BUSINESS AT OECD RESPONSE TO CARF/CRS PUBLIC CONSULTATION DOCUMENT

CRYPTO-ASSET REPORTING FRAMEWORK QUESTIONS

Crypto-Assets in scope

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?

- The CARF Crypto-Asset definition essentially follows the FATF Recommendations—although in certain respects the FATF definition is broader in that the CARF definition relies on distributed ledger or a similar technology whereas the FATF Recommendations for virtual assets do not. Specifically,
    - CARF: "The term "Crypto-Asset" means a digital representation of value that relies on a cryptographically secure distributed ledger or a similar technology to validate and secure transactions."
    - FATF: "Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations" (item 44) and "That is, they should be applied based on the basic characteristics of the asset or the service, not the technology it employs." (item 47).
- We believe the proposed definition of Crypto-Asset as a "digital representation of value that relies on a cryptographically secured distributed ledger or a similar technology to validate and secure transactions" is potentially too broad as the proposed definition is sourced from a description of the technology itself and not the use. Thus, we suggest that the definition be technology-neutral and, following the FATF Recommendations, be limited to virtual assets *used* for payment or investment purposes. For now, the definition should be limited to fungible virtual assets while more time is spent studying and understanding the various use cases of non-fungible virtual assets.
- It will be important to introduce *de minimis* exemptions, as recommended by the OECD in its 2020 Report *Taxing Virtual Currencies - An Overview of Tax Treatments and Emerging Tax Policy Issues* ("Supporting improved compliance, including through the consideration of simplified rules on valuation and on exemption thresholds for small and occasional trades"). This is particularly relevant in the case of "hybrid tokens" that many kids today possess, such as sports fan tokens of limited value.
- It should be clarified in the definition of Relevant Crypto-Asset that those include only those that are listed on a digital asset exchange and actually exchange-traded and not all those that in principle "can be traded or transferred … in a digital manner." The broader definition risks inundating tax administrations with irrelevant information. This concern is particularly relevant in the case of NFTs.
- We agree that "closed-loop crypto-assets" and CBDCs are properly excluded from the definition.
- Prompt guidance will be needed to identify "similar technologies" to facilitate consistent treatment globally.

- We suggest that financial assets' digital representations maintained at financial accounts of CRS Financial Institutions be excluded explicitly from the definition of the Crypto-Asset despite its usage of a cryptographically secured distributed ledger or a similar technology (e.g., security tokens, derivatives on Crypto-Assets). There are three reasons behind this suggestion.
    - First, we consider that the case above does not link to the concerns outlined in the consultation document, which states "Crypto-Assets, which can be transferred and held without interacting with traditional financial intermediaries and without any central administrator having full visibility on either the transactions carried out, or the location of Crypto-Asset holdings" (page3) "are frequently offered by actors that are not covered by the Common Reporting Standard (CRS). . . . Against this background, the OECD is advancing…" (page3), and "The definition of Crypto-Assets thereby targets those assets that can be held and transferred in a decentralised manner, without the intervention of traditional financial intermediaries" (page5).
    - Second, the CARF and CRS seek to be consistent with the FATF Recommendations, whose "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" defines the relevant assets as follows: "Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations" (item 44) and "that is, they should be applied based on the basic characteristics of the asset or the service, not the technology it employs" (item 47).
    - Third, in the case where the digital representations of financial assets fall under the definition of Crypto-Assets, the establishment and implementation of relevant due diligence procedures will be complicated for both customers and Financial Institutions that comply with the CRS, CARF, and FATCA.

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

- We recommend that the definition of "Closed-Loop Crypto-Asset" be modified so that conditions b) and c) are alternative and not concurrent. We make this recommendation to address Closed-Loop Crypto-Assets that can be exchanged among participants. As these situations should not pose tax compliance risks, they should be excluded from the definition.

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?

- Crypto-Assets that maintain a relatively constant value (such as private issue stable coins that have not materially broken their peg) present a low risk of tax evasion, similar to CBDCs, and should be excluded.

