be implemented. It is noted in the Revised Strategy that implementation of the revised FATF Recommendations by all FATF members and members of FATF-style regional bodies is assessed on a regular basis and that a common approach to implementation by Member States is therefore important.

(13) In addition, the Commission Action Plan of 7 May 2020 for a comprehensive Union policy on preventing money laundering and terrorism financing[5] identified six priority areas for urgent action to improve the Union's anti-money laundering and countering financing of terrorism regime, including the establishment of a coherent regulatory framework for that regime in the Union to obtain more detailed and harmonised rules, notably to address the implications of technological innovation and developments in international standards and avoid diverging implementation of existing rules. Work at international level suggests a need to expand the scope of sectors or entities covered by the anti-money laundering and countering financing of terrorism rules and to assess how they should apply to ~~virtual crypto-assets service~~ providers ***~~of crypto-asset transfers~~*** not covered so far.

(14) In order to prevent terrorist financing, measures with the purpose of freezing the funds and the economic resources of certain persons, groups and entities have been taken, including Council Regulations (EC) No 2580/2001[6], (EC) No 881/2002[7] and (EU) No 356/2010[8]. To the same end, measures with the purpose of protecting the financial system against the channelling of funds and economic resources for terrorist purposes have also been taken. ~~Directive (EU) 2015/849 of the European Parliament and of the Council[9] [please insert reference – proposal for a directive on the mechanisms to be~~

---

[5] Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (C(2020) 2800 final).

[6] Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (OJ L 344, 28.12.2001, p. 70).

[7] Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with the ISIL (Da'esh) and Al-Qaida organisations (OJ L 139, 29.5.2002, p. 9).

[8] Council Regulation (EU) No 356/2010 of 26 April 2010 imposing certain specific restrictive measures directed against certain natural or legal persons, entities or bodies, in view of the situation in Somalia (OJ L 105, 27.4.2010, p. 1).

~~[9] 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 purpose 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/EC (see page 73 of this Official Journal).~~

~~put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing~~ Directive (EU) 2015/849] ~~and Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]* contains~~ of the European Parliament and of the Council[10] contains a number of such measures. Those measures do not, however, fully prevent terrorists or other criminals from accessing payment systems for transferring their funds.

(15) The ~~full~~ traceability of transfers of funds and crypto-assets can be a particularly important and valuable tool in the prevention, detection and investigation of money laundering and terrorist financing, as well as in the implementation of restrictive measures, in particular those imposed by Regulations (EC) No 2580/2001, (EC) No 881/2002 and (EU) No 356/2010, in ~~full~~ compliance with Union regulations implementing such measures. It is therefore appropriate, in order to ensure the transmission of information throughout the payment or transfers of crypto-assets chain, to provide for a system imposing the obligation on payment service providers and crypto-asset service providers to accompany transfers of funds and crypto-assets with information on the payer and the payee , and, for transfers of crypto-assets, on the originator and the beneficiary .

(16) This Regulation should apply without prejudice to the restrictive measures imposed by regulations based on Article 215 of the Treaty on the Functioning of the European Union (TFEU), such as Regulations (EC) No 2580/2001, (EC) No 881/2002 and (EU) No 356/2010, which may require that payment service providers of payers and of payees, as well as intermediary payment service providers, take appropriate action to freeze certain funds or that they comply with specific restrictions concerning certain transfers of funds.

(17) ***Processing of personal data under*** this Regulation should ***take place in full compliance with*** to Regulation (EU) 2016/679 of the European Parliament and of the Council[11] ~~national legislation transposing Directive 95/46/EC of the European Parliament and of the Council[12]. For example, personal data collected for the purpose of complying with this Regulation should not be further processed in a way that is incompatible with Directive 95/46/EC. In particular,~~ Ffurther processing of personal data for commercial purposes should be strictly prohibited. The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States. ~~Therefore,~~ Iin applying this Regulation, the transfer of personal data to a third country ~~which does not ensure an adequate level of protection~~ must be carried out in accordance with ~~Article 25 of Directive 95/46/EC~~ Chapter V of Regulation (EU) 2016/679 ~~should be permitted in accordance with Article 26 thereof~~. It is important that payment service providers and crypto-asset service providers operating in multiple jurisdictions with branches or subsidiaries located

---

[10] 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/EC (OJ L 141, 5.6.2015, p. 73).

