Electronic Money Association
Surbiton, Surrey, KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

Organisation for Economic Co-operation and Development

By email taxpublicconsultation@oecd.org

29 April 2022

Dear Sir/Madam

Re: Consultation concerning a new global tax transparency framework to provide for the reporting and exchange of information with respect to crypto-assets, as well as proposed amendments to the Common Reporting Standard (CRS) for the automatic exchange of financial account information between countries.

We welcome the opportunity to provide input to the OECD consultation paper ("Consultation") on a new global tax transparency framework and amendments to the CRS. The EMA represents Payments, FinTech, and crypto asset firms engaging in the provision of innovative digital payment services.

Our members include leading payments and e-commerce businesses providing online payments, card-based products, open banking, electronic marketplaces, and increasingly cryptocurrency exchanges and other cryptocurrency related products and services.

The EMA has been active for over 20 years, and has a wealth of experience regarding the regulatory framework for payments and FinTech services. A list of current EMA members is provided at Annex 1 to this document.

We have addressed issues relating to CRF in section 1-4 of our response and to specified electronic money products in section 5.

We would be grateful for your consideration of our comments, which are set out below.

Yours faithfully

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA Response to Consultation:

I CRYPTO-ASSET REPORTING FRAMEWORK QUESTIONS

1. Crypto-Assets in scope

1.1. Question 1: Does the CARF cover the appropriate scope of Crypto-Assets? Do you see a need to either widen or restrict the scope of Crypto-Assets and, if so, why?

Response

1.1.1. We are of the view that the scope of what CARF considers as crypto assets is too broad, and it is appropriate to restrict the scope.

1.1.2. The CARF definition of crypto assets ("a digital representation of value that relies on a cryptographically secured distributed ledger or a similar technology to validate and secure transactions") is extremely broad, particularly compared with FATF's definition ("a digital representation of value *that can be digitally traded, or transferred, and can be used for payment or investment purposes*").

1.1.3. The proposed scope may mean products which are not intended to be captured are included in scope, such as those which may not function as a payment or an investment asset.

1.1.4. We suggest **introducing the narrower FATF definition** for closer alignment and to avoid the capture of products that are not intended to be in scope.

1.2. Question 2: Does the definition of Closed-Loop Crypto-Assets contain the correct criteria for identifying Crypto-Assets that operate in a closed-loop environment?

Response

1.2.1. The criteria for Closed-Loop crypto assets is:
a) is issued as a means of payment with Participating Merchants for the purchase of goods or services;
b) can only be transferred by or to the issuer or a Participating Merchant; and
c) can only be redeemed for Fiat Currency by a Participating Merchant redeeming with the issuer.

1.2.2. The criteria appear to cover most limited network implementations, provided the issuer does not allow users to redeem the token directly. This limits however the ability of tokens being exchanged for other similar tokens, as may be the case of the equivalent non crypto loyalty products, and may place such products at a disadvantage in this respect.

1.2.3. We suggest additionally allowing such products to be exchangeable independently from the issuer for products of a similar type. This will increase the value of loyalty products to their users and enable loyalty product issuers to increase the utility of the tokens as an incentive product. An example would be enabling air miles issued by an airline to be exchanged for store tokens issued by a particular merchant or for airmiles issued by another airline, where they have a joint agreement. This stops short of allowing such tokens to be freely exchangeable for all tokens or for fiat currency.

1.3. Question 3: Are you aware of existing types of Crypto-Assets, other than Closed-Loop Crypto Assets or Central Bank Digital Currencies that present a low risk from a tax compliance perspective and should therefore be excluded from the scope?

Response

1.3.1. Yes, security tokens that are already subject to regulation as a financial asset will fall under CRS and there is little merit in being addressed again under CARF.

1.3.2. Products that would not be captured under the FATF definition which excludes products not utilised as a payment or an investment also merit exclusion. One class of such assets are NFTs, and particularly those that are issued in a non professional manner and which circumscribe common activities of hobbyists, artists, musicians and ordinary users. This is addressed in our response to Question 4 below.

1.3.3. Please also see our response to Question 1 above regarding the different scope of what the OECD and FATF consider as a crypto asset.