- Financial assets' digital representations (e.g. security tokens) that meet the following requirements also should be excluded as otherwise there is a significant risk of amounts being double counted under the CRS and the CARF.
    - The assets are subject to the CRS so that CRS Financial Institutions comply with the due-diligence and reporting obligations.
    - Customers cannot exchange and transfer the assets without interacting with the Financial Institutions.
    - The Financial Institutions have full visibility on the transactions and the asset holdings at the financial accounts.
- In addition, small-value transactions (such as the use of Crypto-Assets to purchase a meal) should be exempt from reporting (even if otherwise in scope).
- "Vanity" tokens that individuals, groups, and organizations create primarily for marketing and promotion purposes also should be excluded. Certain NFL football players, for example, have created tokens that fans can purchase in exchange for benefits and services that only fans of that celebrity will care about. Such tokens are used more for branding, marketing, and loyalty purposes than as financial or investment assets. Such marketing-related tokens should also be included in the definition of Closed-Loop Crypto Assets.
- Finally, tokens that are issued to contributors of a protocol that allow that contributor to "earn" tokens that represent rights to approve technical changes to the protocol should be excluded. Such tokens have the primary purpose of governing and ensuring the technical integrity of a protocol and have little value to those outside of a community of enthusiasts and hobbyists for a certain protocol.

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?

- We agree that only those NFTs covered under the FATF Recommendations should be in scope under the CARF.
- Clarifying guidance will be necessary to exempt NFTs (such as one granting the holder the right to attend a concert) that may have some modest "collectible" value, either because of the nature of NFT or simply after the right represented by the NFT has been rendered.
- It should be clarified that the definition includes only those that are actively exchange-traded and not all those that "can be traded or transferred … in a digital manner," as in theory any NFT can be traded or transferred in a digital manner. Our suggestion is based upon considerations of administrability and efficiency.
- Given the rapidly evolving nature of NFTs, dialogue with business should be ongoing to minimize innovation-stifling uncertainties. Business at OECD stands ready to assist in ensuring a productive ongoing dialogue.

Intermediaries in scope

1. Do you see a need to either widen or restrict the scope of the intermediaries (i.e. Reporting Crypto-Asset Service Providers)?

- More clarity is needed in the case of DeFI which appears to be at least in part included ("an entity making available a trading platform….."). At the moment the Commentary hinges on the FATF guidance, which refers to control and significant influence, but the question may remain of who is legally obliged (*see*, para. 19 of Commentary: "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, or otherwise having sufficient knowledge (e.g. by virtue of acting as an interface providing access to the platform for purposes of an Exchange Transaction or acting as an aggregator), allowing it to comply with the due diligence and reporting obligations with respect to Exchange Transactions concluded on the platform." It is not clear who decides whether it is in a condition to comply and what are the consequences of that determination.
- More clarity would also be welcome in relation to the obligations of DAOs (Decentralised Autonomous Organisations).
- Considering the lack of clarity regarding DeFi transactions and the obligations of DAOs, we suggest delayed implementation of reporting such transactions until guidance is provided.
- Again, to promote compliance, the topic of Intermediaries in scope should be addressed together with the topic of consequences of complying/not complying with the rules.
- Coordination between the CARF and the CRS will be needed to prevent duplicative reporting and gaps.

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?

- Whenever multiple RCASPs could be considered to effectuate the same transaction with the same customer, reporting should be performed only by the RCASP with the closest relationship to the customer. We are working to provide additional thoughts on how to ensure that reporting occurs once and only once.

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?

- While we have not identified circumstances in which a RCASP would not have nexus in any jurisdiction, the possibility cannot be dismissed. Should this situation arise, the RCASP with the closest relationship with the customer should report.
- This topic should be addressed together with the topic of consequences of not complying.

Reporting requirements

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

- Intermediaries may maintain a Fiat Currency value for Crypto-Assets.
- Valuations, particularly for less liquid Crypto-Assets, can be exceedingly difficult.
- Many service providers are not equipped to do more than take valuations provided via professionals/public websites.
- Valuations also could be performed based upon jurisdictionally applicable accounting standards (such as IFRS or US GAAP).