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[12] ~~Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).~~

outside the Union should not be prevented from transferring data about suspicious transactions within the same organisation, provided that they apply adequate safeguards. In addition, the crypto-asset service providers of the originator and the beneficiary, the payment service providers of the payer and of the payee and the intermediary payment service providers should have in place appropriate technical and organisational measures to protect personal data against accidental loss, alteration, or unauthorised disclosure or access, ***as well as a procedure for the notification of personal data breaches***~~.~~

(18) Persons that merely convert paper documents into electronic data and are acting under a contract with a payment service provider and persons that provide payment service providers solely with messaging or other support systems for transmitting funds or with clearing and settlement systems ~~do~~ should not fall within the scope of this Regulation.

(18a) Natural or legal persons and entities that merely provide ancillary infrastructure allowing another entity to provide services for the transfer of crypto-assets, such as persons that only provide internet services and cloud services or software developers, should not fall within the scope of this Regulation unless they provide services for the transfer of crypto-assets on behalf of another person.

(18aa) This Regulation should not apply to person-to-person transfers of crypto-assets conducted without the use or involvement of a crypto-asset service provider or other obliged entity; or when both the originator and the beneficiary are crypto-asset service providers acting on their own behalf.

(19) Transfers of funds corresponding to services referred to in points (a) to (m) and (o) of Article 3 of Directive (EU) 2015/2366~~2007/64/EC of the European Parliament and of the Council~~[13][14] do not fall within the scope of this Regulation. It is also appropriate to exclude from the scope of this Regulation transfers of funds that represent a low risk of money laundering or terrorist financing. Such exclusions should cover payment cards, electronic money instruments, mobile phones or other digital or information technology (IT) prepaid or postpaid devices with similar characteristics, where they are used exclusively for the purchase of goods or services and the number of the card, instrument or device accompanies all transfers. However, the use of a payment card, an electronic money instrument, a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics in order to effect a person-to-person transfer of funds, falls within the scope of this Regulation. In addition, Automated Teller Machine withdrawals, payments of taxes, fines or other levies, transfers of funds carried out through cheque images exchanges, including truncated cheques, or bills of exchange, and transfers of funds where both the payer and the payee are payment service providers acting on their own behalf should be excluded from the scope of this Regulation.

---

[13] ~~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).~~

[14] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

(19a) Providers of kiosks or automated machines connected to a distributed ledger network, also known as crypto-asset automated teller machines ('crypto-ATMs') enable users to perform transfers of crypto-assets to a crypto-asset address, by depositing cash, often without any form of customer identification and verification. Crypto-ATMs are particularly exposed to money laundering risks because the anonymity provided and the possibility of operating with cash of unknown origin, makes them an ideal vehicle for illicit activities. Given their role in providing or actively facilitating transfers of crypto-assets, transfers of crypto-assets linked to crypto-ATMs should fall under the scope of this Regulation.

(20) In order to reflect the special characteristics of national payment and crypto-asset transfer systems, and provided that it is always possible to trace the transfer of funds back to the payer or the transfer of crypto-assets back to the beneficiary , Member States should be able to exempt from the scope of this Regulation certain domestic low-value transfers of funds, including electronic giro payments, or low-value transfers of crypto-assets, used for the purchase of goods or services. *Due to the inherent borderless nature and global reach of crypto-asset transfers and the provision of services in crypto-assets, a distinction between, on the one hand, purely national transfers and, on the other, cross-border transfers is difficult to make. Furthermore, the speed at which transactions are carried out, and the virtual nature and technological characteristics of crypto-assets facilitate the use of techniques aimed at evading the scope of any rules based on thresholds. In order to reflect those specific features of crypto-assets, an exemption for low-value transfers is therefore not appropriate for transfers of crypto-assets.*

(21) Payment service providers and crypto-asset service providers should ensure that the information on the payer and the payee or the originator and the beneficiary is not missing or incomplete.