1.4. Question 4: An NFT is in scope of the FATF Recommendations as a virtual asset if it is to be used for payment or investment purposes in practice. Under the Crypto-Asset Reporting Framework, an NFT would need to represent value and be tradable or transferable to be a Crypto-Asset. On that basis it is expected that relevant NFTs would generally be covered under both the CARF (as a Crypto-Asset) and the FATF Recommendations (either as a virtual asset or a financial asset). Are you aware of any circumstances where this would not be the case, in particular, any NFTs that would be covered under the definition of Crypto-Assets and that would not be considered virtual assets or financial assets under the FATF Recommendations or vice versa?

Response

1.4.1. The proposed criteria of which NFTs are classified as crypto assets ("an NFT would need to represent value and be tradable or transferable to be a Crypto Asset") is very broad, and in its current guise may capture the entire range of NFTs.

1.4.2. This will include personal collectibles which may "represent value and be tradeable" by definition but are not financial service products; they could be produced by artists, musicians and may be exchanged by minors as well as non professionals and hobbyists. We urge caution here, as CDD and data reporting obligations are not likely to be appropriate in such circumstances. The definition of NFTs here also goes beyond FATFs definition, which only classifies an NFT as a virtual asset "if it is used for payment or investment purposes in practise". We propose that the definition is amended to align with FATF's definition of NFTs, and that a distinction is made between NFTs used for payment or investment purposes and others.

1.4.3. The FATF Virtual Asset Guidance of 2019 states the following:

> 53. Digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, can be referred to as a non-fungible tokens (NFT) or crypto-collectibles. Such assets, depending on their characteristics, are generally not considered to be VAs under the FATF definition. However, it is important to consider the nature of the NFT and its function in practice and not what terminology or marketing terms are used.

1.4.4. It is clear that a considerable is not the majority of products that meet the definition of NFTs are not intended to be captured by the FATF definition. This merits consideration under CRS, particularly as set out above, the consequences of collecting CDD information on minors, hobbyists, ordinary individuals creating NFTs etc. is overwhelmingly onerous and disproportionate.

1.4.5. It may be appropriate to allow the market to develop before updating the standards in relation to NFTs, finding the appropriate perimeter based on more mature market practices. If this is not accepted, then a monetary threshold is appropriate to restrict what is captured to a reasonably high limit.

2. Intermediaries in scope

2.1. Question1: Do you see a need to either widen or restrict the scope of the intermediaries (i.e. Reporting CryptoAsset Service Providers)?

Response

2.1.1. Intermediaries proposed by the consultation text to be in scope are:

- Intermediaries facilitating exchanges between Crypto-Assets;
- Intermediaries facilitating exchanges between Crypto-Assets and Fiat Currencies;
- Intermediaries providing exchange services such as brokers and dealers in Crypto-Assets;
- Operators of Crypto-Asset ATMs; and
- Decentralised exchanges and decentralised finance more broadly.

2.1.2. The proposed scope of intermediaries is quite broad and may capture intermediaries which are not intended to be captured, such as merchant acquirers, service providers to intermediaries and those intermediaries who do not deal with retail clients but only with other intermediaries. This may create reporting obligations for entities that may not have a customer relationship.

2.1.3. Intermediaries who provide technical services to enable exchanges between crypto assets should be deemed out of scope, similar for example to PSD 2, which excludes technical service providers from the scope of payment services regulation.

2.2. Question 2: Are there any circumstances in which multiple (affiliated or unaffiliated) Reporting Crypto-Asset Service Providers could be considered to effectuate the same Relevant Transaction with respect to the same customer? If so, which types of intermediaries (e.g. the one with the closest relationship with the client) would be best placed to ensure reporting?

Response

2.2.1. We concur that the CASP with the closest relationship with the customer in relation to either acquiring or disposing of the crypto asset should be responsible for reporting, as they would hold the relevant customer due diligence information under AML/KYC. This means that other intermediaries should not have to make such reports and a means for establishing the reporting entity should be developed.

2.3. Question 3: Do the nexuses described in paragraph A of Section I of the CARF ensure a comprehensive coverage of all relevant Reporting Crypto-Asset Service Providers? If not, under what circumstances would relevant Reporting Crypto-Asset Service Providers not have a nexus in any jurisdiction? In your view, should this be a potential concern, and if so, what solutions could be considered to address it?

Response

2.3.1. Reporting Crypto-Asset Service Providers will, in principle, be subject to the rules when they are
(i) tax resident in,
(ii) both incorporated in, or organised under the laws of, and have legal personality or are subject to tax reporting requirements in,
(iii) managed from,
(iv) disposing of a regular place of business in, or
(v) effectuating Relevant Transactions through a branch based in, a jurisdiction adopting the rules.