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

- As this marketplace is evolving, an alternative that is preferable today may be less appropriate tomorrow. Consequently, it seems preferable to permit an intermediary to apply any reasonable approach—so long as that approach is applied consistently.

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.

- We do not see great benefit, as noted above, in reporting illiquid tokens. In any case, the valuation process is more difficult when an asset or product is thinly traded.
- Delayed implementation of information reporting, until regulatory clarity is provided, would be appropriate.

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?

- If information is not available to a RCASP via the travel rule, significant reporting difficulties may arise. An exchange that hosts a business, for example, is unlikely to know the business' customers.

- A *de minimis* exception for low-value transactions would reduce compliance burdens.
- We recommend:
    - a *de minimis* threshold and that RCASPs be subject to a "reason to know" standard when determining whether a customer is attempting to circumvent the threshold by splitting apart one transaction into multiple transactions; or
    - that only the number of transactions be reported with tax administrations then having discretion to use exchange of information on request.

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?

- RCASPs may not have the necessary knowledge to report these transactions. An exchange, for example, will not maintain records of any newly created Crypto-Asset that it does not support. Indeed, the user itself may not be aware of the newly created Crypto-Asset.

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?

- While RCASPs can report information within their possession, such as the wallet address that is the destination of a transfer, they cannot always distinguish wallet addresses associated with another RCASP. Significant lead time would be required to build systems to maintain and report information into which a RCASP may have sight.
- While we appreciate the desire for more line of sight into transactions occurring in self-custodied wallets, RSCAPs would be burdened substantially were they required to build the infrastructure to maintain or report originating wallet addresses. The possibility of duplicative reporting also would be significant.
- Finally, the reporting of on-chain wallet addresses goes much further than the CRS as it would be the equivalent of obtaining transactional details of credit card payments. We

consider that the same objectives, in terms of tax compliance and tackling tax evasion, can be reached in different ways that would avoid legitimate policy concerns.

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?

- CARF reporting time periods should be consistent with those under the CRS. Importantly, no reporting should be required before the due date under the CRS; this approach will minimize the need for corrections. Penalty relief should be provided for all reasonable efforts.
- Experience with FATCA and the CRS—and the delays provided by governments as the magnitude of the undertaking became more apparent—informs our view that substantial time will be required. The steps needed to develop the systems necessary to capture, maintain, and then report the information required under the CARF will require a substantial resource and time commitment. Anecdotally, even those financial institutions with well-developed information systems needed, on average, about four years to implement FATCA and another two years to implement the CRS.
- Consequently, we recommend staggered (phased) implementation dates.
    - A phased approach could be considered so as to provide more time in the first years of application of the CARF.
    - Reporting for exchanges could be implemented more quickly than reporting for DeFi and NFTs.

Due diligence procedures

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?

- RCASPs should be subject to the same due diligence procedures that are imposed on FIs under the CRS. Thus, RCASPs should not be required to document Controlling Persons of all Entity Crypto-Asset Users, other than Excluded Persons.
- As under the CRS, self-certifications received should remain valid indefinitely—subject to the requirements to apply the change of circumstances rules. At a minimum, the CARF's 36-month rule should not be applied to any account for which indefinite validity is provided by the CRS.

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?

- Income from mining should be considered active income anytime there is a substantial investment in terms of assets and facilities.

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?

- RCASPs should be treated as Excluded Persons because they pose a low risk of tax evasion.
- This exclusion would be available when an entity has certified its RCASP status during the account onboarding process.
- Business should not be required to verify the status of an entity that certifies its RCASP status unless the business has reason to know that the certification is invalid.
- Such an exclusion would reduce duplicative reporting and thereby improve government efficiency.

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?

- Businesses should be allowed to continue to effectuate customer transactions, as they can under the CRS, so long as they report the Crypto-Asset user to the relevant jurisdiction for which there is indicia if a self-certification form cannot be obtained. The crypto user could be reported as an unknown recipient. RCASPs are already subject to strict AML/KYC requirements. Failure to comply will result in severe monetary and criminal sanctions as well as possible revocation of a firm's business permit. If a user otherwise has met AML/KYC requirements, firms should not be prevented from effectuating transactions for lack of a self-certification. Tax authorities have other tools at their disposal, such as applying penalties and backup withholding on users, that will assist in the completion of a valid self-certification form.
- Appropriate time should be provided to correct and verify missing or conflicting information for both validity and reasonable purposes without stopping business.