(22) In order not to impair the efficiency of payment systems ~~and crypto-asset transfer services~~ ,and in order to balance the risk of driving transactions underground as a result of overly strict identification requirnements against the potential terrorist threat posed by small transfers of funds ~~or crypto-assets~~ , the obligation to check whether information on the payer or the payee ~~, or, for transfers of crypto-assets, the originator and the beneficiary,~~ is accurate should, in the case of transfers of funds where verification has not yet taken place, be imposed only in respect of individual transfers of funds ~~or crypto-assets~~ that exceed EUR 1000, unless the transfer appears to be linked to other transfers of funds ~~or transfers of crypto-assets~~ which together would exceed EUR 1000, the funds ~~or crypto-assets~~ have been received or paid out in cash or in anonymous electronic money, or where there are reasonable grounds for suspecting money laundering or terrorist financing.

(22a) Transfers of crypto-assets are different from transfers of funds in a number of ways. The combination of the inherent borderless nature, the global reach and the technological characteristics of crypto-assets enable users to transfer crypto-assets through thousands of wallets across multiple jurisdictions at a far larger scale and at greater speed than conventional wire transfers. Criminals are able to carry out illicit transfers and avoid detection by structuring a large transaction into smaller amounts using multiple seemingly unrelated wallet addresses, including one time use wallet addresses. Associating those wallet addresses to the real identity of a natural or legal person, or detecting linked transfers for the purpose of applying a de minimis threshold, is more challenging as compared to conventional transfers of funds. Most crypto-assets are also highly volatile and their value can fluctuate

significantly in a very short time frame. This volatility could complicate the implementation and enforcement of a de minimis threshold for authorities as well as for crypto-asset service providers. In order to facilitate the detection of linked transfers and prevent the misuse of crypto-assets to facilitate, fund and hide criminal activities and to launder proceeds, a de minimis threshold should not be set for crypto-asset transfers.

(23) For transfers of funds or for transfers of crypto-assets where verification is deemed to have taken place, payment service providers and crypto-asset service providers should not be required to verify information on the payer or the payee accompanying each transfer of funds, or on the originator and the beneficiary accompanying each transfer of crypto-assets, provided that the obligations laid down in ~~Directive (EU) 2015/849~~ [please insert reference – proposal for a directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849] ~~and Regulation *[please insert reference – proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849]*~~ are met.

(24) In view of the Union legislative acts in respect of payment services, namely Regulation (EC) No 924/2009 of the European Parliament and of the Council[15], Regulation (EU) No 260/2012 of the European Parliament and of the Council[16] and Directive (EU) 2015/2366~~2007/64/EC~~, it should be sufficient to provide that only simplified information accompany transfers of funds within the Union, such as the payment account number(s) or a unique transaction identifier , or for transfers of crypto-assets, in the case of a transfer not made from or to an account, other means ensuring that the transfer of crypto-assets can be individually identified and that the originator and beneficiary address identifiers are recorded on the distributed ledger .

(25) In order to allow the authorities responsible for combating money laundering or terrorist financing in third countries to trace the source of funds or crypto-assets used for those purposes, transfers of funds or transfer of crypto-assets from the Union to outside the Union should carry complete information on the payer and the payee. Complete information on the payer and the payee should include the Legal Entity Identifier (LEI) when this information is provided by the payer to the payer's service provider, ***or, in its absence, any official equivalent identifier available***, since that would allow for better identification of the parties involved in a transfer of funds and could easily be included in existing payment message formats such as the one developed by the International Organisation for Standardisation for electronic data interchange between financial institutions. ~~Those~~ The authorities responsible for combating money laundering or terrorist financing in third countries should be granted access to complete information on the payer and the payee ***as well as on the originator and the beneficiary*** only for the purposes of preventing, detecting and investigating money laundering and terrorist financing.

(25a) Crypto-assets exist in a borderless virtual reality and can be transferred to any crypto-asset service provider in any jurisdiction, or even without a jurisdictional registration. Many non-Union jurisdictions have in place rules relating to data protection and enforcement that are of a different nature than those laid down in

---

15 Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 on cross-border payments in the Community and repealing Regulation (EC) No 2560/2001 (OJ L 266, 9.10.2009, p. 11).

16 Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 (OJ L 94, 30.3.2012, p. 22).

the Union. When transferring crypto-assets on behalf of a customer to a crypto-asset service provider that is not registered in the Union, the crypto-asset service provider of the originator should, in addition to the customer due diligence measures laid down in Article 13 of Directive (EU) 2015/849, assess the ability of the crypto-asset service provider of the beneficiary to receive and retain the information required under this Regulation and to protect the confidentiality of the originator's personal data. Where that information cannot be transmitted with the transfer, a record of the information on the originator and the beneficiary should nevertheless be retained and made available to competent authorities upon request.