2.3.2. We are of the view that a reportable CASP not having a nexus in any jurisdiction may indeed be a potential concern, though we have not identified any circumstances of this occurring at this time.

2.3.3. We do have some concern over the scope of paragraph (iii) which may be interpreted very broadly and would therefore benefit from additional clarification. Does management refer to overall seat of management of the business, or does the presence of any member of the management in a particular jurisdictions trigger nexus? We would support the former but question the merits of the latter.

3. Reporting requirements

3.1. Question 1: Do intermediaries maintain valuations on the equivalent Fiat Currency fair market values of CryptoAssets? Do you see challenges in reporting on the basis of such fair market value? If yes, what do you suggest to address them?

3.1.1. We understand that some intermediaries, such as crypto exchanges, do maintain a Fiat Currency value for crypto assets. However, intermediaries who are technical service providers and do not as deal with consumer transactions do not maintain a Fiat Currency value.

3.1.2. For those specific intermediaries who do not maintain Fiat Currency value, it may be a challenge to report on such fair market value, particularly because not all crypto transactions are tied to a corresponding fiat currency.

3.2. Question 2: Are there preferable alternative approaches to valuing Relevant Transactions in Crypto-Assets?

3.2.1. We have not provided a response to this question.

3.3. Question 3: Are there specific difficulties in applying the valuation rules for illiquid tokens, for example, NFTs or other tokens that may not be listed on a marketplace, to identify a fair market value? If so, please provide details of any preferable valuation methods that could be adopted within the CARF.

Response

3.3.1. It may not be possible to apply the valuation rules to illiquid tokens. In such circumstances, a potential solution could be to use the 'last known value' or 'last traded value' to determine the fair market value.

3.4. Question 4: Regarding Reportable Retail Payment Transactions, what information would be available to Reporting Crypto-Asset Service Providers pursuant to applicable AML requirements (including the FATF travel rule, which foresees virtual asset service providers collecting information on originators and beneficiaries of transfers in virtual assets) with respect to the customers of merchants in particular where the customer does not have a relationship with a Reporting Crypto-Asset Service Provider, for whom it effectuates Reportable Retail Payment Transactions? Are there any specific challenges associated with collecting and reporting information with respect to Reportable Retail Payment Transactions? What measures could be considered to address such challenges? Would an exclusion of low-value transactions via a de minimis threshold help reducing compliance burdens? If so, what would be an appropriate amount and what measures could be adopted to avoid circumvention of such threshold by splitting a transaction into different transactions below the threshold?

Response

3.4.1. The proposal to require Reporting Crypto Asset Service Providers to report transactions relating to the purchase of goods and services is in our view disproportionate and contrary to the treatment of other means of payment. There are no other circumstances where transactions for the purchase of goods and services are reportable in the financial services space, and we strongly discourage the OECD from adopting this requirement.

3.4.2. The disproportionate nature is then accentuated by the fact that the customers whose transactions are being reported have no business relationship with the Reporting entity, and their identity is not known. It is our view that given that transfers of crypto assets are reportable by the reporting entity, there is little additional value to be gained from tracking purchases of goods and services, and the additional compliance cost will discriminate against the use of crypto assets for payments, in favour of fiat currency.

3.4.3. It is expected that in the medium term, stable coins will be more widely available for making payment transactions, and these will have non discernible capital gains attached to them resulting in little value from tracking payment transactions. We propose that this element of the reporting obligations be reviewed and its merits be reconsidered.

3.4.4. In the event that this persists, then a threshold is essential, and for this to be set at a sufficiently high value as to make such transactions non-reportable except in the most extreme of cases.

3.4.5. Circumvention of thresholds by using lower values is always visible to the receiving Reporting entity, and can be reported as a suspicious activity report where this takes place.

3.5. Question 5: Concerning the requirement to report transfers based on certain pre-defined transfer types (e.g. hardforks, airdrops due to other reasons, loans or staking), do Reporting Crypto-Asset Service Providers have the knowledge necessary to identify, and classify for reporting purposes, transfers effectuated according to such transfer types? Are there any other transfer types that typically occur and that are separately identified for customers or for other purposes?