- Alternative customer verification procedures, such as publicly available information, that are consistent with CRS requirements should be provided.
- Self-certifications should remain valid indefinitely—as they are under the CRS—absent a change in circumstances.

Other elements of the proposal

1. Comments are also welcomed on all other aspects of the Crypto-Asset Reporting Framework.

- Voluntary Disclosure Regime
    - Taxing jurisdictions should consider a voluntary disclosure regime so that taxpayers can come forward to remedy any past compliance shortfalls. Relief from tax understatement penalties would be afforded any taxpayer not currently under audit. Any disclosures should be accompanied by a list of exchanges on which the taxpayer has traded, as well as the public address of the wallets used. These additional disclosures will enable tax authorities to independently confirm any representations made by the taxpayer.
- Tax Nomads
    - Guidance will be needed on the proper treatment of persons who claim to have no tax residence ("tax nomads").
- Consistency with the CRS
    - Differences between CARF and CRS definitions should be limited to situations supported by clear and sound tax policy considerations. A few observations regarding these differences are provided as responses to the CRS Amendment "other comments" question regarding the seamless interaction of the CRS with the CARF.

AMENDMENTS TO THE COMMON REPORTING STANDARD

Specified Electronic Money Products

- The e-money industry mostly caters for specific purpose payments, and users seeking to register for most products are unprepared to offer-up additional data at onboarding. They may not feel this is warranted or justified by the product proposition and would not therefore expect a lengthier registration process. In our experience additional data fields and additional verification gives rise to significant user abandonment at this stage. For many products, this will impact the viability of the product.
- For this reason, the industry has sought to benefit from simplified due diligence (SDD) for the majority of its products for some 20 years. The ability to continue to implement SDD is key, but this would not be the case if additional data collection and verification was required at the outset, or within conditions of low risk. This would impact the risk-based approach and require full customer due diligence (CDD) at the outset for all products, undermining the implementation of the risk-based AML/CTF CDD regime. This is because it will result in a non-risk-based allocation of resources, spreading time and effort thinly, at

the expense of products, customers and circumstances that may better benefit from the firm’s resource allocation.

- We believe that allowing issuers to implement SDD according to the general risk assessment requirements in AML legislation and FATF Recommendations, taking into account all AML/CTF risks including tax evasion, is a sound approach to implementing CRS whilst ensuring consistency with the broader AML regime. The provision of a threshold for low-risk conditions will guard against such disruption.
- There are also key uses of e-money products or e-wallets in furthering economic development and inclusion, enabling electronic payments to be made in rural areas, enabling electronic payment of wages to migrant workers and in the distribution of aid. In all such circumstances, the e-wallet user has no access to a traditional bank account and the collection of CRS related data is extremely difficult or impossible, hence would certainly frustrate the use of such products, and in order to preserve such utility, these products need to be exempted, or given the benefit of an appropriately calibrated threshold.
- There is additionally a good rationale for excluding products that are not used to store value, despite meeting the definition of e-money, but are rather used for money transfer type of transactions, excluding a functionality for the sheltering of funds.

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?

- The definition of specified electronic money products 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.
- We do suggest however the addition of the words ‘in payment’ after ‘accepted’ in paragraph (d) to reinforce the function of such products.
- 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.
- 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.
- 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.