(26) The Member State authorities responsible for combating money laundering and terrorist financing, and relevant judicial and law enforcement ~~agencies~~ authorities in the Member States and at Union level , should intensify cooperation with each other and with relevant third country authorities, including those in developing countries, in order further to strengthen transparency and the sharing of information and best practices.

(27) ~~Regarding transfers of crypto-assets, T~~the requirements of this Regulation should apply to crypto-asset service providers whenever their transactions, whether in fiat currency or a crypto-asset, involve a traditional wire transfer or a transfer of crypto-assets ~~involving~~ ***as long as there is at least*** a crypto-asset service provider ***or another obliged entity involved.***

(28) Due to the ~~cross-border~~ ***borderless*** nature and the risks associated with crypto-asset activities and crypto-asset service providers operations, all transfers of crypto-assets should be treated as cross-border wire transfers, with no simplified domestic wire transfers regime.

(29) The crypto-asset service provider of the originator should ensure that transfers of crypto-assets are accompanied by the name of the originator, the originator's account number, where such an account exists and is used to process the transaction, ***the originator's wallet address, the originator's crypto-asset account number, where a transfer of crypto-assets is not registered on a network using distributed ledger technology or similar technology*** and the originator's address, ***country,*** official personal document number, customer identification number or date and place of birth ***and the current LEI of the originator, where provided by the originator to the originator's crypto-asset service provider***. The crypto-asset service provider of the originator should also ensure that transfers of crypto-assets are accompanied by the name of the beneficiary, ~~and~~ the beneficiary's ***wallet address, the beneficiary's*** account number ***where a transfer of crypto-assets is not registered on a network using distributed ledger technology, and the current LEI of the beneficiary*** ~~where such an account exists and is used to process the transaction~~. ***The information shuld be submitted in a secure manner and previously, simultaneosly or currently with the transfer of crypto-assets when a the crypto-asset service provider of the beneficiary is a regulated entity established within the Union; or established in a third country and is able to receive and retain the information with adequate safeguards for ensuring data protection. Where the crypto-asset service provider of the originator knows, suspects or has reasonable grounds to suspect that the crypto-asset service provider of the beneficiary does not apply adequate safeguards for ensuring data protection, the crypto-asset service provider of the originator should proceed with the execution of the transfer without transmitting the information. The information should however be retained and made available to competent authorities upon request.***

(29a) In cases of a transfer of crypto-assets made from or to an unhosted wallet, the provider should collect information from its customer both on the originator and the beneficiary. The crypto-asset service provider should verify the accuracy of information with respect to the originator or beneficiary behind the unhosted wallet, and ensure that the transfer of crypto-assets can be individually identified. For transfers to unhosted crypto-wallets which are already verified and have a known beneficiary, crypto-asset service providers should not be required to verify information of the originator accompanying each transfer of crypto-assets. Such information should be made available to competent authorities upon request in accordance with article 33 of Directive (EU) 2015/849. In order not to impair the efficiency of the crypto-asset transfers from providers to unhosted wallets, providers of crypto-asset transfers should implement effective measures to ensure that the intended transfers are not unduly delayed by verification of the ownership information in relation to unhosted wallets and reporting procedures.

(30) As regards transfers of funds from a single payer to several payees that are to be sent in batch files containing individual transfers from the Union to outside the Union, provision should be made for such individual transfers to carry only the payment account number of the payer or the unique transaction identifier, as well as complete information on the payee, provided that the batch file contains complete information on the payer that is verified for accuracy and complete information on the payee that is fully traceable.

(31) As regards transfers of crypto-assets, the submission of originator and beneficiary information in batches should be accepted, as long as submission occurs immediately and securely. It should not be permitted to submit the required information after the transfer, as submission must occur before or at the moment the transaction is completed, and crypto-asset service providers or other obliged entities should submit the required information simultaneously with the batch crypto-assets transfer itself.