Response

3.5.1. To our knowledge, Reporting CASPs may not have the knowledge necessary to identify, classify and report certain transfers such as hard forks and airdrops.

3.5.2. It would also be difficult to track this information account by account, as once the assets are deposited to a customers account, they would be commingled. There is not a notation that certain funds are from an air drop or from a hard fork – the funds are mixed with other assets procured through activities such as trading.

3.5.3. CASPs also may not be able to track gains made by a customer on the ownership of a particular asset – as the same token can be received in multiple ways. For examples, it could be transferred in from an external wallet, in which case the CASP has no way of determining the original purchase price.

3.6. Question 6: Concerning the proposal for reporting with respect to wallet addresses, are there any specific challenges for Reporting Crypto-Asset Service Providers associated with the proposed requirement to report wallet addresses that are the destination of transfers sent from a customer's wallet maintained by a Reporting Crypto-Asset Service Provider? Do Reporting

Crypto-Asset Service Providers have, or are they able to obtain, information to distinguish wallet addresses associated with other Reporting Crypto-Asset Service Providers from wallet addresses that are not associated with another Reporting Crypto-Asset Service Provider? The OECD is also considering to require, in addition, reporting with respect to wallet addresses that are the origins of transfers to a customer's wallet maintained by a Reporting Crypto-Asset Service Provider. Is this information available and would providing it materially increase compliance burdens for Reporting Crypto-Asset Service Providers? Are there alternative requirements (e.g. reporting of the public keys associated with Crypto-Asset Users instead of wallet addresses) that could be considered to more efficiently increase visibility over transactions carried out without the intervention of the Reporting Crypto-Asset Service Provider?

Response

3.6.1. To our knowledge, Reporting CASP's do generally have access to information such as wallet addresses that are the destination of transfers sent from a customer's wallet maintained by a Reporting Crypto-Asset Service Provider and thus can report it.

3.6.2. Regarding the determination as to whether the recipient account or wallet is associated with another Reporting CASP, this may not always be possible to determine

3.7. Question 7: Information pursuant to the CARF is to be reported on an annual basis. What is the earliest date by which information on the preceding year could be reported by Reporting Crypto-Asset Service Providers?

Response

3.7.1. We agree with the proposal that information pursuant to the CARF should be reported on an annual basis, and that it will be reporting in the following year after which the transactions have been undertaken. This will help to provide Reporting CASPs with requisite time to collect and classify such information.

3.7.2. Regarding the earliest reporting date, we are of the view that it would be beneficial for the reporting schedule of CARF to align with the existing CRS reporting date.

4. <u>Due diligence procedures</u>

4.1. Question 1: The due diligence procedures of the CARF are in large part based on the CRS. Accordingly, the CARF requires Reporting Crypto-Asset Service Providers to determine whether their Entity Crypto-Asset Users are Active

Entities (corresponding largely to the definition of Active NFE in the CRS) and, on that basis, identify the Controlling Persons of Entities other than Active Entities. Would it be preferable for Reporting Crypto-Asset Service Providers to instead document the Controlling Persons of all Entity Crypto-Asset Users, other than Excluded Persons? Are there other elements of the CRS due diligence procedures that should be included in the CARF to ensure that Reporting Financial Institutions that are also Reporting Crypto-Asset Service Providers can apply efficient and consistent due diligence procedures?

Response

4.1.1. We believe existing proposal for due diligence procedures of the CARF to be in large part based on the CRS are sufficient. It also sets a level playing field with other categories of reporting entities.

4.1.2. As such, it follows that this proposal would be preferable to the alternative which would require Reporting CASPs having to document the controlling persons of all entity crypto asset users other than Excluded Persons.

4.1.3. Similarly, existing CDD information provided by customers should be acceptable and should not require recertification unless there is a change in circumstances or other CDD related engagement with the customer.

4.1.4. Consistency between the CARF and CRS rules should be maintained wherever possible.

4.2. Question 2: An Entity Crypto-Asset User qualifies as an Active Entity if less than 50% of the Entity's gross income is passive income and less than 50% of the assets held by the Entity produce, or are held for the production of, passive income. The Commentary on the term "Active Entity" provides that passive income includes "income derived from Relevant Crypto-Assets". Are there any specific instances in which such income (e.g. income from mining, staking, forks or airdrops) should qualify as active income?

Response

4.2.1. From the examples mentioned above, it is our view that mining may qualify as active income, but this would not be the case for staking, forks, or airdrops. It requires the user to undertake on-going action to mine and earn income through utilisation of computer software.