- These products are usually associated with low-value payments. We believe that 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.
- It is also possible to distinguish **financial inclusion** products from other e-money products; in such instances, it is proposed that such products be excluded from the definition of e-money altogether. This is because beneficiaries of such products are seldom also seeking to evade tax.
- Similarly, products that are used to **distribute government and social benefits** or emergency aid and which can only be funded by a government or aid agency also merit exclusion for the scope of CRS.
- Finally, we would like to draw attention on possible issues that may arise with the proposed definition of "Specified Electronic Money products" in relation to pre-paid cards and gift cards.
    - It will be important to identify which products are in-scope or out of scope given the variety of products that businesses may provide, use, or commercialize. There may also be a need to further restrict the proposed definition of "Specified Electronic Money Products".
    - Because the definition of "Specified Electronic Money products" is drafted in a wide way, certain products, which we believe are not the primary target of the CARF/CRS rules, may unintendedly be captured in the non-financial sector.
    - One example may be "fuel cards" which can generally be described as secure identification and loyalty card that authorise the purchase of fuels, vehicle-related services (e.g. vehicle wash) and on-road services such as tolls and road taxes.[1]
        - **It is important to note that fuel cards consist of means of authorisation rather than means of payment:** the Fuel Card generally does not provide a means of payment but serves as an authorisation to verify that the user is acquiring fuel through arrangements with the Fuel Card Issuer. A Fuel Card therefore generally operates differently from a credit card or other payment cards. Fuel Cards have no payment function and are not subject to Financial Regulatory Authority supervision.
        - In our view, Fuel Cards should not fall into the definition of "Specified Electronic Money Product;" this should be clarified in the proposed rules

[1] This product generally involves: (i) a Fuel Card Issuer (the entity which issues and operates the Fuel Card. This may be a subsidiary of a Mineral Oil Company or an independent entrepreneur). The Fuel Card Issuer will enter into separate contracts with the Mineral Oil Company and the Fuel Card Users ; (ii) a Mineral Oil Company which is the entity owning the Fuel at the service/petrol station immediately prior to it being filled into the tank ; (iii) a Fuel Card User / Customer: the person or legal entity which purchases the fuel ; (iv) a Commissionaire i.e. an intermediary transferring goods or services pursuant to a contract under which commission is payable on purchase or sale.
The Fuel Cards business model may work under two main arrangements: (i) a buy/resell model whereby the Mineral Oil Company sells the fuel to the Fuel Card Issuer. The Fuel Card Issuer sells the Fuel to the Fuel Card User. Physical delivery of the Fuel takes place directly from the Mineral Oil Company to the Fuel Card User. The Fuel Card typically has no payment function and only serves the purpose of identifying the Fuel Card User as the person legitimately acting in the name of the Fuel Card Issuer; (ii) a commissionaire model whereby the Fuel Card User appoints the Fuel Card Issuer as its buying agent (commissionaire). The Fuel Card Issuer acts as purchasing agent for the Fuel Card User, but does not take legal title to the Fuel.

(the details under 29sexies on page 83 seem to suggest that Fuel Cards are out of scope, but we think it would be worth clarifying further). Other pre-paid cards may function in a similar way as fuel cards or may present similar features (e.g. not a means of payment). We stand ready to provide more details if necessary.

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?

- 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.
- **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 and would be disproportionate to the purpose and characteristics of the e-money product.
- The impact of such requests is observed in significant rates of abandonment at onboarding, and a sharp 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.
- A **risk-based approach** is far 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 then seeking more information and verifying such additional information when the risk posed by the customer and the product increases and justifies this burden.
- 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.
- **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.

- 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.
- **SDD** would not be capable of adoption 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 would 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.
- 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.
- Another instance is in enabling wage payments to be made electronically to migrant workers (such as construction workers for example) in circumstances where migrant workers are not permitted access to bank accounts under local law. The payroll service e-wallet is directly linked to the employment contract; thus, it is opened upon commencement of employment and simultaneously closed once the employment contract is terminated. Furthermore, it is not possible for the e-wallet user to unilaterally place any funds into the e-wallet itself; only the employer is able to place funds (wage) into such e-wallet. In all such instances, e-money and e-wallets are a significant means of economic and financial inclusion.
- 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 either provide for exclusion from the scope of CRS altogether, or to offer a reasonably calibrated threshold that would enable this and other e-money products to continue to be offered to users.
- 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.
- 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.
- 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 and put into practice, and to represent a balance between business needs and legitimate tax authority concerns.
- 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.

- 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.
- This limit would be subject to the **aggregation rule.**
- 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.
- We also 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.

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?

