3 Commentary to the Rules

Commentary on Section I: Obligations of Reporting Crypto-Asset Service Providers

1. This Section sets out the criteria pursuant to which a Reporting Crypto-Asset Service Provider is subject to the reporting and due diligence requirements in Sections II and III in [Jurisdiction].

2. Paragraph A contains four distinct criteria that link a Reporting Crypto-Asset Service Provider to [Jurisdiction]:

- the Entity or individual is resident for tax purposes in [Jurisdiction];
- the Entity is (a) incorporated or organised under the laws of [Jurisdiction], and (b) either has legal personality in [Jurisdiction] or has an obligation to file tax returns or tax information returns to the tax authorities in [Jurisdiction] with respect to the income of the Entity. As such, this criterion captures situations where an Entity Reporting Crypto-Asset Service Provider selects the law of a certain jurisdiction for purposes of establishing its organisation, including through the act of incorporation. However, in addition to being incorporated or organised under the laws of [Jurisdiction], the Entity must also either have legal personality in [Jurisdiction] or be subject to an obligation to file tax returns or tax information returns to the tax authorities in [Jurisdiction] with respect to its income. This condition is intended to ensure that [Jurisdiction]'s tax administration will be able to enforce the reporting requirements. For the purposes of subparagraph A(2), a tax information return is any filing used to notify the tax administration regarding part or all of the income of the Entity, but which does not necessarily state a pursuant tax liability of the Entity;
- the Entity is managed from [Jurisdiction]. This criterion includes situations where a trust (or a functionally similar Entity) that is a Reporting Crypto-Asset Service Provider is managed by a trustee (or functionally similar representative) that is tax resident in [Jurisdiction]. This criterion captures the place of effective management, as well as any other place of management of the Entity; or
- the Entity or individual has a regular place of business in [Jurisdiction]. In this respect, any Branch is to be considered a regular place of business. This criterion captures the principal, as well as other regular places of business.

3. Paragraph B provides that an Entity also has due diligence and reporting obligations in [Jurisdiction] with respect to Relevant Transactions effectuated through a Branch based in [Jurisdiction].

4. A Reporting Crypto-Asset Service Provider must report the information to each jurisdiction for which it fulfils the criteria of paragraphs A and B, subject to the rules in paragraphs C through H to prevent duplicative reporting. For that purpose, paragraphs C through F introduce a hierarchy among the four criteria in paragraph A that link a Reporting Crypto-Asset Service Provider to [Jurisdiction]. This hierarchy ensures that the due diligence and reporting requirements in [Jurisdiction] do not apply in instances where there is a stronger link with another jurisdiction.

5. As such, paragraph C foresees that an Entity that is a Reporting Crypto-Asset Service Provider which is linked to [Jurisdiction] on the basis of the criteria set out in subparagraphs A(2), (3) or (4) (i.e. it is incorporated, or organised under the laws of [Jurisdiction] and has either legal personality or has an obligation to file tax returns or tax information returns to the tax authorities in [Jurisdiction] with respect to the income of the Entity, or is managed from [Jurisdiction], or it has a regular place of business in [Jurisdiction]), is not required to complete the reporting and due diligence requirements in Sections II and III in [Jurisdiction] if it is tax resident in a Partner Jurisdiction and completes the due diligence and reporting requirements in such Partner Jurisdiction.

6. In addition, paragraph D foresees that an Entity that is a Reporting Crypto-Asset Service Provider is not required to complete the reporting and due diligence requirements in Sections II and III in [Jurisdiction] it is subject to pursuant to subparagraphs A(3) or (4) (i.e. it is managed from [Jurisdiction], or has a regular place of business in [Jurisdiction]), to the extent it has legal personality or has an obligation to file tax returns or tax information returns to the tax authorities in [Jurisdiction] with respect to the income of the Entity and is incorporated, or organised under the laws of such Partner Jurisdiction and completes the due diligence and reporting requirements in such Partner Jurisdiction.

7. Paragraph E foresees that an Entity that is a Reporting Crypto-Asset Service Provider is not required to complete the reporting and due diligence requirements in Sections II and III in [Jurisdiction] it is subject to pursuant to subparagraph A(4) (i.e. its regular place of business is in [Jurisdiction]), to the extent such reporting and due diligence requirements are completed by such Reporting Crypto-Asset Service Provider in a Partner Jurisdiction, by virtue of it being managed from such Partner Jurisdiction.

8. Paragraph F foresees that an individual that is a Reporting Crypto-Asset Service Provider is not required to complete the reporting and due diligence requirements in Sections II and III in [Jurisdiction] it is subject to pursuant to subparagraph A(4) (i.e. its regular place of business is in [Jurisdiction]), to the extent such reporting and due diligence requirements are completed in a Partner Jurisdiction, where the individual Reporting Crypto-Asset Service Provider is resident for tax purposes.

9. Paragraph G foresees that a Reporting Crypto-Asset Service Provider is not subject to the reporting and due diligence requirements in Sections II and III in [Jurisdiction], to the extent these are completed in a Partner Jurisdiction, by virtue of effectuating Relevant Transactions for Crypto-Asset Users through a Branch in such Partner Jurisdiction. A Reporting Crypto-Asset Service Provider that maintains one or more Branches fulfils the due diligence and reporting requirements with respect to a Crypto-Asset User, if any one of its Branches in [Jurisdiction] or a Partner Jurisdiction fulfils such requirements.

10. Finally, paragraph H foresees that a Reporting Crypto-Asset Service Provider is not required to complete the reporting and due diligence requirements in Section II and III in [Jurisdiction] it is subject to pursuant to subparagraphs A(1), (2), (3) or (4), to the extent it has a lodged a notification with [Jurisdiction] in a format specified by [Jurisdiction] confirming that such reporting and due diligence requirements are completed by such Reporting Crypto-Asset Service Provider under the rules of a Partner Jurisdiction pursuant to a substantially similar nexus that it is subject to in [Jurisdiction].

11. Paragraph H only applies to instances where a Reporting Crypto-Asset Service Provider is subject to the same nexus in two or more jurisdictions. For example, a Reporting Crypto-Asset Service Provider that is tax resident in two or more jurisdictions, may rely on paragraph H to select one of the two jurisdictions of tax residence where it complies with the due diligence and reporting requirements. Similarly, a Reporting Crypto-Asset Service Provider that has a regular place of business in two or more jurisdictions may rely on paragraph H to select one of these jurisdictions where it complies with the due diligence and reporting requirements; however, such reliance is not permitted if the Reporting Crypto-Asset Service Provider has nexus in a jurisdiction pursuant to subparagraphs A(1), (2), or (3).

Commentary on Section II: Reporting requirements

1. Section II describes the general reporting requirements applicable to Reporting Crypto-Asset Service Providers. Paragraph A specifies the information to be reported with respect to Crypto-Asset Users and Controlling Persons as a general rule, and subject to the due diligence procedures in Section III, while paragraphs B and C provide for exceptions in connection with TIN and place of birth. Paragraphs D and E contain the valuation and currency translation rules. Paragraph F specifies the requirement to identify the Fiat Currency in which the amount of a Relevant Transaction is reported. Paragraph G specifies the timing of the reporting by the Reporting Crypto-Asset Service Provider.

Paragraph II (A) – Information to be reported

Subparagraph A(1) – Information on Reportable Persons

Jurisdiction(s) of residence

2. The jurisdiction(s) of residence to be reported with respect to a Reportable Person is (are) the jurisdiction(s) of residence identified by the Reporting Crypto-Asset Service Provider pursuant to the due diligence procedures in Section III. In the case of a Reportable Person that is identified as having more than one jurisdiction of residence, the jurisdictions of residence to be reported are all the jurisdictions of residence identified by the Reporting Crypto-Asset Service Provider for the Reportable Person.

Taxpayer Identification Number

3. The TIN to be reported is the TIN assigned to the Reportable Person by its jurisdiction of residence (i.e. not by a jurisdiction of source). In the case of a Reportable Person that is identified as having more than one jurisdiction of residence, the TIN to be reported is the Reportable Person's TIN with respect to each Reportable Jurisdiction. In this respect, the term "TIN" includes a functional equivalent in the absence of a Taxpayer Identification Number.

Subparagraph A(2) – Information on the Reporting Crypto-Asset Service Provider

4. Subparagraph A(2) requires that the Reporting Crypto-Asset Service Provider must report its name, address and identifying number (if any). Identifying information on the Reporting Crypto-Asset Service Provider is intended to allow the identification of the source of the information reported and subsequently exchanged in order to allow the providing jurisdiction to, e.g. follow-up on an error that may have led to incorrect or incomplete information reporting. The "identifying number" of a Reporting Crypto-Asset Service Provider is one of the following types of numbers assigned to a Reporting Crypto-Asset Service Provider for identification purposes: a TIN, or in the absence thereof, a business/company registration code/number, or a Global Legal Entity Identifier (LEI). If no identifying number is assigned to the Reporting Crypto-Asset Service Provider, then only the name and address of the Reporting Crypto-Asset Service Provider are required to be reported.

Subparagraph A(3) – Information on Relevant Transactions

5. Subparagraph A(3) contains the financial reporting requirements applicable to Reporting Crypto-Asset Service Providers, whereby Reporting Crypto-Asset Service Providers must report certain information items with respect to Relevant Transactions effectuated for each relevant calendar year or other appropriate reporting period and in relation to each Reportable User. In this respect, subparagraph A(3) specifies the information to be reported, while paragraphs D and E contain the applicable valuation and currency translation rules.

6. Reflecting the different categories of Relevant Transactions, Reporting Crypto-Asset Service Providers must, for each type of Relevant Crypto-Asset, report on:

- the full name of the type of Relevant Crypto-Asset under subparagraph A(3)(a);
- acquisitions and disposals of Relevant Crypto-Assets against Fiat Currency under subparagraphs A(3)(b) and A(3)(c), respectively;
- acquisitions and disposals of Relevant Crypto-Assets against other Relevant Crypto-Assets, under subparagraphs A(3)(d) and A(3)(e), respectively;
- Reportable Retail Payment Transactions, under subparagraph A(3)(f); and
- other Transfers of Relevant Crypto-Assets to and by the Reportable User, under subparagraphs A(3)(g), A(3)(h) and A(3)(i) respectively.

7. Transfers to and by Reportable Users, reported upon under subparagraphs A(3)(g), A(3)(h) and A(3)(i), include acquisitions and disposals in respect of which the Reporting Crypto-Asset Service Provider has no actual knowledge of the consideration paid or received, as well as Transfers that are not acquisitions or disposals (e.g. a Transfer of Crypto-Assets by a user to its private wallet or to its account with another Reporting Crypto-Asset Service Provider).

8. The applicable valuation rules vary between the reporting categories. In the case of Crypto-Asset-to-Fiat Currency transactions under subparagraphs A(3)(b) and A(3)(c), Reporting Crypto-Asset Service Providers must report the amount paid or received by the Reportable User net of transaction fees. Paragraph D provides that such amounts must be reported in the Fiat Currency in which they were paid or received. However, in case amounts were paid or received in multiple Fiat Currencies, they must be reported in a single currency, converted at the time of each Relevant Transaction in a manner that is consistently applied by the Reporting Crypto-Asset Service Provider.

9. For Crypto-Asset-to-Crypto-Asset transactions under subparagraphs A(3)(d) and A(3)(e), Reportable Retail Payment Transactions under subparagraph A(3)(f), other Transfers under subparagraphs A(3)(g) and A(3)(h), as well as reporting on Transfers to wallets not known by the Reporting Crypto-Asset Service Provider to be associated with virtual asset service providers or financial institutions (as such terms are defined in the Financial Action Task Force Recommendations updated in June 2019 pertaining to virtual asset service providers) under A(3)(i), in light of the absence of (known) consideration, Reporting Crypto-Asset Service Providers must report the fair market value of the Relevant Crypto-Assets acquired and disposed or transferred, net of transaction fees. Paragraph E provides that such amounts must be determined and reported in a Fiat Currency, valued at the time of each Relevant Transaction in a manner that is consistently applied by the Reporting Crypto-Asset Service Provider. For the purposes of paragraphs D and E, a jurisdiction may require reporting in a particular Fiat Currency, for example its local currency.

10. For all reporting categories under subparagraphs A(3)(b) through A(3)(i), the rules require the aggregation, i.e. summing up, of all transactions attributable to each reporting category for each type of Relevant Crypto-Asset, as converted and valued pursuant to paragraphs D and E. For example, if units of a Relevant Crypto-Asset can be mutually substituted for corresponding units of the same Relevant Crypto-Asset, then they should all be treated as the same type of Relevant Crypto-Asset for aggregation purposes. If, however, a Relevant Crypto-Asset is non-fungible, and different variations of the Relevant Crypto-Asset do not have the same value among fixed units, each unit should be treated as a separate type of Relevant Crypto-Asset.

Type of Relevant Crypto-Asset

11. The information under subparagraphs A(3)(b) through A(3)(i) must be reported by type of Relevant Crypto-Asset. For these purposes, the full name of the type of Relevant Crypto-Asset is required to be

reported under subparagraph A(3)(a), rather than a Relevant Crypto-Asset's "ticker" or abbreviated symbol that a Reporting Crypto-Asset Service Provider uses to identify a specific type of Relevant Crypto-Asset.

Crypto-Asset-to-Fiat Currency transactions

12. Subparagraph A(3)(b) requires that, in the case of acquisitions of Relevant Crypto-Assets against Fiat Currency, Reporting Crypto-Asset Service Providers must report the aggregate amount paid net of transaction fees by the Reportable User for each type of Relevant Crypto-Assets acquired by the Reportable User.

13. An acquisition is any transaction effectuated by the Reporting Crypto-Asset Service Provider where the Reportable User obtains a Relevant Crypto-Asset, irrespective of whether such asset is obtained from a third-party seller, or from the Reporting Crypto-Asset Service Provider itself.

14. In the case of disposals of Relevant Crypto-Assets against Fiat Currency, subparagraph A(3)(c) requires that the Reporting Crypto-Asset Service Provider must report the aggregate amount received in Fiat Currency net of transaction fees for any Relevant Crypto-Assets alienated by the Reportable User.

15. A disposal is any transaction effectuated by the Reporting Crypto-Asset Service Provider where the Reportable User alienates a Relevant Crypto-Asset, irrespective of whether such asset is delivered to a third-party purchaser, or to the Reporting Crypto-Asset Service Provider itself.

16. There may be instances where a Reportable User acquires or disposes of a Relevant Crypto-Asset against Fiat Currency, although the Reporting Crypto-Asset Service Provider does not have actual knowledge of the underlying Fiat Currency consideration. This would, for example, be the case if the Reporting Crypto-Asset Service Provider only conducted the Transfer of the Relevant Crypto-Assets to and from the Reportable User, without actual knowledge of the Fiat Currency leg of the transaction. Such transactions should be reported upon as Transfers sent to or by a Reportable User under subparagraphs A(3)(g) and A(3)(h), respectively.

Crypto-Asset-to-Crypto-Asset transactions

17. A Crypto-Asset-to-Crypto-Asset transaction that is effectuated by a Reporting Crypto-Asset Service Provider will give rise to reporting under both subparagraphs A(3)(d) and A(3)(e). In this respect, subparagraph A(3)(d) provides that in the case of acquisitions against other Relevant Crypto-Assets, the Reporting Crypto-Asset Service Provider must report the fair market value of the Relevant Crypto-Assets acquired net of transaction fees. Similarly, subparagraph A(3)(e) requires that in the case of disposals against other Relevant Crypto-Assets, the Reporting Crypto-Asset Service Provider must report the fair market value of the Relevant Crypto-Assets disposed net of transaction fees.

18. By way of an example, in respect of an exchange of Relevant Crypto-Asset A for Relevant Crypto-Asset B, the Reporting Crypto-Asset Service Provider must report both the fair market value of Relevant Crypto-Asset A, i.e. the Relevant Crypto-Asset disposed, under subparagraph A(3)(e) and the fair market value of Relevant Crypto-Asset B, i.e. the Relevant Crypto-Asset acquired, under subparagraph A(3)(d), valued at the time of the Relevant Transaction and both net of transaction fees.