(32) In order to check whether the required information on the payer and the payee accompanies transfers of funds, and to help identify suspicious transactions, the payment service provider of the payee and the intermediary payment service provider should have effective procedures in place ~~in order~~ to detect whether information on the payer and the payee is missing or incomplete. Those procedures should include ~~ex-post~~ monitoring ~~or real-time monitoring~~ after or during the transfers where appropriate. Competent authorities should ensure that payment service providers include the required transaction information with the wire transfer or related message throughout the payment chain.

(33) As regards transfers of crypto-assets, the crypto-asset service provider of the beneficiary should implement effective procedures to detect whether the information on the originator *or the beneficiary* is missing or incomplete *or whether the transfer is supicious*. These procedures should include, where appropriate, monitoring after or during the transfers, in order to detect whether the required information on the originator or the beneficiary is missing *or incomplete or whether the trasnfer is suspicious*. *Before making the crypto-assets available to the beneficiary, the crypto-asset service provider of the beneficiary should verify that the originator of the transfer is not an individual, entity or group subject to targeted restrictive measures or determine if there are any other money laundering or terrorism financing risks. Crypto-asset service providers should rely on suitable tools, including innovative technological solutions, to ensure that the transfer of crypto-assets can be individually identified. Crypto-asset service providers should establish and maintain*

alternative procedures in this respect, including the possibility of not sending personally identifiable information.

(33a) *In the case of a transfer of crypto-assets from an unhosted wallet, the crypto-asset service provider of the beneficiary should collect the information and inform the competent authorities in case any of its customers received a total of over 1 000 EUR from unhosted wallets.*

(34) Given the potential threat of money laundering and terrorist financing presented by anonymous transfers, it is appropriate to require payment service providers to request information on the payer and the payee. In line with the risk-based approach developed by FATF, it is appropriate to identify areas of higher and lower risk, with a view to better targeting the risk of money laundering and terrorist financing. Accordingly, the crypto-asset service provider of the beneficiary, the payment service provider of the payee and the intermediary payment service provider should have effective risk-based procedures that apply where a transfer of funds lacks the required information on the payer or the payee, or where a transfer of crypto-assets lacks the required information on the originator or the beneficiary, in order to allow them to decide whether to execute, reject or suspend that transfer and to determine the appropriate follow-up action to take.

(34a) Providers of crypto-asset transfers should not facilitate any transfer of crypto-assets to or from providers of crypto-assets services that are not established in any jurisdiction or that do not have any central contact point or substantive management presence in any jurisdiction and which are unaffiliated with a regulated entity. Such providers should be deemed as non-compliant providers of crypto-asset services. Once the MiCA Regulation will become applicable, notwithstanding any applicable transitional provisions, providers should not interact with any provider of crypto-asset services which may operate in the Union without valid authorisation.

(34b) Providers of crypto-assets transfers should also refrain from executing or facilitating transfers associated with high risk of money-laundering, terrorist financing and other criminal activities. In order to detect situations of high risk, providers should apply ongoing enhanced due diligence measures with respect to counterparty providers, crypto-asset services and wallet addresses, taking into account a series of specific indicators of potential high risk as well as any information provided by the competent authorities.

(34c) In order to help service providers to comply with such obligations, the EBA should mantain a public register of entities, services and wallets that are associated with high risk of money-laundering, terrorist financing and other criminal activities. Such register should include a non-exhaustive list of non-compliant providers of crypto-asset transfers and other providers associated with high risk as well as a non-exhaustive list of high risk crypto-asset services and wallet addresses. The inclusion of a specific entity, service or address in the public register should not replace the obligation on the provider of crypto-asset transfer to take adequate and effective measures to comply with the prohibition from interacting with those entities, services and wallets. The public register should enable centralised access to information on high risk entities, services and wallets provided by competent

authorities after evaluation. The EBA may also identify high risk entities, services or wallets to be included in the register on its own initiative.

(34d) The use of mixing and tumbling services should only be allowed in circumstances where it can be shown that the use of such services is necessary to overcome legitimate concerns, such as for privacy reasons. The receiver of crypto-assets that have been used in mixing and tumbling services should demonstrate, where necessary, the legitimacy of the practice for which the crypto-asset is used. Where the legitimacy of its use cannot be proven, a transfer of crypto-assets is to be considered high-risk.

(34e) This Regulation should be reviewed and streamlined in the context of the adoption of the [AMLR] in order to ensure full consistency with the relevant provisions and avoid in particular the duplication of due diligence requirements and legal uncertainty.