4.2.2. Staking may be considered as being similar, but the key distinction is that there is no on-going, active action required – the customer stakes their assets to earn rewards, and there is no subsequent activity on their part.

4.3. Question 3: The CARF removes the information collection and reporting obligations with respect to Crypto-Asset Users which are Excluded Persons. The OECD is still considering whether Reporting Crypto-Asset Service Providers should be included in the definition of Excluded Persons. Against this background, would Reporting Crypto-Asset Service Providers have the ability to obtain sufficient information on clients that are Reporting Crypto-Asset Service Providers to verify their status?

Response

4.3.1. It is customary in the regulated sector for transactions between regulated entities acting on their own account to be excluded from regulation. This As the OECD is still considering whether Reporting CASPs should be included in the definition of Excluded Persons, we are of the view that this may be beneficial, and Reporting CASPs should be excluded in circumstances such as them being subject to regulation or registration with a financial authority (similar to FI under CRS).

4.4. Question 4: Section III.D enumerates effective implementation requirements in instances where a Reporting Crypto-Asset Service Provider cannot obtain a self-certification from a Crypto-Asset User or Controlling Person. Notably, these requirements specify that the Reporting Crypto-Asset Service Provider must refuse to effectuate any Relevant Transactions on behalf of the Crypto-Asset User until such self-certification is obtained and its reasonableness is confirmed. Are there potential alternative effective implementation measures to those listed in Section III.D? If so, what are the alternative or additional effective implementation measures and which persons, or Entities would be best-placed to enforce such measures?

Response

4.4.1. We are broadly in agreement, and this approach is consistent with the approach for money laundering under Recommendation 10 of the FATF Forty Recommendations. In order to address exceptional circumstances and to ease the transition to the CARF regime, some risk based time allowance may be appropriate, beyond which the Reporting entity would be required not to execute any further transactions.

4.4.2. Regarding the requirements to renew self-certifications, we would propose that unless there is a material change, self-certifications should remain valid indefinitely. This would ease the burden on Reporting CASPs to collect and report such information periodically.

II AMENDMENTS TO THE COMMON REPORTING STANDARD QUESTIONS

5. Specified Electronic Money Products

5.1. **Question 1: taking into account that the definition of "Specified Electronic Money Product" aims to cover products that do not give rise to gain or loss by reference to the underlying fiat currency, would the proposed definition cover the correct e-money products and be practically implementable? Do you see a need to either widen or restrict the scope or amend the criteria? If so, why and in which manner?**

Response:

5.1.1. Section VIII A of the CRS is proposed to be amended to introduce the new definition of specified electronic money products at paragraph A 9 which provides that:

"9. The term "Specified Electronic Money Product" means any product 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 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."

5.1.2. Additionally, depository accounts are proposed to be amended to include accounts holding Specified Electronic Money, and depository institutions broadened to include issuers of specified electronic money.

5.1.3. **Exemptions from scope** have also been provided for electronic money products that solely **facilitate funds transfers**, and those that fall **below a threshold** balance value, which we have addressed further at paragraphs 5.2.12-5.2.19 below. We have additionally proposed exemption for products that amount to a '**limited network' –** see paragraph 5.1.10.

5.1.4. The standards seek to capture products that enable the creation of a store of value, that is repayable on demand, and thereby may be of interest to tax authorities. The proposed definition seeks to capture such products, requiring that e-money be issued on receipt of funds (paragraph (b)), in other words to be prepaid and creating a store of value. Other limbs of the definition act to inform on the scope of products that are captured.

5.1.5. The definition distinguishes between prepayments that may be made to a single supplier of goods or services (for example gift cards) and prepayment products that act as a more general means of payment. This is set out at paragraph (d) which requires acceptance of the value in payment by third parties other than the issuer. The inclusion of this limb of the definition is significant and supported.

5.1.6. We do suggest however the addition of the words 'in payment' after 'accepted' in paragraph (d) to reinforce the function of such products.

5.1.7. We also note the provisions of paragraph (e) which require that the prepaid balance is redeemable for fiat currency and at par. This is also a key provision that requires the products to be a store of value that can be exchanged back for bank funds. It is only such products that can give rise to the type of risk of tax evasion that is contemplated. It is also a common requirement of the regulatory regimes that govern such products, to our knowledge, on a global basis.