19. All Crypto-Asset-to-Crypto-Asset transactions conducted by the same Reporting Crypto-Asset Service Provider are subject to reporting under both subparagraphs A(3)(d) and A(3)(e). As for Crypto-Asset-to-Fiat Currency transactions, there may be instances where a Reportable User effectuates a Crypto-Asset-to-Crypto-Asset transaction, although the Reporting Crypto-Asset Service Provider does not have actual knowledge of the Relevant Crypto-Asset acquired or disposed. This would, for example, be the case when the Reporting Crypto-Asset Service Provider only effectuates the Transfer of either the Relevant Crypto-Assets disposed or acquired, without actual knowledge of the other leg of the transaction. Depending on which leg of the transaction the Reporting Crypto-Asset Service Provider has actual

knowledge of, such transactions should be reported upon as Transfers sent to or by a Reportable User under subparagraphs A(3)(g) and A(3)(h), respectively.

20. **Example**: A Reportable User acquires Relevant Crypto-Asset D in exchange for Relevant Crypto-Asset C. The Reporting Crypto-Asset Service Provider effectuates the Transfer of Relevant Crypto-Asset C to the wallet of the seller of Relevant Crypto-Asset D. In exchange, the seller of Relevant Crypto-Asset D transfers Relevant Crypto-Asset D directly to a cold wallet controlled by the Reportable User. Unless the Reporting Crypto-Asset Service Provider has actual knowledge of the consideration, i.e. the Relevant Crypto-Asset D Transfer, it should report the transaction as a Transfer by a Reportable User of Relevant Crypto-Asset C under subparagraph A(3)(h).

Reportable Retail Payment Transactions

21. Pursuant to subparagraph A(3)(f), aggregate information on Transfers that constitute Reportable Retail Payment Transactions is required to be reported as a separate category of Relevant Transactions. With respect to such Reportable Retail Payments Transactions, the customer of the merchant for, or on behalf of, whom the Reporting Crypto-Asset Service Provider is providing a service effectuating Reportable Retail Payment Transactions must be treated as the Crypto-Asset User (subject to the conditions specified in the definition of Crypto-Asset User), and therefore as the Reportable User, in addition to the merchant. Aggregate information with respect to Reportable Retail Payment Transactions by the customer of the merchant must not be included in the aggregate information reported with respect to Transfers under subparagraph A(3)(h). Aggregate information with respect to Transfers that do not constitute Reportable Retail Payment Transactions solely by virtue of not meeting the de minimis threshold, should be included in the aggregate information reported with respect to Transfers under A(3)(g) and (h). The following examples illustrate the application of subparagraphs A(3)(f) and A(3)(g).

22. **Example 1**: (Reportable Retail Payment Transaction): To facilitate the use of Crypto-Assets by customers to purchase goods, a merchant has entered into an agreement with a Reporting Crypto-Asset Service Provider to process payments to the merchant made in Crypto-Assets by the merchant's customers. The Reporting Crypto-Asset Service Provider does not maintain a separate relationship with the merchant's customers.

The customer makes a payment in Relevant Crypto-Assets for goods acquired from the merchant for a value exceeding USD 50,000. This transaction is a Reportable Retail Payment Transaction. The Reporting Crypto-Asset Service Provider should treat the customer of the merchant as the Crypto-Asset User, and report the payment in Relevant Crypto-Assets as specified under subparagraph A(3)(f) (Reportable Retail Payment Transactions), provided that the Reporting Crypto-Asset Service Provider is required to verify the identity of such customer pursuant to domestic anti-money laundering rules, by virtue of the Reportable Retail Payment Transaction. The Reporting Crypto-Asset Service Provider should also treat the merchant as the Crypto-Asset User of this transaction, and the transaction is reportable as a Transfer to the merchant under subparagraph A(3)(g).

23. **Example 2**: (transaction that is not a Reportable Retail Payment Transaction by virtue of de minimis threshold): The customer engages in another transaction with the merchant that is identical to the transaction described in Example 1, except that the transaction amount is less than USD 50,000. The transaction is not a Reportable Retail Payment Transaction. The Reporting Crypto-Asset Service Provider should therefore treat the merchant as the Crypto-Asset User of this transaction, and the transaction is reportable as a Transfer to the merchant under subparagraph A(3)(g).

Transfers other than Reportable Retail Payment Transactions

24. Subparagraphs A(3)(g) and A(3)(h) require that Reporting Crypto-Asset Service Providers must report the fair market value of other Transfers sent to, and by, a Reportable User, respectively.

Furthermore, the Reporting Crypto-Asset Service Provider should subdivide the aggregate fair market value, aggregate number of units and number of Transfers effectuated on behalf of a Reportable User, during the reporting period, per underlying transfer type, where such transfer type is known by the Reporting Crypto-Asset Service Provider. For instance, where a Reporting Crypto-Asset Service Provider is aware that Transfers effectuated on behalf of a Reportable User are due to an airdrop (resulting from a hard-fork), an airdrop (for reasons other than a hard-fork), income derived from staking, the disbursement, reimbursement or associated return on a loan, or an exchange for goods or services, it should indicate the aggregate fair market value, aggregate number of units and number of Transfers effectuated for each transfer type.

Transfers to external wallet addresses

25. Subparagraph A(3)(i) requires the Reporting Crypto-Asset Service Provider to report, by type of Relevant Crypto-Asset, the aggregate number of units, as well as the aggregate fair market value, in Fiat Currency, of Transfers it effectuates on behalf of a Reportable User to any wallet addresses (including other equivalent identifiers used to describe the destination of a Transfer) not known to be associated with a virtual asset service provider or financial institution, as defined in the FATF Recommendations. The Reporting Crypto-Asset Service Provider is not required to report the aggregate number of units or the aggregate fair market value of Transfers, under subparagraph A(3)(i), in case the Reporting Crypto-Asset Service Provider knows that the wallet address to which the Relevant Crypto-Asset is transferred is associated with a virtual asset service provider or financial institution, as defined in the FATF Recommendations.

26. This rule does not require the reporting of wallet addresses associated with Transfers of Relevant Crypto-Assets. However, pursuant to subparagraph D(3) of Section III and to ensure that necessary information is available to tax administrations in the context of follow up requests, a Reporting Crypto-Asset Service Provider is required to collect and retain within its records, for a period not less than five years, any external wallet addresses (including other equivalent identifiers) associated with Transfers of Relevant Crypto-Assets that are subject to reporting under subparagraph A(3)(i).

Appropriate reporting period

27. The information to be reported under paragraphs A(1) through A(3) must be that in respect of the end of the relevant calendar year or other appropriate reporting period. In determining what is meant by "appropriate reporting period", reference must be made to the meaning that the term has at that time under each jurisdiction's reporting rules.

Paragraphs II (B) and (C) – Exceptions

Taxpayer Identification Number

28. Paragraph B contains an exception pursuant to which a TIN is not required to be reported if either:

- a TIN is not issued by the relevant Reportable Jurisdiction; or
- the domestic law of the relevant Reportable Jurisdiction does not require the collection of the TIN issued by such Reportable Jurisdiction.

29. A TIN is considered not to be issued by a Reportable Jurisdiction (i) where the jurisdiction does not issue a TIN nor a functional equivalent in the absence of a TIN, or (ii) where the jurisdiction has not issued a TIN to a particular individual or Entity. As a consequence, a TIN is not required to be reported with respect to a Reportable Person that is resident in such a Reportable Jurisdiction, or with respect to whom a TIN has not been issued. However, if and when a Reportable Jurisdiction starts issuing TINs and issues a TIN to a particular Reportable Person, the exception contained in paragraph B no longer applies

and the Reportable Person's TIN would be required to be reported if the Reporting Crypto-Asset Service Provider obtains a self-certification that contains such TIN, or otherwise obtains such TIN.

30. The exception described in clause (ii) of paragraph B focuses on the domestic law of the Reportable Person's jurisdiction. Where a Reportable Jurisdiction has issued a TIN to a Reportable Person and the collection of such TIN cannot be required under such jurisdiction's domestic law (e.g. because under such law the provision of the TIN by a taxpayer is on a voluntary basis), the Reporting Crypto-Asset Service Provider is not required to obtain and report the TIN. However, the Reporting Crypto-Asset Service Provider is not prevented from asking for, and collecting the Reportable Person's TIN for reporting purposes if the Reportable Person chooses to provide it. In this case, the Reporting Crypto-Asset Service Provider must report the TIN. In practice, there may be only a few jurisdictions where this is the case (e.g. Australia).

31. Jurisdictions are expected to provide Reporting Crypto-Asset Service Providers with information with respect to the issuance, collection and, to the extent possible and practical, structure and other specifications of taxpayer identification numbers. The OECD will endeavour to facilitate its dissemination.

Place of birth

32. Paragraph C contains an exception with respect to place of birth information, which is not required to be reported, unless the Reporting Crypto-Asset Service Provider is otherwise required to obtain and report it under domestic law and it is available in the electronically searchable data maintained by the Reporting Crypto-Asset Service Provider. Thus, the place of birth is required to be reported if, with respect to the Reportable Person, both:

- the Reporting Crypto-Asset Service Provider is otherwise required to obtain the place of birth and report it under domestic law; and
- the place of birth is available in the electronically searchable information maintained by the Reporting Crypto-Asset Service Provider.

Paragraphs II (D), (E) and (F) – Valuation and currency

Valuation and currency translation rules for Crypto-Asset-to-Fiat Currency transactions

33. Paragraph D provides that, for the purposes of subparagraph A(3)(b) and A(3)(c), the amounts must be reported in the Fiat Currency in which they were paid. However, in case amounts were paid or received in multiple Fiat Currencies, they must be reported in a single Fiat Currency, converted at the time of each Relevant Transaction in a manner that is consistently applied by the Reporting Crypto-Asset Service Provider. For example, the Reporting Crypto-Asset Service Provider may apply the spot rate(s) as at the time of the transaction(s) to translate such amounts into a single Fiat Currency determined by the Reporting Crypto-Asset Service Provider. The information reported must also identify the Fiat Currency in which each amount is reported.

34. Further, for the purposes of reporting under subparagraphs A(3)(b) and A(3)(c), the Reporting Crypto-Asset Service Provider must aggregate, i.e. sum up, all transactions attributable to each reporting category for each type of Relevant Crypto-Asset, as converted pursuant to paragraph D.

Valuation and currency translation rules for Crypto-Asset-to-Crypto-Asset transactions

35. For the purposes of subparagraphs A(3)(d) and A(3)(e), the fair market value must be determined and reported in a single currency, valued at the time of each Relevant Transaction in a reasonable manner that is consistently applied by the Reporting Crypto-Asset Service Provider. In this respect, a Reporting Crypto-Asset Service Provider may rely on applicable Crypto-Asset-to-Fiat Currency trading pairs that it

maintains to determine the fair market value of both Relevant Crypto-Assets. For instance, in respect of a disposal of Relevant Crypto-Asset A against Relevant Crypto-Asset B, the Reporting Crypto-Asset Service Provider may, at the time the transaction is executed: (i) perform an implicit conversion of Relevant Crypto-Asset A to Fiat Currency to determine the fair market value of the disposed Relevant Crypto-Asset A for the purposes of reporting under subparagraph A(3)(e); and (ii) perform an implicit conversion of the acquired Relevant Crypto-Asset B to Fiat Currency to determine the fair market value of the acquired Relevant Crypto-Asset B for the purposes of reporting under subparagraph A(3)(d).

36. It may arise that a difficult-to-value Relevant Crypto-Asset is exchanged for a Relevant Crypto-Asset that can be readily valued. In such cases, the valuation in Fiat Currency of the Relevant Crypto-Asset against which the difficult-to-value Relevant Crypto-Asset is exchanged should be relied upon to establish a Fiat Currency value for the difficult-to-value Relevant Crypto-Asset, as illustrated by the below example:

- **Example**: a Crypto-Asset User makes use of a Reporting Crypto-Asset Service Provider to dispose of Relevant Crypto-Asset A against the acquisition of Relevant Crypto-Asset B. Relevant Crypto-Asset A has a readily obtainable Fiat Currency equivalent value and the Reporting Crypto-Asset Service Provider can perform an implicit conversion to determine the fair market value of the disposal of Relevant Crypto-Asset A. However, Relevant Crypto-Asset B is a recently launched Crypto-Asset and the Reporting Crypto-Asset Service Provider is not able to determine an equivalent fair market value as there is no available Fiat Currency conversion amount. In this case, to determine the acquisition value attributable to the Crypto-Asset User's acquisition of Crypto-Asset B, the Reporting Crypto-Asset Service Provider can perform an implicit conversion of Relevant Crypto-Asset B by attributing to it the same Fiat Currency amount attributed to Relevant Crypto-Asset A.

37. Further, for the purposes of reporting under subparagraphs A(3)(d) and A(3)(e), the Reporting Crypto-Asset Service Provider must aggregate, i.e. sum up, all transactions attributable to each reporting category, as converted pursuant to paragraph D.

Valuation and currency translation rules for Reportable Retail Payment Transactions and other Transfers

38. For the purposes of subparagraphs A(3)(f), A(3)(g), A(3)(h) and A(3)(i), the fair market value must be determined and reported in a single currency, using a reasonable valuation method that looks to contemporaneous evidence of value at the time of each Relevant Transaction in a manner that is consistently applied by the Reporting Crypto-Asset Service Provider. In performing such valuation, the Reporting Crypto-Asset Service Provider may use as a reference the values of Relevant Crypto-Asset and Fiat Currency trading pairs it maintains to determine the fair market value of the Relevant Crypto-Asset at the time it is transferred. The information reported must also identify the Fiat Currency in which each amount is reported. The following example illustrates this approach:

- **Example**: A Reporting Crypto-Asset Service Provider maintains a trading platform and also facilitates Transfers of Relevant Crypto-Assets. The Reporting Crypto-Asset Service Provider effectuates a Transfer of Relevant Crypto-Asset A for Crypto-Asset User A. Relevant Crypto-Asset A is also regularly traded for Fiat Currency on Reporting Crypto-Asset Service Provider's trading platform. The Reporting Crypto-Asset Service Provider A may rely on such trading data to determine the fair market value of Relevant Crypto-Asset A at the time of the Transfer.

39. Where the Reporting Crypto-Asset Service Provider effectuating the Transfer does not maintain an applicable reference value of the Relevant Crypto-Asset and Fiat Currency trading pairs, the following valuation methods must be relied upon:

- firstly, the internal accounting book values the Reporting Crypto-Asset Service Provider maintains with respect to the Relevant Crypto-Asset must be used;
- if a book value is not available, a value provided by third-party companies or websites that aggregate current prices of Relevant Crypto-Assets must be used, if the valuation method used by that third party is reasonably expected to provide a reliable indicator of value;
- if neither of the above is available, the most recent valuation of the Relevant Crypto-Asset by the Reporting Crypto-Asset Service Provider must be used; and
- if a value can still not be attributed, a reasonable estimate may be applied as a measure of last resort.

40. With respect to each Relevant Crypto-Asset for which the Reporting Crypto-Asset Service Provider has relied on an alternative valuation method outlined in paragraph 39, the method must be indicated via the appropriate element in the relevant XML Schema.

41. Further, for the purposes of reporting under subparagraphs A(3)(f), A(3)(g) A(3)(h) and A(3)(i), the Reporting Crypto-Asset Service Provider must aggregate, i.e. sum up, all transactions attributable to each reporting category for each type of Relevant Crypto-Asset, as converted pursuant to paragraph D.

Paragraph II (G) – Timing of reporting

42. Paragraph G provides the time by which the information pursuant to paragraph A needs to be reported. While the selection of the date by which information is to be reported by the Reporting Crypto-Asset Service Provider is a decision of the jurisdiction implementing the rules, it is expected that such date will allow the jurisdiction to exchange the information within the timelines specified in the competent authority agreement.