(35) T~~T~~he payment service provider of the payee, ~~and~~ the intermediary payment service provider and the crypto-asset service provider of the beneficiary should exercise special vigilance, assessing the risks, when either becomes aware that information on the payer or the payee , or the originator or the beneficiary is missing or incomplete, *or where a transfer of crypto-assets is required to be considered suspicious based on the origin or destination of the crypto-assets concerned* and should report suspicious transactions to the competent authorities in accordance with the reporting obligations set out in Regulation~~Directive~~ (EU) [...]~~2015/849~~ ~~and with national measures transposing that Directive~~.

(35a) Similar to transfers of funds between payment service providers, there may be transfers of crypto-assets that involve "intermediary providers of crypto-asset transfers" that facilitate transfers as an intermediate element in a chain of crypto-asset transfers. In line with international standards, such intermediary providers should also be subject to the requirements set out in this Regulation, similarly to the existing obligations a on intermediaries payment service providers. The EBA should issue guidelines to clarify how the relevant obligations imposed on providers of crypto-asset transfers apply to intermediary providers of crypto-asset transfers, in order to ensure that all the required information is transmitted along the chain of a crypto-asset transfer and the information are made available to the competent authorities upon request.

(36) The provisions on transfers of funds and transfers of crypto-assets in relation to which information on the payer or the payee or the originator or the beneficiary is missing or incomplete *and in relation to which transfers of crypto-assets are required to be considered suspicious based on the origin or destination of the involved crypto-assets,* apply without prejudice to any obligations on payment service providers, ~~and~~ intermediary payment service providers and crypto-asset service providers, to suspend and/or reject transfers of funds which breach a provision of civil, administrative or criminal law.

(37) With the aim of assisting payment *service providers and* ~~crypto-asset service~~ providers *of crypto-asset transfers* to put effective procedures in place to detect cases

in which they receive transfers of funds with missing or incomplete payer or payee information ***or transfers of crypto-assets with missing or incomplete originator or beneficiary information or that are suspicious in nature,*** and to take ***effective*** follow-up actions, the ~~European Supervisory Authority (~~European Banking Authority~~)~~ (EBA), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council[17], the ~~European Supervisory Authority (~~European Insurance and Occupational Pensions Authority~~)~~ (EIOPA), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council[18], and the ~~European Supervisory Authority (~~European Securities and Markets Authority~~)~~ (ESMA), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council[19], should issue guidelines. ***The EBA should also issue guidelines specifying technical aspects of the application of this Regulation to direct debits as well as the measures to be taken by payment initiation service providers under this Regulation***.

(38) To enable prompt action to be taken in the fight against money laundering and terrorist financing, payment service providers and crypto-asset service providers should respond promptly to requests for information on the payer and the payee or on the originator and the beneficiary from the authorities responsible for combating money laundering or terrorist financing in the Member State where those payment service providers and crypto-asset service provider are established.

(39) The number of working days in the Member State of the payment service provider of the payer or crypto-asset service provider of the ~~beneficiary~~ ***originator*** determines the number of days to respond to requests for information on the payer or the originator .

(40) As it may not be possible in criminal investigations to identify the data required or the individuals involved in a transaction until many months, or even years, after the original transfer of funds or transfer of crypto-assets , and in order to be able to have access to essential evidence in the context of investigations, it is appropriate to require payment service providers or ~~crypto-asset service providers~~ ***providers of crypto-asset transfers*** to keep records of information on the payer and the payee or the originator and the beneficiary for a period of time for the purposes of preventing, detecting and investigating money laundering and terrorist financing. That period should be limited to five years, after which all personal data should be permanently deleted ~~unless national law provides otherwise~~. ***Where legal proceedings concerned with the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing are pending in a Member State, and a payment service provider holds information or documents relating to those pending proceedings, the payment service provider might retain that information or those documents in accordance with national law for a further period of five years. The storing of personal data beyond the first five years should be consistent with the Law Enforcement Directive.*** ~~If necessary for the purposes of preventing, detecting or investigating money laundering or terrorist financing, and after carrying out an~~

---

17 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).

18 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).

19 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).