5.1.8. The CRS electronic money definition is thus closely aligned with the regulated definition for prepaid payment products or electronic money that are adopted in jurisdictions globally. This is helpful as entities falling within the scope of reporting obligations are more likely to be subject to financial services regulation and thus under other reporting and CDD provisions that will facilitate compliance with the CRS.

5.1.9. There are a group of products that are exempt from regulation because they more closely resemble prepayment for goods and services purchased from a single merchant, than they do a widely accepted payment product. Such products are sometimes described as providing payment services within a 'limited network'. Such limited networks may reflect a geographic limitation, a limitation on the number of merchants participating or the range of goods and services that can be purchased.

5.1.10. These products are usually associated with low value payments, and we believe merit exemption from the scope of CRS. In the absence of such exemption, a reasonable exemption threshold for e-money products more generally, would also serve as a risk based solution for this type of product. We have addressed the need for a threshold more fully in our response to question 2 below.

5.2. Question 2: what would in your view be the appropriate account balance threshold to exclude low-risk e-money products from the scope of the CRS and why? Are there any alternative criteria to define low-risk e- money products?

Response:

5.2.1. There are multiple reasons for the establishment of a balance threshold for the application of CRS obligations to e-money products; these vary from the limited purpose of e-money products, to the need to implement a risk based approach to AML compliance for e-money, and to fulfilling policy objectives in relation to financial inclusion. We have set out these arguments previously, and provide an elaboration of these issues in the paragraphs that follow.

5.2.2. **Specific uses** for e-money: unlike bank accounts which have been suggested as a comparator, the vast majority of e-money products are used for very specific purposes and with the exception of financial inclusion types of services, they are not used for day to day transactions. Consequently, users are not prepared to provide the kind of data that is required under the CRS at onboarding. Data relating to place of birth, country of residence, TIN etc. are regarded as overly intrusive requirements when seeking to open a limited purpose account or to purchase a prepaid card. This request becomes a barrier to entry once the e-money issuer then attempts to verify such information and may demand

documents or access to data that would be disproportionate to the purpose and characteristics of the e-money product.

5.2.3. The impact of such requests is observed in significant rates of abandonment at onboarding, and a shard drop in product take-up. This has been observed to be in the region of 25-50% by various issuers depending on the extent of data that is required, and the degree of verification that is implemented.

5.2.4. **A risk based approach** is far more preferable in such circumstances, where data elements and means of verification are applied on a risk sensitive basis. This involves requesting a minimum amount of information at the outset, and seeking more information and verifying such additional information when the risk posed by the customer and the product increase, and justify this burden.

5.2.5. This has **twin benefits**, the first is to ensure minimal friction at the point of onboarding, providing customers with access to regulated payment services, which are also subject to risk based balance and transaction limits. Secondly, it enables a greater allocation of business resources to those customers or products that pose a more significant risk of money laundering or other financial crime, including tax evasion. The risk based approach results in more effective outcomes that identify and deter financial crime.

5.2.6. **Simplified due diligence** ("SDD") is the process by which the risk based approach is applied to the customer due diligence process and which is predicated on the risk of money laundering and other financial crime being assessed as low, enabling a lower degree of customer due diligence to be applied within specific product constraints.

5.2.7. This is widely adopted in the e-money and payments industry for the reasons set out in the previous paragraphs. It is also a key part of the FATF regime and of FATF member countries' AML regimes, enabling a better allocation of resources through this risk-based approach.

5.2.8. **SDD** could not be applied to e-money users if CRS CDD obligations were to apply simultaneously, and without a reasonable threshold. CRS makes extensive demands on the elements of identity that must be collected and the degree of verification that must be applied that exceed those of SDD. A threshold is therefore necessary to enable SDD to continue to be applied below this threshold. This is key, and essential to the continued application of SDD under the risk based approach.

5.2.9. As set out at paragraph 5.2.2, e-money products also play a key part in economic development in developing and/or emerging countries. Parts of the population may have little access to traditional bank products because they live in remote rural areas without sufficient infrastructure. E-money or e-wallets enable access to electronic payments, enable participation in online commerce and in many instances are utilised for the distribution of aid.

5.2.10. Another instance is in enabling salary payments to be made electronically to migrant workers (such as construction workers for example), paying wages into e-wallets, and in circumstances where migrant workers may not be permitted access to bank accounts under local law. In all such instances, e-money and e-wallets are a significant means of economic and financial inclusion.