Commentary on Section III: Due diligence procedures

1. Section III contains the due diligence procedures for identifying Reportable Persons. These requirements are split into four paragraphs:

- paragraph A sets out the procedures for Individual Crypto-Asset Users;
- paragraph B sets out the procedures for Entity Crypto-Asset Users;
- paragraph C specifies the validity requirements for self-certifications of Individual Crypto-Asset Users, Controlling Persons and Entity Crypto-Asset Users; and
- paragraph D specifies the general due diligence requirements.

Paragraph A – Due diligence procedures for Individual Crypto-Asset Users

2. Paragraph A sets out that a Reporting Crypto-Asset Service Provider must collect a self-certification, and confirm its reasonableness, in respect of its Individual Crypto-Asset Users.

3. Subparagraph A(1) specifies that, upon the establishment of a relationship with the user, which may include a one-off transaction, a Reporting Crypto-Asset Service Provider must:

- obtain a self-certification that allows the Reporting Crypto-Asset Service Provider to determine the Individual Crypto-Asset User's residence(s) for tax purposes; and
- confirm the reasonableness of such self-certification based on the information obtained by the Reporting Crypto-Asset Service Provider in connection with the establishment of a relationship with the user. Such information includes information the Reporting Crypto-Asset Service Provider collected for AML/KYC Procedures.

4. With respect to Preexisting Individual Crypto-Asset Users, subparagraph A(1) clarifies that Reporting Crypto-Asset Service Providers must obtain a valid self-certification and confirm its reasonableness at the latest 12 months after the jurisdiction introduces the rules.

Obtaining a self-certification

5. The self-certification obtained under subparagraph A(1) must allow the determination of the Individual Crypto-Asset User's residence(s) for tax purposes. See Commentary on subparagraph C(1) of Section III for further details on the required contents of self-certifications for Individual Crypto-Asset Users. The domestic laws of the various jurisdictions lay down the conditions under which an individual is to be treated as fiscally "resident". They cover various forms of attachment to a jurisdiction which, in the domestic taxation laws, form the basis of a comprehensive taxation (full liability to tax). They also cover cases where an individual is deemed, according to the taxation laws of a jurisdiction, to be resident of that jurisdiction (e.g. diplomats or other persons in government service). Generally, an individual will only have one jurisdiction of residence. However, an individual may be resident for tax purposes in two or more jurisdictions. In those circumstances, the expectation is that all jurisdictions of residence are to be declared in a self-certification and that the Reporting Crypto-Asset Service Provider must treat the Individual Crypto-Asset User as a Reportable User in respect of each Reportable Jurisdiction.

6. Reportable Jurisdictions are expected to help taxpayers determine, and provide them with information with respect to, their residence(s) for tax purposes. That may be done, for example, through the various service channels used for providing information or guidance to taxpayers on the application of tax laws. The OECD will endeavour to facilitate the dissemination of such information.

Reasonableness of self-certifications

7. Subparagraph A(1) specifies that the Reporting Crypto-Asset Service Provider must confirm the reasonableness of the self-certification.

8. A Reporting Crypto-Asset Service Provider is considered to have confirmed the "reasonableness" of a self-certification if, in the course of establishing a relationship with an Individual Crypto-Asset User and upon review of the information obtained in connection with the establishment of the relationship (including any documentation collected pursuant to AML/KYC Procedures), it does not know or have reason to know that the self-certification is incorrect or unreliable. Reporting Crypto-Asset Service Providers are not expected to carry out an independent legal analysis of relevant tax laws to confirm the reasonableness of a self-certification.

9. The following examples illustrate the application of the "reasonableness" test:

- **Example 1**: A Reporting Crypto-Asset Service Provider obtains a self-certification from the Individual Crypto-Asset User upon the establishment of the relationship. The jurisdiction of the residence address contained in the self-certification conflicts with that contained in the documentation collected pursuant to AML/KYC Procedures. Because of the conflicting information, the self-certification is incorrect or unreliable and, as a consequence, it fails the reasonableness test.
- **Example 2**: A Reporting Crypto-Asset Service Provider obtains a self-certification from the Individual Crypto-Asset User upon the establishment of the relationship. The residence address contained in the self-certification is not in the jurisdiction in which the Individual Crypto-Asset User claims to be resident for tax purposes. Because of the conflicting information, the self-certification fails the reasonableness test.

10. In the case of a self-certification that fails the reasonableness test, it is expected that the Reporting Crypto-Asset Service Provider would obtain either (i) a valid self-certification, or (ii) a reasonable explanation and documentation (as appropriate) supporting the reasonableness of the self-certification

(and retain a copy or a notation of such explanation and documentation) before providing services effectuating Relevant Transactions to the Individual Crypto-Asset User. Examples of such "reasonable explanation" include a statement by the individual that he or she (1) is a student at an educational institution in the relevant jurisdiction and holds the appropriate visa (if applicable); (2) is a teacher, trainee, or intern at an educational institution in the relevant jurisdiction or a participant in an educational or cultural exchange visitor program, and holds the appropriate visa (if applicable); (3) is a foreign individual assigned to a diplomatic post or a position in a consulate or embassy in the relevant jurisdiction; or (4) is a frontier worker or employee working on a truck or train travelling between jurisdictions. The following example illustrates the application of this paragraph: A Reporting Crypto-Asset Service Provider obtains a self-certification for the Individual Crypto-Asset User upon the establishment of the relationship. The jurisdiction of residence for tax purposes contained in the self-certification conflicts with the residence address contained in the documentation collected pursuant to AML/KYC Procedures. The Individual Crypto-Asset User explains that she is a diplomat from a particular jurisdiction and that, as a consequence, she is resident in such jurisdiction; she also presents her diplomatic passport. Because the Reporting Crypto-Asset Service Provider obtained a reasonable explanation and documentation supporting the reasonableness of the self-certification, the self-certification passes the reasonableness test.

Reliance on self-certifications

11. Subparagraph A(2) specifies that if, at any point, there is a change of circumstances with respect to an Individual Crypto-Asset User that causes the Reporting Crypto-Asset Service Provider to know, or have reason to know, that the original self-certification is incorrect or unreliable, the Reporting Crypto-Asset Service Provider cannot rely on the original self-certification and must obtain a valid self-certification, or a reasonable explanation and documentation (as appropriate) supporting the validity of the original self-certification.

Standards of knowledge applicable to self-certifications

12. A Reporting Crypto-Asset Service Provider has reason to know that a self-certification is unreliable or incorrect if its knowledge of relevant facts or statements contained in the self-certification or other documentation is such that a reasonably prudent person in the position of the Reporting Crypto-Asset Service Provider would question the claim being made. A Reporting Crypto-Asset Service Provider also has reason to know that a self-certification or is unreliable or incorrect if there is information in the documentation or in the Reporting Crypto-Asset Service Provider's files that conflicts with the person's claim regarding its status.

13. A Reporting Crypto-Asset Service Provider has reason to know that a self-certification provided by a person is unreliable or incorrect if the self-certification is incomplete with respect to any item on the self-certification that is relevant to the claims made by the person, the self-certification contains any information that is inconsistent with the person's claim, or the Reporting Crypto-Asset Service Provider has other information that is inconsistent with the person's claim. A Reporting Crypto-Asset Service Provider that relies on a service provider to review and maintain a self-certification is considered to know or have reason to know the facts within the knowledge of the service provider.

14. A Reporting Crypto-Asset Service Provider may not rely on documentation provided by a person if the documentation does not reasonably establish the identity of the person presenting the documentation. For example, documentation is not reliable if it is provided in person by an individual and the photograph or signature on the documentation does not match the appearance or signature of the person presenting the document. A Reporting Crypto-Asset Service Provider may not rely on documentation if the documentation contains information that is inconsistent with the person's claim as to its status, the Reporting Crypto-Asset Service Provider has other information that is inconsistent with the person's status, or the documentation lacks information necessary to establish the person's status.

Change of circumstances

15. A "change of circumstances" includes any change that results in the addition of information relevant to an Individual Crypto-Asset User's status or otherwise conflicts with such user's status or any change or addition of information to any profile associated with such Individual Crypto-Asset User if such change or addition of information affects the status of the Individual Crypto-Asset User. For these purposes, the Reporting Crypto-Asset Service Provider should determine whether new information that is obtained with respect to the Individual Crypto-Asset User's profile in accordance with re-documentation undertaken in accordance with AML/KYC Procedures or other regulatory obligations includes new information that constitutes a change of circumstances. A change of circumstances affecting the self-certification provided to the Reporting Crypto-Asset Service Provider will terminate the validity of the self-certification with respect to the information that is no longer reliable, until the information is updated.

16. When a change of circumstances occurs, according to subparagraph A(2), the Reporting Crypto-Asset Service Provider cannot rely on the original self-certification and must obtain either (i) a valid self-certification that establishes the residence(s) for tax purposes of the Individual Crypto-Asset User, or (ii) a reasonable explanation and documentation (as appropriate) supporting the validity of the original self-certification (and retain a copy or a notation of such explanation and documentation). Therefore, a Reporting Crypto-Asset Service Provider is expected to institute procedures to ensure that any change that constitutes a change in circumstances is identified by the Reporting Crypto-Asset Service Provider. In addition, a Reporting Crypto-Asset Service Provider is expected to notify any person providing a self-certification of the person's obligation to notify the Reporting Crypto-Asset Service Provider of a change in circumstances.

17. A self-certification becomes invalid on the date that the Reporting Crypto-Asset Service Provider holding the self-certification knows or has reason to know that circumstances affecting the correctness of the self-certification have changed. However, a Reporting Crypto-Asset Service Provider may choose to treat a person as having the same status that it had prior to the change in circumstances until the earlier of 90 calendar days from the date that the self-certification became invalid due to the change in circumstances, the date that the validity of the self-certification is confirmed, or the date that a new self-certification is obtained. If the Reporting Crypto-Asset Service Provider cannot obtain a confirmation of the validity of the original self-certification or a valid self-certification during such 90-day period, the Reporting Crypto-Asset Service Provider must treat the Individual Crypto-Asset User as resident of the jurisdiction(s) in which the Individual Crypto-Asset User claimed to be resident in the original self-certification and the jurisdiction(s) in which the Individual Crypto-Asset User may be resident as a result of the change in circumstances. A Reporting Crypto-Asset Service Provider may rely on a self-certification without having to inquire into possible changes of circumstances that may affect the validity of the statement, unless it knows or has reason to know that circumstances have changed. For instance, where the Reporting Crypto-Asset Service Provider obtains information pursuant to its AML/KYC Procedures or other regulatory requirements that information contained in the self-certification is no longer accurate or reliable, the Reporting Crypto-Asset Service Provider must update the self-certification with respect to the information identified, before the self-certification can be relied on.

18. A Reporting Crypto-Asset Service Provider may retain an original, certified copy, or photocopy (including a microfiche, electronic scan, or similar means of electronic storage) or electronic copy of the self-certification. The self-certification (including the original) may also exist solely in electronic format.

Curing self-certification errors

19. A Reporting Crypto-Asset Service Provider may treat a self-certification as valid, notwithstanding that the self-certification contains an inconsequential error, if the Reporting Crypto-Asset Service Provider has sufficient documentation on file to supplement the information missing from the self-certification due to the error. In such case, the documentation relied upon to cure the inconsequential error must be

conclusive. For example, a self-certification in which the Individual Crypto-Asset User submitting the form abbreviated the jurisdiction of residence may be treated as valid, notwithstanding the abbreviation, if the Reporting Crypto-Asset Service Provider has government issued identification for the person from a jurisdiction that reasonably matches the abbreviation. On the other hand, an abbreviation for the jurisdiction of residence that does not reasonably match the jurisdiction of residence shown on the person's passport is not an inconsequential error. A failure to provide a jurisdiction of residence is not an inconsequential error. In addition, information on a self-certification that contradicts other information contained on the self-certification or in the files of the Reporting Crypto-Asset Service Provider is not an inconsequential error.

Paragraph B – Due diligence procedures for Entity Crypto-Asset Users

20. Paragraph B contains the due diligence procedures for Entity Crypto-Asset Users. Such procedures require Reporting Crypto-Asset Service Providers to determine:

- whether the Entity Crypto-Asset User is a Reportable User; and
- whether an Entity Crypto-Asset User has one or more Controlling Persons who are Reportable Persons, unless the Entity Crypto-Asset User is an Excluded Person or an Active Entity.

21. With respect to Preexisting Entity Crypto-Asset Users, subparagraph B(1)(a) clarifies that Reporting Crypto-Asset Service Providers must obtain a valid self-certification and confirm its reasonableness at the latest 12 months after the jurisdiction introduces these rules.

Review procedure for Entity Crypto-Asset Users

22. Subparagraph B(1) contains the review procedure to determine whether an Entity Crypto-Asset User is a Reportable User. In order to determine whether an Entity Crypto-Asset User is a Reportable User, subparagraph B(1)(a) requires that, when establishing a relationship with the Entity Crypto-Asset User, or with respect to Preexisting Entity Crypto-Assets Users by 12 months after the introduction of the rules, the Reporting Crypto-Asset Service Provider:

- obtains a self-certification that allows the Reporting Crypto-Asset Service Provider to determine the Entity Crypto-Asset User's residence(s) for tax purposes; and
- confirms the reasonableness of such self-certification based on the information obtained by the Reporting Crypto-Asset Service Provider in connection with the establishment of the relationship with the Entity Crypto-Asset User, including any documentation collected pursuant to AML/KYC Procedures. If the Entity Crypto-Asset User certifies that it has no residence for tax purposes, the Reporting Crypto-Asset Service Provider may rely on the place of effective management or the address of the principal office to determine the residence of the Entity Crypto-Asset User.

23. If the self-certification indicates that the Entity Crypto-Asset User is resident in a Reportable Jurisdiction, then, as provided in subparagraph B(1)(b), the Reporting Crypto-Asset Service Provider must treat the Entity Crypto-Asset User as a Reportable User unless it reasonably determines based on the self-certification or information in its possession or that is publicly available, that the Entity Crypto-Asset User is an Excluded Person. Such information includes information that was obtained for the purpose of completing the due diligence procedures pursuant to the Common Reporting Standard.

24. "Publicly available" information includes information published by an authorised government body (for example, a government or an agency thereof, or a municipality) of a jurisdiction, such as information in a list published by a tax administration; information in a publicly accessible register maintained or authorised by an authorised government body of a jurisdiction; or information disclosed on an established

securities market. In this respect, the Reporting Crypto-Asset Service Provider is expected to retain a notation of the type of information reviewed, and the date the information was reviewed.

25. In determining whether an Entity Crypto-Asset User is a Reportable User, the Reporting Crypto-Asset Service Provider may follow the guidance on subparagraphs B(1)(a) and (b) in the order most appropriate under the circumstances. That would allow a Reporting Crypto-Asset Service Provider, for example, to determine under subparagraph B(1)(b) that an Entity Crypto-Asset User is an Excluded Person and, thus, is not a Reportable User.

26. The self-certification must allow the determination of the Entity Crypto-Asset User's residence(s) for tax purposes. The domestic laws of the various jurisdictions lay down the conditions under which an Entity is to be treated as fiscally "resident". They cover various forms of attachment to a jurisdiction which, in the domestic taxation laws, form the basis of a comprehensive taxation (full tax liability). Generally, an Entity will be resident for tax purposes in a jurisdiction if, under the laws of that jurisdiction, it pays or should be paying tax therein by reason of its place of management or incorporation, or any other criterion of a similar nature, and not only from sources in that jurisdiction. If an Entity is subject to tax as a resident in more than one jurisdiction, all jurisdictions of residence are to be declared in a self-certification and the Reporting Crypto-Asset Service Provider must treat the Entity Crypto-Asset User as a Reportable User in respect of each Reportable Jurisdiction.

27. Reportable Jurisdictions are expected to help taxpayers determine, and provide them with information with respect to, their residence(s) for tax purposes. That may be done, for example, through the various service channels used for providing information or guidance to taxpayers on the application of tax laws. The OECD will endeavour to facilitate the dissemination of such information.