~~assessment of the necessity and proportionality of the measure, Member States should be able to allow or require retention of records for a further period of no more than five years, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings.~~

(41) In order to improve compliance with this Regulation, and in accordance with the Commission Communication of 9 December 2010 entitled 'Reinforcing sanctioning regimes in the financial services sector', the power to adopt supervisory measures and the sanctioning powers of competent authorities should be enhanced. Administrative sanctions and measures should be provided for and, given the importance of the fight against money laundering and terrorist financing, Member States should lay down sanctions and measures that are effective, proportionate and dissuasive. Member States should notify the Commission and the Joint Committee of EBA, EIOPA and ESMA (the 'ESAs') thereof.

(42) In order to ensure uniform conditions for the implementation of ~~Chapter VI of~~ this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[20].

(43) A number of countries and territories which do not form part of the territory of the Union share a monetary union with a Member State, form part of the currency area of a Member State or have signed a monetary convention with the Union represented by a Member State, and have payment service providers that participate directly or indirectly in the payment and settlement systems of that Member State. In order to avoid the application of this Regulation to transfers of funds between the Member States concerned and those countries or territories having a significant negative effect on the economies of those countries or territories, it is appropriate to provide for the possibility for such transfers of funds to be treated as transfers of funds within the Member States concerned.

~~Given the number of amendments that would need to be made to Regulation (EC) No 1781/2006 of the European Parliament and of the Council[21] pursuant to this Regulation, that Regulation should be repealed for reasons of clarity.~~

(44) Since the objectives of this Regulation , namely to fight money laundering and the financing of terrorism, including by implementing International Standards, by ensuring the availability of basic information on payers and payees of transfer of funds, and on originators and beneficiaries of transfers of crypto-assets, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(44a) Given the potential high risks associated with unhosted wallets and the technological and regulatory complexity they pose, including in relation to the verification of the ownership information, 12 months after the entry into application of this Regulation, the Commission should assess the need of additional specific measures to mitigate the risks posed by transfers from or to unhosted wallets,

---

20 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

21 ~~Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds (OJ L 345, 8.12.2006, p. 1).~~

including the introduction of possible restrictions, and assess the effectiveness and proportionality of the -mechanisms used to verify the accuracy of the information concerning the ownership of unhosted wallets.

(44b) By 3 years from the date of entry into force of this Regulation, the Commission should submit to the European Parliament and to the Council a report on the application and enforcement of this Regulation accompanied, if appropriate, by a legislative proposal. This assessment should include an assessment of, inter alia, the effectiveness of the measures provided for in this Regulation and the compliance by payment service providers and crypto-asset service providers, the development of technological solutions, the effectiveness and suitability of the de minimis thresholds, the costs and benefits of introducing de minimis thresholds, the effectiveness of international cooperation and information exchange between competent authorities and FIUs, the impact of the measures provided for in this Regulation on data protection and fundamental rights, the application of sanctions, in particular whether they are effective, proportionate and dissuasive, the trends in the use of unhosted wallets and the systematic coherence of this Regulation with the European legislation on anti-Money Laundering and countering terrorist financing.

(44d) Directive (EU) 2015/849 currently only applies to two categories of crypto-asset service providers, namely custodial wallets and crypto-to-fiat exchanges. In order to close the existing loophole in anti-money laundering and terrorist financing framework, Directive (EU) 2015/849 is amended to update the list of obliged entities -~~including~~ with the inclusion of all categories of crypto-assets service providers as defined in Regulation [Regulation on Markets in Crypto-assets] which contemplates a broader scope of crypto-asset service providers.

(45) This Regulation is subject to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 of the European Parliament and of the Council[22]. It respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private and family life (Article 7), the right to the protection of personal data (Article 8), the right to an effective remedy and to a fair trial (Article 47) and the principle of *ne bis in idem*.

~~In order to ensure the smooth introduction of the anti-money laundering and terrorist financing framework, it is appropriate that the date of application of this Regulation be the same as the deadline for transposition of Directive (EU) 2015/849.~~

(46) The European Data Protection Supervisor was consulted in accordance with Article 42(1)~~28(2)~~ of Regulation (EU) 2018/1725~~(EC) No 45/2001 of the European Parliament and of the Council~~[23] and delivered an opinion on […] [24] ~~4 July 2013~~[25],

---

[22] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

[23] ~~Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).~~

[24] [OJ reference of that opinion]

[25] ~~OJ C 32, 4.2.2014, p. 9.~~