5.2.11. In all such cases, the range of CRS identity information will not be available, and there will also be limited means of verifying such information. It would be appropriate in such circumstances to offer a reasonably calibrated threshold that would enable this and other e-money products to continue to be offered to users.

5.2.12. **A threshold** that is based on the value of the balance of funds held in an e-money account is regarded as the most effective means of defining a threshold, as transaction volume does not provide a measure of the risk of funds being sheltered, but rather a measure of payments being made. The balance metric is also that which is measured for CRS reporting purposes.

5.2.13. **The value of the threshold** needs to accommodate the competing needs of product take-up, of customers' reasonable expectations of data that would be shared, of the need to apply SDD, of implementing a risk-based approach and finally, and significantly, of financial inclusion.

5.2.14. This **value** needs to be relevant for the full range of product propositions, it needs to continue to be appropriate for a number of years whilst the CRS is implemented, put into practice, and to represent a balance between business needs and legitimate tax authority concerns.

5.2.15. Furthermore, a threshold that is too low in value will result in a negative cost-benefit analysis, as large numbers of customers are made to submit data, to have it verified, at a significant time and resource expenditure, but resulting in limited qualifying reports.

5.2.16. Industry believes **an appropriate threshold** may be in the region of **USD 10,000**, providing a practical and yet low value that tax authorities may benefit from tracking.

5.2.17. This limit would be **subject to the aggregation rule**, and would represent the total value held by any customer with an e-money issuer.

5.2.18. The limit would apply where the e-money balance does not exceed the threshold of USD 10,000, calculated as the average end-of-day balance in any calendar month. This reflects the need to capture residual storage of value rather than the execution of individual transactions. If not technically feasible, then a daily balance calculation must be adopted by issuers.

5.2.19. We concur with the proposed exclusion for e-money products where value is only held in order to enable the execution of fund transfers, and where funds are returned to the customer if the transfer is not carried out. This is consistent with the exclusion of money transfer products generally from the scope of CRS.

5.3. Question 3: consistent with other provisions of the CRS, the de minimis thresholds for e-money would be subject to the account aggregation rules contained in paragraph C of Section VII of the CRS to avoid circumvention of CRS reporting by spreading amounts over multiple e-money products. Alternatively, a (significantly) lower threshold could be considered, that would not be subject to the account aggregation rules. Which of the two would be the most workable option and why?

Response:

5.3.1. As set out at paragraph 2.2.12, and in order to implement a value limit that is practical, industry will comply with account aggregation rules set out at paragraph C of section VII of the CRS in relation to individual and entity accounts and will ensure that multiple accounts or card balances held by any customer with a Reporting Financial Institution or with a Related Entity will be aggregated when applying the threshold.

5.3.2. We do not believe a lower threshold is practicable as this will result in unreasonable levels of data collection, in a detrimental impact on the risk-based approach and on the implementation of simplified due diligence within the AML regime.

5.3.3. Furthermore, a low threshold will impact the role played by e-money products in increasing financial inclusion and deterring financial crime.

6. Excluded Accounts

6.1. Question 1: Do you consider the above proposal to qualify certain capital contribution accounts as Excluded Accounts useful? Are the conditions sufficiently clear and practically implementable?

Response:

6.1.1. At present, the Excluded Account category with respect to escrow accounts only covers instances where amounts are put on escrow for purposes of:
(i) a court order or judgement,
(ii) a sale, exchange or lease of real or personal property under certain conditions and
(iii) to cover a future payment of insurance premiums or taxes.

6.1.2. We are of the view that the proposal to qualify certain capital contribution accounts as Excluded Accounts is useful, as their purpose is to block funds for a limited period of time in view of the incorporation of a new company or a pending capital increase.

6.1.3. Regarding the conditions being practically implementable, the proposal to only treat such an account as an Excluded Account for a maximum period of 12 months may present some issues, particularly if regards to unforeseen delays. As such, it may be useful for individual jurisdictions to have the discretion to extend this period if necessary.

6.2. Question 2: Are there any other types of accounts or financial instruments that present low tax compliance risks and that should be added to the Excluded Account definition?