28. If an Entity Crypto-Asset User certifies that it has no residence for tax purposes, the Reporting Crypto-Asset Service Provider may rely on the place of effective management or, as a proxy, on the address of the principal office of the Entity Crypto-Asset User to determine its residence. Examples of cases where an Entity Crypto-Asset User has no residence for tax purposes includes Entities treated as fiscally transparent and Entities resident in a jurisdiction with no corporate income tax system.

Reasonableness of self-certifications

29. Once the Reporting Crypto-Asset Service Provider has obtained a self-certification that allows it to determine the Entity Crypto-Asset User's residence(s) for tax purposes, the Reporting Crypto-Asset Service Provider must confirm the reasonableness of such self-certification based on the information obtained in connection with the establishment of the relationship, including any documentation collected pursuant to AML/KYC Procedures.

30. A Reporting Crypto-Asset Service Provider is considered to have confirmed the "reasonableness" of a self-certification if, in the course of establishing a relationship with the Entity Crypto-Asset User and upon review of the information obtained in connection with the establishment of the relationship (including any documentation collected pursuant to AML/KYC Procedures), it does not know or have reason to know that the self-certification is incorrect or unreliable. Reporting Crypto-Asset Service Providers are not expected to carry out an independent legal analysis of relevant tax laws to confirm the reasonableness of a self-certification.

31. The following examples illustrate the application of the "reasonableness" test:

- **Example 1**: A Reporting Crypto-Asset Service Provider obtains a self-certification from the Entity Crypto-Asset User upon the establishment of the relationship. The address contained in the self-certification conflicts with that contained in the documentation collected pursuant to AML/KYC Procedures. Because of the conflicting information, the self-certification is incorrect or unreliable and, as a consequence, it fails the reasonableness test.

- **Example 2**: A Reporting Crypto-Asset Service Provider obtains a self-certification from the Entity Crypto-Asset User upon the establishment of the relationship. The documentation collected pursuant to AML/KYC Procedures only indicates the Entity Crypto-Asset User's place of incorporation. In the self-certification, the Entity Crypto-Asset User claims to be resident for tax purposes in a jurisdiction that is different from its jurisdiction of incorporation. The Entity Crypto-Asset User explains to the Reporting Crypto-Asset Service Provider that under relevant tax laws its residence for tax purposes is determined by reference to place of effective management, and that the jurisdiction where its effective management is situated differs from the jurisdiction in which it was incorporated. Thus, because there is a reasonable explanation of the conflicting information, the self-certification is not incorrect or unreliable and, as a consequence, passes the reasonableness test.

32. In the case of a self-certification that fails the reasonableness test, it is expected that the Reporting Crypto-Asset Service Provider would obtain either (i) a valid self-certification, or (ii) a reasonable explanation and documentation (as appropriate) supporting the reasonableness of the self-certification (and retain a copy or a notation of such explanation and documentation) before providing services effectuating Relevant Transactions to the Entity Crypto-Asset User. Further guidance in this respect can be found in the Commentary to paragraph A of Section III.

Review procedure for Controlling Persons

33. Subparagraph B(2) contains the review procedure to determine whether an Entity Crypto-Asset User, other than an Excluded Person, is held by one or more Controlling Persons that are Reportable Persons, unless it determines that the Entity Crypto-Asset User is an Active Entity. Such determination should be made based on a self-certification, the reasonableness of which should be confirmed based on any relevant information available to the Reporting Crypto-Asset Service Provider. When the Reporting Crypto-Asset Service Provider has not determined that the Entity Crypto-Asset User is an Active Entity, then the Reporting Crypto-Asset Service Provider must follow the guidance in subparagraphs B(2)(a) and (b) in the order most appropriate under the circumstances. Those subparagraphs are aimed at:

- determining the Controlling Persons of an Entity Crypto-Asset User; and
- determining whether any Controlling Persons of the Entity Crypto-Asset User are Reportable Persons.

34. For the purposes of determining the Controlling Persons of an Entity Crypto-Asset User, according to subparagraph B(2)(a), a Reporting Crypto-Asset Service Provider may rely on information collected and maintained pursuant to AML/KYC Procedures, provided that such procedures are consistent with the 2012 FATF Recommendations (as updated in June 2019 pertaining to virtual asset service providers). If the Reporting Crypto-Asset Service Provider is not legally required to apply AML/KYC Procedures that are consistent with the 2012 FATF Recommendations (as updated in June 2019 pertaining to virtual asset service providers), it must apply substantially similar procedures for the purpose of determining the Controlling Persons.

35. For the purposes of determining whether a Controlling Person of an Entity Crypto-Asset User is a Reportable Person, a Reporting Crypto-Asset Service Provider must, pursuant to subparagraph B(2)(b), rely on a self-certification from either the Entity Crypto-Asset User or the Controlling Person and confirm the reasonableness of such self-certification based on the information obtained by the Reporting Crypto-Asset Service Provider, including any documentation collected pursuant to AML/KYC Procedures.

Change of circumstances

36. Subparagraph B(3) specifies that if, at any point, there is a change of circumstances with respect to an Entity Crypto-Asset User or its Controlling Person(s) that causes the Reporting Crypto-Asset Service

Provider to know, or have reason to know, that the self-certification or other documentation associated with an Entity Crypto-Asset User or its Controlling Person(s) is incorrect or unreliable, the Reporting Crypto-Asset Service Provider cannot rely on the original self-certification and must re-determine their status. In doing so, the procedures set forth in paragraphs 15 through 18 of the Commentary on Section III should be applied.

Paragraph C – Requirements for validity of self-certifications

37. Paragraph C sets out the requirements for obtaining valid self-certifications with respect to Individual and Entity Crypto-Asset Users, as well as Controlling Persons.

Validity of self-certifications for Individual Crypto-Asset Users and Controlling Persons

38. A self-certification referred to in subparagraph C(1) is a certification by the Individual Crypto-Asset User or Controlling Person that provides the Individual Crypto-Asset User's or Controlling Person's status and any other information that may be reasonably requested by the Reporting Crypto-Asset Service Provider to fulfil its reporting and due diligence obligations, such as whether the Individual Crypto-Asset User or the Controlling Person is resident for tax purposes in a Reportable Jurisdiction. A self-certification is valid only if it is signed (or otherwise positively affirmed) by the Individual Crypto-Asset User or Controlling Person, it is dated at the latest at the date of receipt, and it contains the following information with respect to the Individual Crypto-Asset User or Controlling Person:

a) first and last name;
b) residence address;
c) jurisdiction(s) of residence for tax purposes;
d) with respect to each Reportable Person, the TIN with respect to each Reportable Jurisdiction; and
e) date of birth.

39. The self-certification may be pre-populated by the Reporting Crypto-Asset Service Provider to include the Individual Crypto-Asset User's or Controlling Person's information, except for the jurisdiction(s) of residence for tax purposes, to the extent already available in its records. Further, the Reporting Crypto-Asset Service Provider may rely on a self-certification collected in respect of the Individual Crypto-Asset User or Controlling Person under the Common Reporting Standard or a self-certification already collected for other tax purposes, such as for domestic reporting purposes, in the context of the Foreign Account Tax Compliance Act (FATCA), or for purposes of a FATCA Intergovernmental Agreement, to the extent it contains all of the information referred to in subparagraph C(1).

40. If the Individual Crypto-Asset User or Controlling Person is resident for tax purposes in a Reportable Jurisdiction, the self-certification must include the Individual Crypto-Asset User's or Controlling Person's TIN with respect to each Reportable Jurisdiction, subject to subparagraph C(3).

41. The self-certification may be provided in any manner and in any form. If the self-certification is provided electronically, the electronic system must ensure that the information received is the information sent, and must document all occasions of user access that result in the submission, renewal, or modification of a self-certification. In addition, the design and operation of the electronic system, including access procedures, must ensure that the person accessing the system and furnishing the self-certification is the person named in the self-certification, and must be capable of providing upon request a hard copy of all self-certifications provided electronically.

42. A self-certification may be signed (or otherwise positively affirmed) by any person authorised to sign on behalf of the Individual Crypto-Asset User or Controlling Person under domestic law.

43. Subparagraph C(3) specifies that, notwithstanding the requirements under subparagraphs C(1) and (2) to obtain a TIN in respect of Reportable Users and of Controlling Persons of Entity Crypto-Asset Users that are Reportable Persons, the TIN is not required to be collected if the jurisdiction of residence of the Reportable Person does not issue a TIN to the Reportable Person.

Validity of self-certifications for Entity Crypto-Asset Users

44. A self-certification is a certification by the Entity Crypto-Asset User that provides the Entity Crypto-Asset User's status and any other information that may be reasonably requested by the Reporting Crypto-Asset Service Provider to fulfil its reporting and due diligence obligations, such as whether the Entity Crypto-Asset User is resident for tax purposes in a Reportable Jurisdiction. A self-certification is valid only if it is dated at the latest at the date of receipt, and it contains the Entity Crypto-Asset User's:

a) legal name;

b) address;

c) jurisdiction(s) of residence for tax purposes; and

d) with respect to each Reportable Person, the TIN with respect to each Reportable Jurisdiction; and

e) in case of an Entity Crypto-Asset User other than an Active Entity or an Excluded Person, the information described in subparagraph C(1) with respect to each Controlling Person of the Entity Crypto-Asset User, unless such Controlling Person has provided a self-certification pursuant to subparagraph C(1), as well as the role(s) by virtue of which each Reportable Person is a Controlling Person of the Entity, if not already determined on the basis of AML/KYC Procedures; and

f) if applicable, information as to the criteria it meets to be treated as an Active Entity or Excluded Person.

45. The self-certification may be pre-populated by the Reporting Crypto-Asset Service Provider to include the Entity Crypto-Asset User's information, except for the jurisdiction(s) of residence for tax purposes, to the extent already available in its records. Further, the Reporting Crypto-Asset Service Provider may rely on a self-certification collected in respect of the Entity Crypto-Asset User under the Common Reporting Standard or a self-certification already collected for other tax purposes, such as for domestic reporting purposes, in the context of FATCA, or for purposes of a FATCA Intergovernmental Agreement, to the extent it contains all of the information referred to in subparagraph C(2).

46. A self-certification may be signed (or otherwise positively affirmed) by any person authorised to sign on behalf of the Entity Crypto-Asset User under domestic law. A person with authority to sign a self-certification of an Entity Crypto-Asset User generally includes an officer or director of a corporation, a partner of a partnership, a trustee of a trust, any equivalent of the former titles, and any other person that has been provided written authorisation by the Entity Crypto-Asset User to sign documentation on such person's behalf.

47. The requirements for the validity of self-certifications with respect to Individual Crypto-Asset Users or Controlling Persons in paragraphs 40 and 41 of this section are also applicable for the validity of self-certifications with respect to Entity Crypto-Asset Users.

Paragraph D – General due diligence requirements

48. Subparagraph D(1) seeks to ensure consistent application of the due diligence procedures when a Reporting Crypto-Asset Service Provider is also a Reporting Financial Institution pursuant to the Common Reporting Standard. In such instances, where a Reporting Crypto-Asset Service Provider, by virtue of also being a Reporting Financial Institution, has completed the due diligence procedures pursuant

to Sections IV and VI of the Common Reporting Standard, such Reporting Crypto-Asset Service Provider may rely on such procedures to fulfil its due diligence obligations under the Crypto-Asset Reporting Framework.

49. A Reporting Crypto-Asset Service Provider may also rely on a self-certification already collected for other tax purposes, such as for domestic reporting purposes, in the context of FATCA, or for purposes of a FATCA Intergovernmental Agreement, provided such self-certification meets the requirements of paragraph C of this Section. In such instances, a Reporting Crypto-Asset Service Provider is still subject to the other elements of the due diligence procedures of Section III.

50. A Reporting Crypto-Asset Service Provider may rely on a third party to fulfil the due diligence obligations. The following situations apply in which Reporting Crypto-Asset Service Provider will rely on documentation of a third party to fulfil its due diligence obligations: first, with respect to documentation collected by third party service providers, agents or where a Reporting Crypto-Asset Service Provider relies on documentation of an acquired business and, secondly, with respect to the situation where a Reporting Crypto-Asset Service Provider relies on other Reporting Crypto-Asset Service Providers that handle the same Relevant Transaction. These scenarios are described, in turn, below.

51. Pursuant to subparagraph D(2), [Jurisdiction] may allow Reporting Crypto-Asset Service Providers to use service providers to fulfil their due diligence obligations. In such cases, Reporting Crypto-Asset Service Providers may use the documentation (including a self-certification) collected by service providers, subject to the conditions described in domestic law. The due diligence obligations remain, however, the responsibility of the Reporting Crypto-Asset Service Providers.

52. A Reporting Crypto-Asset Service Provider may also rely on documentation (including a self-certification) collected by an agent of the Reporting Crypto-Asset Service Provider. The agent may retain the documentation as part of an information system maintained for a single Reporting Crypto-Asset Service Provider or multiple Reporting Crypto-Asset Service Providers provided that under the system, any Reporting Crypto-Asset Service Provider on behalf of which the agent retains documentation may easily access data regarding the nature of the documentation, the information contained in the documentation (including a copy of the documentation itself) and its validity, and must allow such Reporting Crypto-Asset Service Provider to easily transmit data, either directly into an electronic system or by providing such information to the agent, regarding any facts of which it becomes aware that may affect the reliability of the documentation. The Reporting Crypto-Asset Service Provider must be able to establish, to the extent applicable, how and when it has transmitted data regarding any facts of which it became aware that may affect the reliability of the documentation and must be able to establish that any data it has transmitted has been processed and appropriate due diligence has been exercised regarding the validity of the documentation. The agent must have a system in effect to ensure that any information it receives regarding facts that affect the reliability of the documentation or the status assigned to the Crypto-Asset User are provided to all Reporting Crypto-Asset Service Providers for which the agent retains the documentation.

53. A Reporting Crypto-Asset Service Provider that acquires the business of another Reporting Crypto-Asset Service Provider that has completed all the due diligence required under Section III with respect to the Individual Crypto-Asset Users transferred, would generally be permitted to also rely upon the predecessor's or transferor's determination of status of an Individual Crypto-Asset User until the acquirer knows, or has reason to know, that the status is inaccurate or a change in circumstances occurs.

54. Subparagraph D(2) also seeks to avoid duplicative or multiple application of the due diligence procedures by individuals or Entities that are all Reporting Crypto-Asset Service Providers effectuating the same Relevant Transaction with respect to the same Crypto-Asset User. This is particularly relevant in instances where another Reporting Crypto-Asset Service Provider may have better access to information to carry out the due diligence procedures, as it is recognised that not all functionalities or services associated with a given Relevant Transaction are necessarily provided by a single individual or Entity. In

certain instances, these functionalities may be split among different individuals or Entities that could each be a Reporting Crypto-Asset Service Provider in respect of the Relevant Transaction. For instance, a broker in Relevant Crypto-Assets may receive an order from a client to conduct a Relevant Transaction in Crypto-Assets. The broker could transmit the client's order to a trading platform, which effectuates the transaction on behalf of the client. In this case, the broker is a Reporting Crypto-Asset Service Provider where it acts on behalf of a client to complete orders to buy or sell interest in Relevant Crypto-Assets. Similarly, the trading platform is also a Reporting Crypto-Asset Service Provider as it conducts the actual Exchange Transaction. As a result there may be more than one Reporting Crypto-Asset Service Provider effectuating the same Relevant Transaction with respect to the same Crypto-Asset User.

55. Subparagraph D(2) allows Reporting Crypto-Asset Service Providers to designate a single Reporting Crypto-Asset Service Provider to comply with all due diligence requirements, in case multiple Reporting Crypto-Asset Service Providers provide services effectuating the same Relevant Transaction.

56. To that end, a Reporting Crypto-Asset Service Provider may rely on a third party to fulfil the due diligence obligations set out in Section III. In order for a Reporting Crypto-Asset Service Provider to be able to rely on a third party (including another Reporting Crypto-Asset Service Provider) for the performance of the due diligence obligations under Section III, appropriate contractual arrangements should be put in place. Such arrangements should include an obligation for the Reporting Crypto-Asset Service Provider to make the information necessary to comply with the due diligence procedures of the Crypto-Asset Reporting Framework available to the third party(ies) fulfilling such obligations. This would include information held by the Reporting Crypto-Asset Service Provider that is needed by a third party(ies) to complete the due diligence procedures. The arrangements should also ensure that the Reporting Crypto-Asset Service Provider can obtain any information collected and verified in respect of Crypto-Asset Users from the third party(ies) to allow the Reporting Crypto-Asset Service Provider to demonstrate compliance with the requirements of Section III, for instance in the framework of an audit.

57. It is important to note that the fact that a Reporting Crypto-Asset Service Provider relies on a third party (including another Reporting Crypto-Asset Service Provider) to complete the due diligence procedures does not mean that the Reporting Crypto-Asset Service Provider is discharged from its obligations under Section III. Rather, subparagraph D(2) stipulates that the Reporting Crypto-Asset Service Provider remains responsible for the completion of the due diligence procedures.

58. Subparagraph D(3) specifies relevant information retention obligations, whereby a Reporting Crypto-Asset Service Provider is required to ensure that all documentation and data remain available for a period of not less than five years (in order to correspond to the requirements for record-keeping pursuant to the Global Forum Standard for the Exchange of Information upon Request) after the end of the period within which the Reporting Crypto-Asset Service Provider must report the information required to be reported pursuant to Section II, including in instances where the Reporting Crypto-Asset Service Provider is liquidated or otherwise terminates its business. Such information includes any information used to identify the Crypto-Asset User, as well as any external wallet addresses (or other equivalent identifiers) associated with Transfers of Relevant Crypto-Assets that are subject to reporting under subparagraph A(3)(i).

Commentary on Section IV: Defined terms

Paragraph IV (A) – Relevant Crypto-Asset

Subparagraph A(1) – Crypto-Asset

1. The term "Crypto-Asset", as defined in subparagraph A(1), refers to a digital representation of value that relies on a cryptographically secured distributed ledger or a similar technology to validate and secure transactions.

2. In this context, a "digital representation of value" means that a Crypto-Asset must represent a right to value, and that the ownership of, or right to, such value can be traded or transferred to other individuals or Entities in a digital manner. For instance, a token based on cryptography that allows individuals to store value, engage in payments and that does not represent any claims or rights of memberships against a person, rights to property or other absolute or relative rights is a Crypto-Asset.

3. Furthermore, a cryptographic token that represents claims or rights of membership against an individual or Entity, rights to property or other absolute or relative rights (e.g. a security token or a derivative contract or right to purchase or sell an asset, including a Financial Asset and a Crypto-Asset, at a set date, price or other pre-determined factor), and that can be digitally exchanged for Fiat Currencies or other Crypto-Assets, is a Crypto-Asset. For instance, the following examples illustrate the reporting requirements in respect of derivatives:

- **Example 1**: (Crypto-Derivative A, a cryptographic token, purchased with Relevant Crypto-Assets (i.e. stablecoins that are not Specified Electronic Money Products)): Crypto-Derivative A, represents a leveraged interest in an underlying Relevant Crypto-Asset, such that, the value of Crypto-Derivative A will mirror changes in the price of the underlying Relevant Crypto-Asset (either upwards or downwards) at three times the change in market price.

  User 1 purchases one unit of Crypto-Derivative A through consideration in the form of stablecoins. As Crypto-Derivative A is a Relevant Crypto-Asset, it is reportable under the Crypto-Asset Reporting Framework, provided the trade is carried out through a Reporting Crypto-Asset Service Provider. The trade entails the following Relevant Transactions:

  1. Disposal of the stablecoin by User 1, reported in Fiat Currency at the fair market value, along with the number of units; and
  2. Acquisition of Crypto-Derivative A by User 1, reported in Fiat Currency at the fair market value, along with the number of units.
- **Example 2**: (Redeeming Crypto-Derivative A, with settlement in stablecoins): Further to the trade in Example 1, User 1 redeems Crypto-Derivative A with the issuer. When User 1 redeems Crypto-Derivative A, the market price of the underlying Relevant Crypto-Asset has gained 10% since User 1 purchased Crypto-Derivative A. User 1's gains are magnified by the leverage of the token, and User 1 redeems Crypto-Derivative A with the issuer for a value 30% greater than the initial purchase price. The Reporting Crypto-Asset Service Provider pays this redemption amount to User 1's wallet in stablecoins. The trade entails the following Relevant Transactions:
  1. Disposal of Crypto-Derivative A, valued in Fiat Currency at its fair market value, along with the number of units; and
  2. Acquisition of stablecoin, valued in Fiat Currency at their fair market value, along with the number of units.
- **Example 3**: (Traditional derivative contract settled by physical delivery of a Relevant Crypto-Asset): Two counterparties, Buyer and Seller, enter into opposing positions of a futures

contract to, respectively, purchase and sell Relevant Crypto-Asset B on a specified date. The settlement of the derivative requires Buyer to purchase Relevant Crypto-Asset B from Seller on a specified date and at a pre-determined price, paid in Fiat Currency. Seller is then obliged to physically deliver Relevant Crypto-Asset B to Buyer's wallet address. On the specified date, Buyer and Seller conduct the transaction, by using a Reporting Crypto-Asset Service Provider to facilitate the following Relevant Transactions in respect of Relevant Crypto-Asset B:

1. Disposal of Relevant Crypto-Asset B by Seller, reported at the Fiat Currency received, along with the number of units; and
2. Acquisition of Relevant Crypto-Asset B by Buyer, reported at the Fiat Currency paid, along with the number of units.

4. The term "Crypto-Asset" is intended to cover any digital representation of value that relies on a cryptographically secured distributed ledger or a similar technology to validate and secure transactions, where the ownership of, or right to, such value can be traded or transferred to other individuals or Entities in a digital manner. As such, the term "Crypto-Asset" encompasses both fungible and non-fungible tokens and therefore includes non-fungible tokens (NFTs) representing rights to collectibles, games, works of art, physical property or financial documents that can be traded or transferred to other individuals or Entities in a digital manner.

5. Other uses of cryptographic technology that are not digital representations of value, are not Crypto-Assets. Examples include the use of cryptography to:

- create a decentralized immutable record of activities or materials involved in making, storing, shipping or delivering a product, where the record does not convey any ownership rights in such product; or
- a declarative record of ownership of assets (such as a real estate ledger or similar agreement) where the record does not convey any ownership rights in the assets represented by such record.

6. In addition to having inherent value that is digitally tradable or transferable, a Crypto-Asset must rely on a cryptographically secured distributed ledger or similar technology to validate and secure transactions whether or not the transaction is actually recorded on such distributed ledger or similar technology. A distributed ledger is a decentralised manner for recording transactions in Crypto-Assets in multiple places and at the same time. Cryptography refers to a mathematical and computational practice of encoding and decoding data that is used to validate and secure transactions in a decentralised or non-intermediated manner. The cryptographic process is used to ensure, in a decentralised manner, the integrity of Crypto-Assets, the clear assignment of Crypto-Assets to users, and the disposal of Crypto-Assets.

7. This cryptographic process allows multiple parties to engage in disintermediated validations of transactions in the Crypto-Asset, often by verifying public and private cryptographic keys to a transaction. This validation ensures that users in possession of a Crypto-Asset have not already exchanged the same Crypto-Asset in another transaction. The cryptographic process also secures transactions made in Crypto-Assets by compiling each transaction within a block of other transactions. The block of transactions is then added to the official, publicly accessible, transaction ledger (such as a blockchain) once the user completes a cryptographic hash.

8. Crypto-Assets may also rely on similar technology that allows for the disintermediated holding or validating of Crypto-Assets. Regardless of the type of software used, if the technology underpinning the Crypto-Asset allows for validating and securing digital transactions in a decentralised or disintermediated manner, it is considered a similar technology to a cryptographically secured distributed ledger.

Subparagraph A(2) – Relevant Crypto-Assets

9. Relevant Crypto-Assets are Crypto-Assets in respect of which Reporting Crypto-Asset Service Providers must fulfil reporting and due diligence requirements. The term Relevant Crypto-Assets applies to all Crypto-Assets except Central Bank Digital Currencies, Specified Electronic Money Products and Crypto-Assets for which the Reporting Crypto-Asset Service Provider has adequately determined that they cannot be used for payment or investment purposes. If an individual or Entity is a Reporting Crypto-Asset Service Provider (e.g. because it otherwise carries out exchanges in Relevant Crypto-Assets), it would nevertheless not be required to report information with respect to exchanges carried out in Crypto-Assets that are not Relevant Crypto-Assets.

10. For the purpose of adequately determining whether a Crypto-Asset cannot be used for payment or investment purposes, Reporting Crypto-Asset Service Providers may, in a first step, rely on the classification of the Crypto-Asset that was made for the purpose of determining whether the Crypto-Asset is a virtual asset for AML/KYC purposes pursuant to the FATF Recommendations. In case a Crypto-Asset is considered a virtual asset pursuant to FATF Recommendations by virtue of being able to be used for payment or investment purposes, it is to be considered a Relevant Crypto-Asset for purposes of the Crypto-Asset Reporting Framework.

11. Where an asset is not a virtual asset pursuant to FATF Recommendations or the Reporting Crypto-Asset Service Provider has not made a determination to that effect, the Reporting Crypto-Asset Service Provider must determine, for each Crypto-Asset, whether it cannot be used for payment or investment purposes. Only when this test can be positively affirmed, the Crypto-Asset is not to be considered a Relevant Crypto-Asset. In case of doubts as to whether the Crypto-Asset can be used for payment or investment purposes, the Crypto-Asset is to be considered a Relevant Crypto-Asset.

12. In assessing whether a Crypto-Asset cannot be used for payment or investment purposes, the following aspects may be taken into account:

- Crypto-Assets that represent Financial Assets or are subject to financial regulation can be used for payment or investment purposes and are therefore to be considered Relevant Crypto-Assets.
- NFTs are in many instances marketed as collectibles. This function does, however, by itself not prevent an NFT from being able to be used for payment or investment purposes. It is important to consider the nature of the NFT and its function in practice and not what terminology or marketing terms are used. NFTs that can be used for payment or investment purposes in practice are Relevant Crypto-Assets. Reporting Crypto-Asset Service Providers should therefore consider on a case-by-case basis whether an NFT cannot be used for payment or investment purposes, taking into account the commonly accepted usage of the Crypto-Asset. NFTs that are traded on a marketplace can be used for payment or investment purposes and are therefore to be considered Relevant Crypto-Assets.
- Certain Crypto-Assets can only be exchanged or redeemed within a limited fixed network or environment for specified goods and services, such as food, book, and restaurant vouchers, as well airline miles or other loyalty program rewards. In this context, the term “goods and services” may also include digital goods and services, such as digital music, games, books or other media, as well as tickets, software applications and online subscriptions. Provided these Crypto-Assets are characterised by operating in a limited fixed network or environment beyond which the Crypto-Assets cannot be transferred or exchanged in a secondary market outside of the closed-loop system, and cannot be sold or exchanged at a market rate inside or outside of the closed-loop, such Crypto-Assets would generally not be able to be used for payment or investment purposes.

Subparagraph A(3) – Central Bank Digital Currency

13. The term "Central Bank Digital Currencies" means any digital Fiat Currency issued by a Central Bank. Central Bank Digital Currencies are not considered Relevant Crypto-Assets, given that they are a digital form of Fiat Currency.

Subparagraph A(4) – Specified Electronic Money Product

14. Subparagraph A(4) defines the term "Specified Electronic Money Product" as any Crypto-Asset that is:

a) a digital representation of a single Fiat Currency;

b) issued on receipt of funds for the purpose of making payment transactions;

c) represented by a claim on the issuer denominated in the same Fiat Currency;

d) accepted in payment by a natural or legal person other than the issuer; and

e) by virtue of regulatory requirements to which the issuer is subject, redeemable at any time and at par value for the same Fiat Currency upon request of the holder of the product.

The term "Specified Electronic Money Product" does not include a product created for the sole purpose of facilitating the transfer of funds from a customer to another person pursuant to instructions of the customer. A product is not created for the sole purpose of facilitating the transfer of funds if, in the ordinary course of business of the transferring Entity, either the funds connected with such product are held longer than 60 days after receipt of instructions to facilitate the transfer, or, if no instructions are received, the funds connected with such product are held longer than 60 days after receipt of the funds.

15. Subparagraph A(4)(a) requires that a Crypto-Asset must be a digital representation of a single Fiat Currency, in order to be a Specified Electronic Money Product. A Crypto-Asset will be considered to digitally represent and reflect the value of the Fiat Currency that it is denominated in. Consequently, a Crypto-Asset that reflects the value of multiple currencies or assets is not a Specified Electronic Money Product.

16. Subparagraph A(4)(b) provides that the Crypto-Asset must be issued on receipt of funds. This part of the definition means that a Specified Electronic Money Products is a prepaid product. The act of "issuing" is interpreted broadly to include the activity of making available pre-paid stored value and means of payment in exchange for funds. In addition, this subparagraph provides that the Crypto-Asset must be issued for the purpose of making payment transactions.

17. Subparagraph A(4)(c) requires that, in order to be a Specified Electronic Money Product, a Crypto-Asset must be represented by a claim on the issuer denominated in the same Fiat Currency. In this respect, a "claim" includes any monetary claim against the issuer, reflecting the value of the Fiat Currency represented by the Crypto-Asset issued to the customer.

18. Under subparagraph A(4)(d), a Crypto-Asset must be accepted by a natural or legal person other than the issuer in order to be a Specified Electronic Money Product, whereby such third parties must accept the Crypto-Asset as a means of payment. Consequently, monetary value stored on specific pre-paid instruments, designed to address precise needs that can be used only in a limited way, because they allow the electronic money holder to purchase goods or services only in the premises of the electronic money issuer or within a limited network of service providers under direct commercial agreement with a professional issuer, or because they can be used only to acquire a limited range of goods or services, are not considered Specified Electronic Money Products.

19. Subparagraph A(4)(e) provides that the issuer of the Crypto-Assets must be subject to supervision to ensure the product is redeemable at any time and at par value for the same Fiat Currency upon request

of the holder of the Crypto-Asset, in order to be a Specified Electronic Money Product. In this respect, the "same" Fiat Currency refers to the Fiat Currency that the Crypto-Asset is a digital representation of. When proceeding to a redemption, it is acknowledged that the issuer can deduct from the redemption amount any fees or transaction costs.

20. The definition excludes those products that are created solely to facilitate a funds transfer pursuant to instructions of a customer and that cannot be used to store value. For example, such products may be used to enable an employer to transfer the monthly wages to its employees or to enable a migrant worker to transfer funds to relatives living in another country. A product is not created for the sole purpose of facilitating the transfer of funds if, in the ordinary course of business of the transferring Entity, either the funds connected with such product are held longer than 60 days after receipt of instructions to facilitate the transfer, or, if no instructions are received, the funds connected with such product are held longer than 60 days after receipt of the funds.

Paragraph IV (B) – Reporting Crypto-Asset Service Provider

Subparagraph B(1) – Reporting Crypto-Asset Service Provider

21. The term "Reporting Crypto-Asset Service Provider" refers to any individual or Entity that, as a business, provides a service effectuating Exchange Transactions for or on behalf of customers (which for the purposes of this definition includes users of services of Reporting Crypto-Asset Service Providers), including by acting as a counterparty, or as an intermediary, to Exchange Transactions, or by making available a trading platform.

22. The phrase "as a business" excludes individuals or Entities who carry out a service on a very infrequent basis for non-commercial reasons. In determining what is meant by "as a business", reference can be made to each jurisdiction's relevant rules.

23. A service effectuating Exchange Transactions includes any service through which the customer can receive Relevant Crypto-Assets for Fiat Currencies, or vice versa, or exchange Relevant Crypto-Assets for other Relevant Crypto-Assets. The activities of an investment fund investing in Relevant Crypto-Assets do not constitute a service effectuating Exchange Transactions since such activities do not permit the investors in the fund to effectuate Exchange Transactions.