6.2.1. We have not provided a response to this question.

7. Treatment of non-profit Entities under the Active / Passive NFE distinction

7.1. Question 1: While most Active NFEs are not treated as Investment Entities even if they meet the Investment Entity definition, this carve-out does not apply to Entities that are Active NFEs by virtue of being a non-profit Entity as defined in subparagraph D(9)(h) of Section VIII. Representatives from the philanthropy sector have highlighted that this can lead to highly undesirable outcomes, requiring genuine public benefit foundations to apply due diligence procedures in respect of all beneficiaries of grant payments and report on grant payments to non-resident beneficiaries, such as for instance disadvantaged students receiving scholarships. At the same time, concerns have been expressed by governments that simply extending the carve out from the Investment Entity definition to all non-profit Entities described in Subparagraph D(9)(h) of Section VIII could give rise to situations where Investment Entities would circumvent their reporting obligations under the CRS by improperly claiming the status of non-profit Entities. Are there other measures or criteria that could be envisaged to ensure that genuine non-profit Entities are effectively excluded from reporting obligations as an Investment Entity in a manner that would not give rise to potential circumvention?

Response

7.1.1. We support the proposal to exclude non profit entities, and this could be accompanied by guidance in relation to misuse of this provision.

8. Reliance on AML/KYC Procedures for determining Controlling Persons

8.1. Question 1: Are there still instances where Financial Institutions do not apply AML/KYC Procedures that are consistent with 2012 FATF Recommendation for the purpose of determining Controlling Persons of Entity Account Holders?

Response

8.1.1. Financial Institutions are under different obligations in different jurisdictions. They do for example in the EU collect information relating to beneficial owners or those with a controlling interest that is above 25%. In other jurisdictions, the obligations may vary.

8.1.2. The approach to dealing with existing accounts holders will need to be risk based and incorporate customer engagement that may take place as a result of changes in circumstance etc.

9. Collection of TIN for Pre-existing Accounts

9.1. Question 1: The inclusion of the TIN of Reportable Persons (if issued by the jurisdiction of residence) significantly increases the reliability and utility of the CRS information for tax administrations. Although not included in the current proposal, the OECD is still exploring feasible

measures to ensure the collection and reporting of TINs with respect to Pre-Existing Accounts. What approaches could Financial Institutions take to collect TIN information in respect of Pre-Existing Accounts, while mitigating potential burdens for Reporting Financial Institutions?

Response

9.1.1. We caution against a departure from the current expectations of CRS; but pre-existing accounts can be updated on a normal compliance cycle as customers' circumstances change.

10. Dual-resident Account Holders

10.1. Question 1. The proposed changes to the Commentary foresee that Account Holders that are resident for tax purposes in two or more jurisdictions under the domestic laws of such jurisdictions declare all jurisdictions of residence in the self-certification and that Reporting Financial Institution must treat the account as a Reportable Account in respect of each jurisdiction. The OECD is still considering whether an exception to this rule should apply where the Account Holder provides the Reporting Financial Institution with government-issued documentation to resolve cases of dual residence under applicable tax treaties. Are there instances where Reporting Financial Institutions have received such documentation and, if so, in what form (e.g. a letter issued by one or more competent authorities)?

10.1.1. We have not responded to this question.

11. Integrating CBI/RBI guidance within the CRS

11.1. Question 1. Are there any additional and/or alternative questions, other than those already in the CBI/RBI guidance, that would be useful to include in the Commentary to the CRS, for purposes of requiring Financial Institutions to determine the jurisdiction(s) of residence of a CBI/RBI holder?

11.1.1. We have not responded to this question.

12. Transitional Measures

12.1. Question 1. Are the proposed transitional measures in Section X appropriate for Reporting Financial Institutions to update their processes and systems to comply with the proposed amendments to the CRS?

Response

12.1.1. We are wholly supportive of transitional measures. We suggest however a longer timeline for transition to enable systems to be built and for operational changes to be introduced. A three year period of transition would be more appropriate.

Annex 1: List of EMA members as of April 2022

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
ArcaPay Ltd
Azimo Limited
Bitpanda Payments GmbH
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
ePayments Systems Limited
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Global Currency Exchange Network Limited
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited
MONAVATE
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Europe Limited
NoFrixion Ltd
OFX
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Oxygen
Park Card Services Limited
Paydoo Payments UAB
Paymentsense Limited
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
Vivid Money Limited
Weavr Limited
WEX Europe UK Limited
Wirex Limited
Wise
WorldFirst
WorldRemit LTD
Yapily Ltd