24. An individual or Entity effectuating Exchange Transactions will only be a Reporting Crypto-Asset Service Provider if it carries out such activities for or on behalf of customers. This means, for example, that an individual or Entity that is solely engaged in validating distributed ledger transactions in Relevant Crypto-Assets is not a Reporting Crypto-Asset Service Provider, even where such validation is remunerated.

25. An individual or Entity may effectuate Exchange Transactions for or on behalf of customers by acting as a counterparty or intermediary to the Exchange Transactions. Examples of individuals or Entities that may provide services effectuating Exchange Transactions as a counterparty, or as an intermediary, include:

- dealers acting for their own account to buy and sell Relevant Crypto-Assets to customers;
- operators of Crypto-Asset ATMs, permitting the exchange of Relevant Crypto-Assets for Fiat Currencies or other Relevant Crypto-Assets through such ATMs;
- Crypto-Asset exchanges that act as a market makers and take a bid-ask spread as a transaction commission for their services;
- brokers in Relevant Crypto-Assets where they act on behalf of clients to complete orders to buy or sell an interest in Relevant Crypto-Assets; and

- individuals or Entities subscribing one or more Relevant Crypto-Assets. While the sole creation and issuance of a Relevant Crypto-Asset would not be considered a service effectuating Exchange Transactions as a counterparty or intermediary, the direct purchase of Relevant Crypto-Assets from an issuer, to resell and distribute such Relevant Crypto-Assets to customers would be considered effectuating an Exchange Transaction.

26. An individual or Entity may also effectuate Exchange Transactions for or on behalf of customers by making available a trading platform that provides the ability for such customers to effectuate Exchange Transactions on such platform. A "trading platform" includes any software program or application that allows users to effectuate (either partially or in their entirety) Exchange Transactions. An individual or Entity that is making available a platform that solely includes a bulletin board functionality for posting buy, sell or conversion prices of Relevant Crypto-Assets would not be a Reporting Crypto-Asset Service Provider as it would not provide a service allowing users to effectuate Exchange Transactions. For the same reason, an individual or Entity that solely creates or sells software or an application is not a Reporting Crypto-Asset Service Provider, as long as it is not using such software or application for the provision of a service effectuating Exchange Transactions for or on behalf of customers.

27. An individual or Entity will be considered to make available a trading platform to the extent it exercises control or sufficient influence over the platform, allowing it to comply with the due diligence and reporting obligations with respect to Exchange Transactions concluded on the platform. Whether an individual or Entity exercises such control or sufficient influence should be assessed in a manner consistent with the 2012 FATF Recommendations (as amended in June 2019 with respect to virtual assets and virtual asset service providers) and related FATF guidance.

28. An individual or Entity may be a Reporting Crypto-Asset Service Provider by carrying out activities other than acting as a counterparty, or intermediary, to an Exchange Transaction, or making available a trading platform, as long as it functionally provides a service, as a business, effectuating Exchange Transactions for or on behalf of customers. The technology involved in providing such service is irrelevant to determine whether an individual or Entity is a Reporting Crypto-Asset Service Provider.

Paragraph IV (C) – Relevant Transaction

Subparagraph C(1) – Relevant Transaction

29. The term "Relevant Transaction" refers to any exchange of Relevant Crypto-Assets and Fiat Currencies, any exchange between one or more forms of Relevant Crypto-Assets and Transfers of Relevant Crypto-Assets, including Reportable Retail Payment Transactions. This definition targets those transactions likely to give rise to taxation events (i.e. capital gains and income taxation).

Subparagraph C(2) – Exchange Transaction

30. An Exchange Transaction, as defined in subparagraph C(2), refers to any exchange between Relevant Crypto-Assets and Fiat Currencies as well as any exchange between one or more forms of Relevant Crypto-Assets. For this purpose, an exchange includes the movement of a Relevant Crypto-Asset from one wallet address to another, in consideration of another Relevant Crypto-Asset or Fiat Currency.

Subparagraph C(3) – Reportable Retail Payment Transaction

31. Subparagraph C(3) defines the term "Reportable Retail Payment Transaction" as a Transfer of Relevant Crypto-Assets in consideration of goods or services for a value exceeding USD 50,000. This term covers situations where a Reporting Crypto-Asset Service Provider transfers Relevant Crypto-Assets used by a customer to purchase goods or services from a merchant who receives the Relevant Crypto-Assets

as consideration. For example, a Reporting Crypto-Asset Service Provider may carry out Relevant Transactions between a merchant and its customers to allow payment for goods or services with Relevant Crypto-Assets. Where a Reporting Crypto-Asset Service Provider transfers payment made in Relevant Crypto-Assets from a customer to the merchant for a value above the specified threshold, the Reporting Crypto-Asset Service Provider should report such Transfer as a Reportable Retail Payment Transaction. With respect to such Transfers, the Reporting Crypto-Asset Service Provider is required to also treat the customer of the merchant as the Crypto-Asset User, provided that the Reporting Crypto-Asset Service Provider is required to verify the identity of such customer pursuant to domestic anti-money laundering rules, by virtue of the Reportable Retail Payment Transaction.

Subparagraph C(4) –Transfers

32. The term "Transfer" means a transaction that moves a Relevant Crypto-Asset from or to the Crypto-Asset address or account of one Crypto-Asset User, other than one maintained by the Reporting Crypto-Asset Service Provider on behalf of same Crypto-Asset User. A Reporting Crypto-Asset Service Provider can only classify a Relevant Transaction as a Transfer if, based on the knowledge of the Reporting Crypto-Asset Service Provider at the time of transaction, the Reporting Crypto-Asset Service Provider cannot determine that the transaction is an Exchange Transaction. Such knowledge should be determined by reference to the Reporting Crypto-Asset Service Provider's actual knowledge based on readily available information and the degree of expertise and understanding required to conduct the Relevant Transaction. For example, there may be instances where a Crypto-Asset User acquires or disposes of a Relevant Crypto-Asset against Fiat Currency, although the Reporting Crypto-Asset Service Provider does not have actual knowledge of the underlying consideration. This would, for example, be the case if the Reporting Crypto-Asset Service Provider only conducted the Transfer of the Relevant Crypto-Assets to and from the Crypto-Asset User's account, without visibility over the Fiat Currency leg of the transaction. Such transactions would still be considered Relevant Transactions, but the Reporting Crypto-Asset Service Provider would need to report such Relevant Transactions as Transfers.

33. A "Transfer" would also include the instance where a Reporting Crypto-Asset Service Provider facilitates an individual or Entity receiving a Relevant Crypto-Asset by means of an airdrop when the Crypto-Asset is newly issued. For instance, in the context of a "hard-fork" a new Relevant Crypto-Asset diverges from a legacy Relevant Crypto-Asset. As a result, developers of the hard fork typically send an airdrop of new Relevant Crypto-Assets to all holders of the legacy Relevant Crypto-Asset and such Crypto-Asset Users will hold the new Relevant Crypto-Assets in addition to the legacy Relevant Crypto-Assets. For example, the receipt of an airdrop of a new Relevant Crypto-Asset is considered an inbound Transfer to the receiving Crypto-Asset User.

Subparagraph C(5) – Fiat Currency

34. The term Fiat Currency refers to the official currency of a jurisdiction, issued by a jurisdiction or by a jurisdiction's designated Central Bank or monetary authority, as represented by physical banknotes or coins or by money in different digital forms, including bank reserves, and Central Bank Digital Currencies. The term also includes commercial bank money and electronic money products (including Specified Electronic Money Products). Accordingly, a stablecoin that qualifies as a Specified Electronic Money Product is treated as Fiat Currency.

Paragraph IV (D) – Reportable User

Subparagraph D(1) – Reportable User

35. The term "Reportable User", as defined in subparagraph D(1), means a Crypto-Asset User that is a Reportable Person.

Subparagraph D(2) – Crypto-Asset User

36. Subparagraph D(2) defines the term "Crypto-Asset User" as a customer of a Reporting Crypto-Asset Service Provider for purposes of carrying out Relevant Transactions. Any individual or Entity identified by the Reporting Crypto Asset Service Provider for purposes of carrying out Relevant Transactions is treated as a Crypto Asset User, irrespective of whether the Reporting Crypto-Asset Service Provider is safekeeping the Relevant Crypto-Assets on behalf of the Crypto-Asset User or the legal characterisation of the relationship between the Reporting Crypto-Asset Service Provider and such individual or Entity.

37. An individual or Entity, other than a Financial Institution or Reporting Crypto-Asset Service Provider, acting as a Crypto-Asset User for the benefit or account of another individual or Entity as agent, custodian, nominee, signatory, investment advisor, or intermediary, is not treated as a Crypto-Asset User, and such other individual or Entity is treated as the Crypto-Asset User. For these purposes a Reporting Crypto-Asset Service Provider may rely on information in its possession (including information collected pursuant to AML/KYC Procedures), based on which it can reasonably determine whether the individual or Entity is acting for the benefit or account of another individual or Entity. In confirming whether a Crypto-Asset User may be a Reporting Crypto-Asset Service Provider or a Financial Institution, a Reporting Crypto-Asset Service provider may, for instance, rely on cross-checking the information provided by its Crypto-Asset User with regulated institutions lists that indicate other Reporting Crypto-Asset Service Providers or Financial Institutions, where available.

38. The following examples illustrate the application of this definition:

- F holds a power of attorney from U that authorises F to establish a relationship as a Crypto-Asset User at Reporting Crypto-Asset Service Provider X for carrying out Relevant Transactions on behalf of U. F has established a relationship at Reporting Crypto-Asset Service Provider X as the person who can carry out Relevant Transactions. However, because F is not a Financial Institution or Reporting Crypto-Asset Service Provider and the Reporting Crypto-Asset Service Provider has information in its AML/KYC files indicating that F acts as an agent for the benefit of U, the Reporting Crypto-Asset Service Provider must treat U as the Crypto-Asset User;
- Reporting Crypto-Asset Service Provider A uses the services of Reporting Crypto-Asset Service Provider B to effectuate Relevant Transactions on the exchange platform maintained by B. Therefore, A is a Crypto-Asset User for B, and B will report the Relevant Transactions effectuated by A. Because A is a Reporting Crypto-Asset Service Provider, it is immaterial whether A effectuates such Relevant Transactions in its own name or as an agent, custodian, nominee, signatory, investment advisor or intermediary.

39. A Reporting Crypto-Asset Service Provider may conduct Relevant Transactions that allow a merchant to offer its customers payment in the form of Relevant Crypto-Assets, in consideration of a purchase of goods or services. In those instances, and provided that the value of the transaction exceeds USD 50 000, the transaction is considered a Relevant Transaction by virtue of being a Reportable Retail Payment Transaction. See Commentary to subparagraph C(3). For Reportable Retail Payment Transactions, the Reporting Crypto-Asset Service Provider must treat the customer of the merchant as the Crypto-Asset User and the transaction should be reported as a Reportable Retail Payment Transaction pursuant to subparagraph A(3)(f) of Section II, provided that the Reporting Crypto-Asset Service Provider is required to verify the identity of such customer pursuant to domestic anti-money laundering rules, by virtue of the Reportable Retail Payment Transaction. The requirement to verify the identity of the customer means a requirement pursuant to domestic anti-money laundering rules that requires the Reporting Crypto-Asset Service Provider to verify the identity using reliable, independent source documents, data or information.

Subparagraphs D(3) through (6) – Preexisting, Individual and Entity Crypto-Asset Users

40. Subparagraphs D(3) through (6) contain the various categories of Crypto-Asset Users classified by reference to date of the establishment of the relationship or type of Crypto-Asset User: "Individual Crypto-Asset User", "Preexisting Individual Crypto-Asset User", "Entity Crypto-Asset User", "Preexisting Entity Crypto-Asset User".

41. A Crypto-Asset User is classified, firstly, depending on whether it is an individual or an Entity and, secondly, depending on the date it established a relationship as such with a Reporting Crypto-Asset Service Provider. Thus, a Crypto-Asset User can be either a "Preexisting Individual Crypto-Asset User", a "Preexisting Entity Crypto-Asset User", an "Individual Crypto-Asset User" and/or an "Entity Crypto-Asset User".

42. As such, Preexisting Individual Crypto-Asset Users and Preexisting Entity Crypto-Asset Users are Crypto-Asset Users that have established a relationship as a customer of the Reporting Crypto-Asset Service Provider as of [xx/xx/xxxx] and are therefore a subset of Individual Crypto-Asset Users and Entity Crypto-Asset Users, respectively.

Subparagraph D(7) – Reportable Person

43. Subparagraph D(7) defines the term "Reportable Person" as a Reportable Jurisdiction Person other than an Excluded Person.

Subparagraph D(8) – Reportable Jurisdiction Person

44. As a general rule, an individual or Entity is a "Reportable Jurisdiction Person" if it is resident in a Reportable Jurisdiction under the tax laws of such jurisdiction.

45. Domestic laws differ in the treatment of partnerships (including limited liability partnerships). Some jurisdictions treat partnerships as taxable units (sometimes even as companies) whereas other jurisdictions adopt what may be referred to as the fiscally transparent approach, under which the partnership is disregarded for tax purposes. Where a partnership is treated as a company or taxed in the same way, it would generally be considered to be a resident of the Reportable Jurisdiction that taxes the partnership. Where, however, a partnership is treated as fiscally transparent in a Reportable Jurisdiction, the partnership is not "liable to tax" in that jurisdiction, and so cannot be a resident thereof.

46. An Entity such as a partnership, limited liability partnership or similar legal arrangement that has no residence for tax purposes shall be treated as resident in the jurisdiction in which its place of effective management is situated. For these purposes, a legal person or a legal arrangement is considered "similar" to a partnership and a limited liability partnership where it is not treated as a taxable unit in a Reportable Jurisdiction under the tax laws of such jurisdiction.

47. The "place of effective management" is the place where key management and commercial decisions that are necessary for the conduct of the Entity's business as a whole are in substance made. All relevant facts and circumstances must be examined to determine the place of effective management.

48. The term "Reportable Jurisdiction Person" also includes an estate of a decedent that was a resident of a Reportable Jurisdiction. In determining what is meant by "estate", reference must be made to each jurisdiction's particular rules on the transfer or inheritance of rights and obligations in the event of death (e.g. the rules on universal succession).

Subparagraph D(9) – Reportable Jurisdiction

49. Subparagraph D(9) defines "Reportable Jurisdiction" as any jurisdiction (a) with which an agreement or arrangement is in effect pursuant to which [Jurisdiction] is obligated to provide the information

specified in Section II with respect to Reportable Persons resident in such jurisdiction, and (b) which is identified as such in a list published by [Jurisdiction]. Subparagraph D(9) therefore requires that the jurisdiction is identified in a published list as a Reportable Jurisdiction. Each jurisdiction must make such a list publicly available, and update it as appropriate (e.g. every time the jurisdiction signs an agreement with respect to exchanging information under these rules, or such an agreement enters into force).

Subparagraph D(10) – Controlling Persons

50. Subparagraph D(10) sets forth the definition of the term "Controlling Persons". This term corresponds to the term "beneficial owner" as described in Recommendation 10 and the Interpretative Note on Recommendation 10 of the FATF Recommendations (as adopted in February 2012), and must be interpreted in a manner consistent with such Recommendations, with the aim of protecting the international financial system from misuse including with respect to tax crimes.

51. For an Entity that is a legal person, the term "Controlling Persons" means the natural person(s) who exercises control over the Entity. "Control" over an Entity is generally exercised by the natural person(s) who ultimately has a controlling ownership interest in the Entity. A "controlling ownership interest" depends on the ownership structure of the legal person and is usually identified on the basis of a threshold applying a risk-based approach (e.g. any person(s) owning more than a certain percentage of the legal person, such as 25%). Where no natural person(s) exercises control through ownership interests, the Controlling Person(s) of the Entity will be the natural person(s) who exercises control of the Entity through other means. Where no natural person(s) is identified as exercising control of the Entity, the Controlling Person(s) of the Entity will be the natural person(s) who holds the position of senior managing official.

52. In the case of a trust, the term "Controlling Persons" means the settlor(s), the trustee(s), the protector(s) (if any), the beneficiary(ies) or class(es) of beneficiaries, and any other natural person(s) exercising ultimate effective control over the trust. The settlor(s), the trustee(s), the protector(s) (if any), and the beneficiary(ies) or class(es) of beneficiaries, must always be treated as Controlling Persons of a trust, regardless of whether or not any of them exercises control over the trust. It is for this reason that the second sentence of subparagraph D(10) supplements the first sentence of such subparagraph. In addition, any other natural person(s) exercising ultimate effective control over the trust (including through a chain of control or ownership) must also be treated as a Controlling Person of the trust. With a view to establishing the source of funds in the account(s) held by the trust, where the settlor(s) of a trust is an Entity, Reporting Crypto-Asset Service Providers must also identify the Controlling Person(s) of the settlor(s) and report them as Controlling Person(s) of the trust. For beneficiary(ies) of trusts that are designated by characteristics or by class, Reporting Crypto-Asset Service Providers should obtain sufficient information concerning the beneficiary(ies) to satisfy the Reporting Crypto-Asset Service Provider that it will be able to establish the identity of the beneficiary(ies) at the time of the pay-out or when the beneficiary(ies) intends to exercise vested rights. Therefore, that occasion will constitute a change in circumstances and will trigger the relevant procedures.

53. In the case of a legal arrangement other than a trust, the term "Controlling Persons" means persons in equivalent or similar positions as those that are Controlling Persons of a trust. Thus, taking into account the different forms and structures of legal arrangements, Reporting Crypto-Asset Service Providers should identify and report persons in equivalent or similar positions, as those required to be identified and reported for trusts.

54. In relation to legal persons that are functionally similar to trusts (e.g. foundations), Reporting Crypto-Asset Service Providers should identify Controlling Persons through similar customer due diligence procedures as those required for trusts, with a view to achieving appropriate levels of reporting.

Subparagraph D(11) – Active Entity

55. An Entity is an Active Entity, provided that it meets any of the criteria listed in subparagraph D(11).

56. Subparagraph D(11)(a) describes the criterion to qualify for the Active Entity status by reason of income and assets as follows: less than 50% of the Entity's gross income for the preceding calendar year or other appropriate reporting period is passive income and less than 50% of the assets held by the Entity during the preceding calendar year or other appropriate reporting period are assets that produce or are held for the production of passive income.

57. In determining what is meant by "passive income", reference must be made to each jurisdiction's particular rules. Passive income would generally be considered to include the portion of gross income that consists of:

a) dividends;

b) interest;

c) income equivalent to interest or dividends;

d) rents and royalties, other than rents and royalties derived in the active conduct of a business conducted, at least in part, by employees of the Entity;

e) annuities;

f) income derived from Relevant Crypto-Assets;

g) the excess of gains over losses from the sale or exchange of Relevant Crypto-Assets or Financial Assets;

h) the excess of gains over losses from transactions (including futures, forwards, options, and similar transactions) in any Relevant Crypto-Assets or Financial Assets;

i) the excess of foreign currency gains over foreign currency losses;

j) net income from swaps; or

k) amounts received under cash value insurance contracts.

Notwithstanding the foregoing, passive income will not include, in the case of an Entity that regularly acts as a dealer in Relevant Crypto-Assets or Financial Assets, any income from any transaction entered into in the ordinary course of such dealer's business as such a dealer. Further, income received on assets to invest the capital of an insurance business can be treated as active income.

58. Subparagraph D(11)(b) describes the criterion to qualify for the Active Entity status for "holding Entities that are members of a nonfinancial group" as follows: substantially all of the activities of the Entity consist of holding (in whole or in part) the outstanding stock of, or providing financing and services to, one or more subsidiaries that engage in trades or businesses other than the business of a Financial Institution, except that an Entity does not qualify for this status if the Entity functions (or holds itself out) as an investment fund, such as a private equity fund, venture capital fund, leveraged buyout fund, or any investment vehicle whose purpose is to acquire or fund companies and then hold interests in those companies as capital assets for investment purposes.

59. With respect to the activities mentioned in subparagraph D(11)(b), "substantially all" means 80% or more. If, however, the Entity's holding or group finance activities constitute less than 80% of its activities but the Entity receives also active income (i.e. income that is not passive income) otherwise, it qualifies for the Active Entity status, provided that the total sum of activities meets the "substantially all test". For purposes of determining whether the activities other than holding and group finance activities of the Entity qualify it as an Active Entity, the test of subparagraph D(11)(a) can be applied to such other activities. For example, if a holding company has holding or finance and service activities to one or more subsidiaries for 60% and also functions for 40% as a distribution centre for the goods produced by the group it belongs to and the income of its distribution centre activities is active according to subparagraph D(11)(a), it is an

Active Entity, irrespective of the fact that less than 80% of its activities consist of holding the outstanding stock of, or providing finance and services to, one or more subsidiaries. The term "substantially all" covers also a combination of holding stock of and providing finance and services to one or more subsidiaries. The term "subsidiary" means any entity whose outstanding stock is either directly or indirectly held (in whole or in part) by the Entity.

60. One of the requirements listed in subparagraph D(11)(f) for "non-profit Entities" to qualify for the Active Entity status is that the applicable laws of the Entity's jurisdiction of residence or the Entity's formation documents do not permit any income or assets of the Entity to be distributed to, or applied for the benefit of, a private person or non-charitable Entity other than pursuant to the conduct of the Entity's charitable activities, or as payment of reasonable compensation for services rendered, or as payment representing the fair market value of property which the Entity has purchased. In addition, the income or assets of the Entity could be distributed to, or applied for the benefit of, a private person or noncharitable Entity as payment of reasonable compensation for the use of property.

Paragraph IV (E) – Excluded Person

Subparagraph E(1) – Excluded Person

61. Subparagraph E(1) defines the term "Excluded Person" as (a) an Entity the stock of which is regularly traded on one or more established securities markets; (b) any Entity that is a Related Entity of an Entity described in clause (a); (c) a Governmental Entity; (d) an International Organisation; (e) a Central Bank; or (f) a Financial Institution other than an Investment Entity described in Section IV E(5)(b). Those Entities that are covered by the term "Excluded Person" are not subject to reporting under the Crypto-Asset Reporting Framework, in light of the limited tax compliance risks these Entities represent and/or the other tax reporting obligations certain of these Entities are subject to, including pursuant to the Common Reporting Standard. As such, the scope of Excluded Persons is, wherever adequate, aligned to the exclusions from reporting foreseen in the Common Reporting Standard.

Subparagraphs E(2)-(4) – Financial Institution, Custodial Institution, and Depository Institution

62. The terms "Financial Institution", "Custodial Institution" and "Depository Institution" in subparagraphs E(2), (3) and (4), respectively, should be interpreted consistently with the Commentary of the Common Reporting Standard, as amended.

Subparagraph E(5) – Investment Entity

63. The term "Investment Entity" includes two types of Entities: Entities that primarily conduct, as a business, investment activities or operations on behalf of other persons, and Entities that are managed by those Entities or other Financial Institutions.

64. Subparagraph E(5)(a) defines the first type of "Investment Entity" as any Entity that primarily conducts as a business one or more of the following activities or operations for or on behalf of a customer:

a) trading in money market instruments (cheques, bills, certificates of deposit, derivatives, etc.); foreign exchange; exchange, interest rate and index instruments; transferable securities; or commodity futures trading;

b) individual and collective portfolio management; or

c) otherwise investing, administering, or managing Financial Assets, or money (including Central Bank Digital Currencies), or Relevant Crypto-Assets on behalf of other persons.

65. Such activities or operations do not include rendering non-binding investment advice to a customer. For purposes of subparagraph E(5)(a), the term “customer” includes the Equity Interest holder of a collective investment vehicle, whereby the collective investment vehicle is considered to conduct its activities or operations as a business. For purposes of subparagraph E(5)(a)(iii), the term "investing, administering, or trading" does not comprise the provision of services effectuating Exchange Transactions for or on behalf of customers.

66. Subparagraph E(5)(b) defines the second type of “Investment Entity” as any Entity the gross income of which is primarily attributable to investing, reinvesting, or trading in Financial Assets or Relevant Crypto-Assets, if the Entity is managed by another Entity that is a Depository Institution, a Custodial Institution, a Specified Insurance Company, or an Investment Entity described in subparagraph E(5)(a). An Entity is ‘managed by’ another Entity if the managing Entity performs, either directly or through another service provider, any of the activities or operations described in subparagraph E(5)(a) on behalf of the managed Entity. However, an Entity does not manage another Entity if it does not have discretionary authority to manage the Entity’s assets (in whole or part). Where an Entity is managed by a mix of Financial Institutions and individuals or Entities other than Financial Institutions, the Entity is considered to be managed by another Entity that is a Depository Institution, a Custodial Institution, a Specified Insurance Company, or an Investment Entity described in subparagraph E(5)(a), if any of the managing Entities is such another Entity. For example, a private trust company that acts as a registered office or registered agent of a trust or performs administrative services unrelated to the Financial Assets, Relevant Crypto-Assets or money of the trust, does not conduct the activities and operations described in subparagraph E(5)(a) on behalf of the trust and thus the trust is not “managed by” the private trust company within the meaning of subparagraph E(5)(b). Also, an Entity that invests all or a portion of its assets in a mutual fund, exchange traded fund, or similar vehicle will not be considered “managed by” the mutual fund, exchange traded fund, or similar vehicle. In both of these examples, a further determination needs to be made as to whether the Entity is managed by another Entity for the purpose of ascertaining whether the first-mentioned Entity falls within the definition of Investment Entity, as set out in subparagraph E(5)(b).

67. An Entity is treated as primarily conducting as a business one or more of the activities described in subparagraph E(5)(a), or an Entity’s gross income is primarily attributable to investing, reinvesting, or trading in Financial Assets or Relevant Crypto-Assets for purposes of subparagraph E(5)(b), if the Entity’s gross income attributable to the relevant activities equals or exceeds 50% of the Entity’s gross income during the shorter of:

- the three-year period ending on 31 December of the year preceding the year in which the determination is made; or
- the period during which the Entity has been in existence.

68. For the purposes of the gross income test, all remuneration for the relevant activities of an Entity is to be taken into account, independent of whether that remuneration is paid directly to the Entity to which the test is applied or to another Entity.

69. The term “Investment Entity”, as defined in subparagraph E(5), does not include an Entity that is an Active Entity because it meets any of the criteria in subparagraphs D(11)(b) through (e).

70. An Entity would generally be considered an Investment Entity if it functions or holds itself out as a collective investment vehicle, mutual fund, exchange traded fund, private equity fund, hedge fund, venture capital fund, leveraged buy-out fund or any similar investment vehicle established with an investment strategy of investing, reinvesting, or trading in Financial Assets or Relevant Crypto-Assets. An Entity that primarily conducts as a business investing, administering, or managing non-debt, direct interests in real property on behalf of other persons, such as a type of real estate investment trust, will not be an Investment Entity.

71. Subparagraph E(5) also states that the definition of the term "Investment Entity" shall be interpreted in a manner consistent with similar language set forth in the definition of "financial institution" in the Financial Action Task Force Recommendations.

Subparagraphs E(6)-(15) – "Specified Insurance Company", "Governmental Entity", "International Organisation", "Central Bank", "Financial Asset", "Equity Interest", "Insurance Contract", "Annuity Contract", "Cash Value Insurance Contract" and "Cash Value"

72. The terms "Specified Insurance Company", "Governmental Entity", "International Organisation", "Central Bank", "Financial Asset", "Equity Interest", "Insurance Contract", "Annuity Contract", "Cash Value Insurance Contract", and "Cash Value" in subparagraphs E(6) through (15) should be interpreted consistently with the Commentary of the Common Reporting Standard, as amended.

Paragraph IV (F) – Miscellaneous

Subparagraph F(1) – Partner Jurisdiction

73. The term "Partner Jurisdiction" means any jurisdiction that has put in place equivalent legal requirements and that is included in a public list issued by [Jurisdiction].

Subparagraph F(2) – AML/KYC Procedures

74. The term "AML/KYC Procedures", as defined in subparagraph F(2), means the customer due diligence procedures of a Reporting Crypto-Asset Service Provider pursuant to the anti-money laundering or similar requirements to which such Reporting Crypto-Asset Service Provider is subject (e.g. know your customer provisions). These procedures include identifying and verifying the identity of the customer (including the beneficial owners of the customer), understanding the nature and purpose of the transactions, and on-going monitoring.

Subparagraph F(3) and (4) – Entity and Related Entity

75. Subparagraph F(3) defines the term "Entity" as a legal person or a legal arrangement. This term is intended to cover any person other than an individual (i.e. a natural person), in addition to any legal arrangement. Thus, e.g. a corporation, partnership, trust, *fideicomiso*, foundation (*fondation*, *Stiftung*), company, co-operative, association, or *asociación en participación*, falls within the meaning of the term "Entity".

76. An Entity is a "Related Entity" of another Entity, as defined in subparagraph F(4), if either Entity controls the other Entity, or the two Entities are under common control. For this purpose control includes direct or indirect ownership of more than 50% of the vote and value in an Entity. In this respect, Entities are considered Related Entities if these Entities are connected through one or more chains of ownership by a common parent Entity and if the common parent Entity directly owns more than 50% of the stock or other equity interest in at least one of the other Entities. A chain of ownership is to be understood as the ownership by one or more Entities of more than 50% of the total voting power of the stock of an Entity and more than 50% of the total value of the stock of an Entity, as illustrated by the following example:

Entity A owns 51% of the total voting power and 51% of the total value of the stock of Entity B. Entity B in its turn owns 51% of the total voting power and 51% of the total value of the stock of Entity C. Entities A and C are considered "Related Entities" pursuant to subparagraph F(4) of Section IV because Entity A has a direct ownership of more than 50% of the total voting power of the stock and more than 50%of total value of the stock of Entity B, and because Entity B has a direct ownership of more than 50% of the total voting power of the stock and more than 50% of total value of the stock of Entity C. Entities A and C are, hence,

connected through chains of ownership. Notwithstanding the fact that Entity A proportionally only owns 26% of the total value of the stock and voting rights of Entity C, Entity A and Entity C are Related Entities.

Subparagraph F(5) – Taxpayer Identification Number

77. According to subparagraph F(5), the term "TIN" means Taxpayer Identification Number (or functional equivalent in the absence of a Taxpayer Identification Number). A Taxpayer Identification Number is a unique combination of letters or numbers, however described, assigned by a jurisdiction to an individual or an Entity and used to identify the individual or Entity for purposes of administering the tax laws of such jurisdiction.

78. TINs are also useful for identifying taxpayers who invest in other jurisdictions. TIN specifications (i.e. structure, syntax, etc.) are set by each jurisdiction's tax administrations. Some jurisdictions even have a different TIN structure for different taxes or different categories of taxpayers (e.g. residents and non-residents).

79. While many jurisdictions utilise a TIN for personal or corporate taxation purposes, some jurisdictions do not issue a TIN. However, these jurisdictions often utilise some other high integrity number with an equivalent level of identification (a "functional equivalent"). Examples of that type of number include, for individuals, a social security/insurance number, citizen/personal identification/service code/number, and resident registration number; and for Entities, a business/company registration code/number.

80. In addition, some jurisdictions may also offer government verification services for the purpose of ascertaining the identity and tax residence of their taxpayers. Such government verification services are electronic processes made available by the jurisdiction to entities or individuals with third party reporting obligations (such as Reporting Crypto-Asset Service Providers) for the purposes of ascertaining the identity and tax residence of reportable persons (such as Crypto-Asset Users or their Controlling Persons). Where a tax administration opts for identification of Crypto-Asset Users or Controlling Persons based on an Application Programming Interface (API) solution, it would normally make an API portal accessible to Reporting Crypto-Asset Service Providers. Subsequently, if the Crypto-Asset User's or Controlling Person's self-certification indicates residence in that jurisdiction, the Reporting Crypto-Asset Service Provider can direct the Crypto-Asset User or Controlling Person to the API portal which would allow the jurisdiction to identify the Crypto-Asset User or Controlling Person based on its domestic taxpayer identification requirements (for example a government ID or username). Upon successful identification of the Crypto-Asset User or Controlling Person as a taxpayer of that jurisdiction, the jurisdiction, via the API portal, would provide the Reporting Crypto-Asset Service Provider with a unique reference number or code allowing the jurisdiction to match the Crypto-Asset User or Controlling Person to a taxpayer within its database. Where the Reporting Crypto-Asset Service Provider subsequently reports information concerning that Crypto-Asset User or Controlling Person, it would include the unique reference number or code to allow the jurisdiction receiving the information to enable matching of the Crypto-Asset User or Controlling Person. In this respect, a unique reference number, code or other confirmation received by a Reporting Crypto-Asset Service Provider in respect of a Crypto-Asset User or a Controlling Person via a government verification service is also a functional equivalent to a TIN.

81. Jurisdictions are expected to provide Reporting Crypto-Asset Service Providers with information with respect to the issuance, collection and, to the extent possible and practical, the structure and other specifications of taxpayer identification numbers and their functional equivalents. The OECD will endeavour to facilitate its dissemination. Such information will facilitate the collection of accurate TINs by Reporting Crypto-Asset Service Providers.

Subparagraph F(6) – Branch

82. The term "Branch" means a unit, business or office of a Reporting Crypto-Asset Service Provider that is treated as a branch under the regulatory regime of a jurisdiction or that is otherwise regulated under the laws of a jurisdiction as separate from other offices, units, or branches of the Reporting Crypto-Asset Service Provider. All units, businesses, or offices of a Reporting Crypto-Asset Service Provider in a single jurisdiction shall be treated as a single branch.

Commentary on Section V: Effective implementation

1. The CARF is built around the following key building blocks, designed to ensure the collection and automatic exchange of information on transactions in Relevant Crypto-Assets: (i) the scope of Crypto-Assets to be covered; (ii) the Entities and individuals subject to data collection and reporting requirements; (iii) the transactions subject to reporting as well as the information to be reported in respect of such transactions; and (iv) the due diligence procedures to identify Crypto-Asset Users and the relevant tax jurisdictions for reporting and exchange purposes.

2. For the CARF to deliver on its objectives, jurisdictions must ensure the correct implementation of each of these building blocks, such that they are complied with and that they are not circumvented. The aim of the Commentary on Section V is to describe these implementation requirements.

3. A jurisdiction should have in place a proportionate and risk-based comprehensive compliance strategy to ensure the effective implementation of the due diligence and reporting obligations in such jurisdiction, taking into account the jurisdiction's particular domestic context. This compliance strategy should address the following three main areas of focus. Firstly, a jurisdiction implementing the CARF should ensure the identification of all Entities and individuals that, by virtue of their activities, are Reporting Crypto-Asset Service Providers and have a nexus with such jurisdiction. Secondly, a jurisdiction should ensure that Reporting Crypto-Asset Service Providers accurately follow the reporting and due diligence procedures of the CARF. Finally, a jurisdiction should raise awareness of, and promote and enforce compliance with, the CARF. This should include a penalty framework to address instances of non-compliance, efforts to proactively promote and encourage compliance, as well as a compliance verification strategy to identify new practices that potentially pose high risks to the functioning of the CARF.

Ensuring the identification of all Reporting Crypto-Asset Service Providers

Potential challenges in identifying Reporting Crypto-Asset Service Providers

4. The nexus criteria of Section I will likely result in a broad range of Entities and individuals being considered Reporting Crypto-Asset Service Providers in a given jurisdiction. Among these, some Reporting Crypto-Asset Service Providers (e.g. Financial Institutions) are likely to be well-established actors in the traditional financial sector and are therefore likely aware of relevant regulatory and reporting requirements. However, many other Reporting Crypto-Asset Service Providers may be emerging actors less aware of such requirements. Depending on the jurisdiction, some of these emerging actors may currently be subject only to light or no regulation and therefore may not be identified by regulatory authorities. In addition, Reporting Crypto-Asset Service Providers with due diligence and reporting obligations as a result of having a place of business in, or being managed from, a jurisdiction may not regularly engage in activities that lend themselves to being easily identifiable to the jurisdiction.

5. Hence, a jurisdiction's compliance framework should consider the likelihood that some Reporting Crypto-Asset Service Providers with a nexus to the jurisdiction are not readily identifiable by such jurisdiction and may potentially not be aware of their due diligence and reporting obligations.

Potential approaches to ensure identification of Reporting Crypto-Asset Service Providers

6. To ensure identification of Reporting Crypto-Asset Service Providers in accordance with the requirements of Section I, jurisdictions should have mechanisms in place to identify Reporting Crypto-Asset Service Providers that have a nexus to their jurisdiction. As outlined below, these mechanisms may be included in an existing domestic regulatory framework, or a jurisdiction may need to design a new framework for this purpose.

7. In certain circumstances, a jurisdiction may rely on mechanisms already in place to identify Reporting Crypto-Asset Service Providers operating in its jurisdiction. For example, some jurisdictions may be able to rely on domestic regulatory frameworks already in place for other purposes (e.g. AML or financial markets registration requirements) to identify Reporting Crypto-Asset Service Providers. A jurisdiction that relies on an existing regulatory framework should first determine that such framework generally corresponds with the scope of the CARF, with respect to the different aspects of the Reporting Crypto-Asset Service Provider definition and the nexus rules, such that the domestic regulatory framework would ensure all individuals and Entities meeting the definition of Reporting Crypto-Asset Service Provider are identified.

8. If a jurisdiction determines that its domestic regulatory framework would not ensure the identification of certain or all Reporting Crypto-Asset Service Providers with a nexus to its jurisdiction, it should put in place additional mechanisms to ensure Reporting Crypto-Asset Service Providers with a nexus to its jurisdiction are identified. With respect to Reporting Crypto-Asset Service Providers whose only nexus with the jurisdiction is via its place of management or business, jurisdictions should take reasonable measures to ensure their identification.

9. There exist a number of examples of additional mechanisms, such as those described in this paragraph, that jurisdictions could adopt to identify Reporting Crypto-Asset Service Providers. For example, additional mechanisms for identifying all Reporting Crypto-Asset Service Providers, in particular those not already subject to registration or regulation, could include a requirement for Reporting Crypto-Asset Service Providers to proactively register with a domestic centralised registry. Jurisdictions could further consider imposing a nil reporting requirement on Reporting Crypto-Asset Service Providers. It could also be considered to establish a mechanism (e.g. an anonymous tip line or inbox) whereby information about non-compliant Reporting Crypto-Asset Service Providers could be reported to authorities. Furthermore, jurisdictions could consider introducing a requirement on their domestic Crypto-Asset Users to report, for instance in their tax returns, the name and address of the Reporting Crypto-Asset Service Providers they have used. This would allow tax authorities to identify Reporting Crypto-Asset Service Providers in either their own or a partner jurisdiction. Further coordination among partner jurisdictions may be necessary to ensure Reporting Crypto-Asset Service Providers operating in a cross-border context are identified. To that end, when a jurisdiction has reason to believe that a Reporting Crypto-Asset Service Provider with a nexus to another jurisdiction is not identified as such, it could rely on mechanisms foreseen in the competent authority agreements for the exchange of information pursuant to the CARF. Finally, jurisdictions could consider relying on publicly available resources, such as market research portals, to determine Reporting Crypto-Asset Service Providers with a nexus to their jurisdiction. The sufficiency of any additional mechanisms, combined with the domestic regulatory framework, would need to be evaluated in their totality. Jurisdictions that need additional mechanisms should ensure that the mechanism or mechanisms chosen are sufficiently robust as to achieve the objective of identifying Reporting Crypto-Asset Service Providers with a nexus to such jurisdiction.

Ensuring compliance of Reporting Crypto-Asset Service Providers with their due diligence and reporting requirements

10. Once a jurisdiction has identified Reporting Crypto-Asset Service Providers with due diligence and reporting obligations in such jurisdiction, the jurisdiction should ensure that such Reporting Crypto-Asset Service Providers continue to comply with the reporting and due diligence procedures in Sections II and III for as long as such obligations exist. To this end, a jurisdiction should designate one or more administrative bodies as responsible for ensuring, on the basis of a proportionate and risk-based compliance strategy, compliance of Reporting Crypto-Asset Service Providers with their due diligence and reporting obligations under Sections II and III.

Designated administrative bodies with powers to verify compliance of Reporting Crypto-Asset Service Providers

11. As an initial step, jurisdictions should designate one or more administrative bodies (e.g. a tax authority or financial supervisor), with the power to verify the compliance of Reporting Crypto-Asset Service Providers with the due diligence and reporting obligations in such jurisdiction. Jurisdictions should also ensure that any such designated bodies are adequately resourced to properly verify compliance of Reporting Crypto-Asset Service Providers with their due diligence and reporting requirements. A jurisdiction could also consider making use of alternative mechanisms that reduce burdens on domestic authorities' resources, to the extent such mechanisms are reliable for verifying the compliance of Reporting Crypto-Asset Service Providers (e.g. relying on other government departments or agencies or third-party service providers to verify that Reporting Crypto-Asset Service Providers comply with their due diligence and reporting requirements), provided the domestic authorities remain accountable.

12. To ensure that the domestic authorities can verify Reporting Crypto-Asset Service Providers' compliance, a jurisdiction should have rules in place requiring Reporting Crypto-Asset Service Providers with due diligence and reporting obligations in such jurisdiction to keep records of the steps undertaken and any evidence relied upon for the performance of the due diligence procedures set out in Section III, as well as for the classification of Relevant Transactions, Crypto-Assets and Relevant Crypto-Assets set out in Section IV.

13. Jurisdictions should have rules in place to compel the taxpayer or a third party to provide documents that are necessary to apply their domestic tax legislation. These rules should also apply to obtain information to respond to a request for information from an exchange partner under an exchange of information instrument. A jurisdiction should also have in place adequate measures to ensure the records of Reporting Crypto-Asset Service Providers with respect to the due diligence and reporting obligations in such jurisdiction are made available**,** upon request, to its domestic authorities in order for these authorities to carry out compliance reviews.

Verification issues related to reporting requirements under the CARF

14. A jurisdiction should verify whether Reporting Crypto-Asset Service Providers with due diligence and reporting obligations in such jurisdiction have complied with the requirements of Section II. This includes ensuring the Reporting Crypto-Asset Service Provider has correctly reported the information to the tax authority (or other appropriate authority) of the jurisdiction in a timely manner.

15. As a general matter, the reporting requirements of Section II are conditioned on a Reporting Crypto-Asset Service Provider's classification of Crypto-Assets. Notably, the CARF contains a number of exemptions relieving Reporting Crypto-Asset Service Providers from reporting obligations with respect to Crypto-Assets that cannot be used for payment or investment purposes, Specified Electronic Money Products and Crypto-Assets that are Central Bank Digital Currencies. Jurisdictions should therefore verify

that Reporting Crypto-Asset Service Providers correctly apply the definitions contained in Section IV with respect to Relevant Crypto-Assets.

16. Certain Transfers effectuated by Reporting Crypto-Asset Service Providers may also require additional scrutiny. For example, a jurisdiction may identify that Reporting Crypto-Asset Service Providers, individuals, Entities or merchants seek to fragment transaction amounts, such as retail sales amounts, to avoid reporting obligations with respect to transactions that otherwise meet the definition of Reportable Retail Payment Transactions. In such case, the jurisdiction should ensure that such transactions are treated as Reportable Retail Payment Transactions and reported as such.

Verification issues related to due diligence requirements under the CARF

17. In addition to the verification of compliance with reporting requirements, a jurisdiction should also verify whether Reporting Crypto-Asset Service Providers with due diligence and reporting obligations in such jurisdiction have complied with the due diligence requirements set out in Section III. Such verification should, in particular, ensure that Reporting Crypto-Asset Service Providers complete the collection and validation of self-certifications for Crypto-Asset Users and Controlling Persons in an accurate and timely manner. It is recognised that, depending on the status of a jurisdiction's domestic implementation of the FATF Recommendations pertaining to virtual asset service providers, it may arise that a Reporting Crypto-Asset Service Provider is not considered an AML-obliged person in the jurisdiction where it is subject to the reporting and due diligence obligations of Sections II and III. Section III.B(2)(a) clarifies that if a Reporting Crypto-Asset Service Provider is not legally required to apply AML/KYC Procedures that are consistent with the 2012 FATF Recommendations (as updated in June 2019 pertaining to virtual asset service providers), it should apply substantially similar procedures for the purpose of determining the Controlling Persons. Where a Reporting Crypto-Asset Service Provider is required to apply such substantially similar procedures, the jurisdiction should verify and ensure that such procedures are consistent with the requirements for purposes of identifying Controlling Persons.

Raising awareness of, and promoting and enforcing compliance with, the CARF

18. Jurisdictions should have in place effective measures to raise awareness of, and promote compliance with the due diligence and reporting obligations in such jurisdiction. Accordingly, jurisdictions should take appropriate measures aimed at ensuring that Reporting Crypto-Asset Service Providers in their jurisdiction are made aware of the nexus, due diligence and reporting requirements in the jurisdiction's laws. Jurisdictions should also make available to Reporting Crypto-Asset Service Providers in their jurisdiction the necessary information.

19. Jurisdictions should also have in place enforcement provisions to address instances of non-compliance and should have the ability to impose adequate administrative and/or criminal penalties on Reporting Crypto-Asset Service Providers for failure to comply with the reporting and due diligence procedures in Sections II and III, as well as for failure to respond to requests from authorities.

20. Jurisdictions should also have in place strong measures to ensure valid self-certifications are always collected for Crypto-Asset Users and Controlling Persons. What will constitute a "strong measure" in this context may vary from jurisdiction to jurisdiction and should be evaluated in light of the actual results of the measure. The crucial test for determining what measures can qualify as "strong measures" is whether the measures have a strong enough impact on Crypto-Asset Users, Controlling Persons and/or Reporting Crypto-Asset Service Providers to effectively ensure that self-certifications are obtained and validated in accordance with the rules set out in the CARF. An effective way to achieve this outcome would be to introduce legislation making the effectuating of transactions conditional upon the receipt of a valid self-certification. Other jurisdictions may choose different methods, taking into account their domestic law. This could include, for example, imposing significant penalties on Crypto-Asset Users and Controlling Persons that fail to provide a self-certification, or on Reporting Crypto-Asset Service Providers that do not

take appropriate measures to obtain a self-certification. Beyond administrative measures and penalties, strong measures could also include a requirement to apply a withholding tax on transactions conducted in the absence of a valid self-certification. Furthermore, to increase the reliability of self-certifications, jurisdictions should have a specific provision in their domestic legislation imposing sanctions for signing (or otherwise positively affirming) a false or materially incorrect self-certification.

21. In addition to enforcement provisions for dealing with instances of non-compliance, jurisdictions should seek to identify any practices which, based on the domestic context, potentially threaten the effectiveness of the due diligence and reporting obligations in such jurisdiction and take appropriate compliance measures in response. In particular, a jurisdiction should have rules to prevent any Reporting Crypto-Asset Service Providers, persons or intermediaries from adopting practices intended to circumvent the due diligence and reporting obligations in such jurisdiction. Examples of other actions a jurisdiction could take include considering whether risks resulting from the highly mobile nature of the Crypto-Asset market justify additional measures if it identifies that Reporting Crypto-Asset Service Providers in its jurisdiction are carrying out cross-border Crypto-Asset transactions in jurisdictions that are not Partner Jurisdictions, with the intention of avoiding reporting requirements under its legislation. Similarly, a jurisdiction could consider whether those parts of the Crypto-Asset market that have a decentralised nature (e.g. decentralised finance platforms) pose particular risks in its domestic context if it identifies that Entities or individuals falsely claim not to be a Reporting Crypto-Asset Service Provider even though they in fact exercise control or sufficient influence over a trading platform effectuating Exchange Transactions.