- 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.
- We do not believe a lower threshold is practicable as this will result in unreasonable levels of data collection and have a detrimental impact on the risk-based approach and the implementation of simplified due diligence within the AML regime.
- Furthermore, a low threshold will impact the role played by e-money products in increasing financial inclusion and deterring financial crime.

Excluded Accounts

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?

- We support the proposal to treat these capital contribution accounts as Excluded Accounts.
- The 12-month maximum period might be problematic due to unforeseen circumstances (such as those experienced during the COVID pandemic). Conditional exceptions also increase complexity, cost, and the risk of inadvertent non-compliance. Jurisdictions should be permitted to extend the maximum period for reasonable cause and limit responsibility for good faith determinations that an account qualifies as Excluded.
- Guidance would be appreciated, for example, confirming that generally applicable fees, etc. can be withdrawn by service providers without the account losing its Excluded Account status.

- We suggest referring to "Entity" instead of "company" as capital contribution accounts may be used not only with respect to companies but also in relation to other types of legal persons and legal arrangements.

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?

- We have nothing to add at this time.

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

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?

- We strongly support an exclusion for all genuine non-profit Entities.
- Non-profit Entities should not be discouraged from entering into discretionary mandates with a local custodian to manage their financial assets.
- The risk of tax evasion seems remote given the charitable mandate that provides these organizations with tax-exempt status.
- Operational consistency with the FATCA definition would minimize potential issues for FIs that have implemented a streamlined solution for both the CRS and FATCA.
- A criterion that may be used to ensure that only genuine non-profit Entities are excluded is to extend the carve out from the Investment Entity definition to all non-profit Entities described in Subparagraph D(9)(h) of Section VIII provided that such Entities have been granted tax-exempt status, or otherwise approved as such, by the relevant tax Government Entity.

Reliance on AML/KYC Procedures for determining Controlling Persons

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?

- Based on the FATF's mutual evaluation outcomes (updated 22 March 2022), only 18 jurisdictions are technically compliant with Recommendation 10. From this technical point of view, only FIs in these 18 jurisdictions operate in an environment enabling them to apply AML/KYC procedures that are consistent with the 2012 FATF Recommendation for the purpose of determining Controlling Persons of Entity Account Holders.
- We recommend, consequently, that the CRS requires procedures applied to be consistent with the local jurisdiction's AML/CTF laws, rather than with the 2012 FATF Recommendation.
- The role performed by a Controlling Person may not necessarily be collected for AML/KYC purposes as part of the account opening process or, if collected, maintained with a view to CRS reporting. Because the definition of a Financial Institution is much broader under the CRS, there are entities that will be treated as Financial Institutions for CRS purposes that do not have the same AML/KYC obligations and may not have this information currently.
- For those Financial Institutions that collect this level of detail for CRS purposes currently, this information may not be stored in an electronic format that would allow for easy reporting. Therefore, if this proposed change were applied to accounts in existence at the date the guidance became effective, the likely result would be a wholesale manual review or due diligence redocumentation of all accounts. The value of any such information reported following these extensive efforts is likely to be small compared to the costs of gathering it.
- As discussed during the original CRS consultation period, customer responses are not guaranteed. This is especially so in insurance where, given the long-term nature of the in-scope products, there is often little interaction with the customer between the date the product is first taken out and the point that either the product matures or an insurance event occurs.
- Should the CRS be revised to require reporting of the role that makes a Controlling Person a Reportable Person, an appropriate implementation period will be required. Changing data capture systems and application forms, changing all downstream processing systems, and providing training to staff and independent agents, will be both costly and time consuming. Moreover, we recommend that, for Reportable Accounts documented prior to the implementation of this rule, the Controlling Person status be required to be reported only if (1) the information already is maintained in an accessible format in a system that is linked to the CRS reporting system or (2) the information has been obtained via the normal change of circumstances process.
- Even if an FI collects the role performed by a Controlling Person, it is possible that only one role would be recorded when the person performs multiple roles (such as both a trustee and a beneficiary). Redocumenting these Controlling Persons to identify all potentially applicable roles would be a huge effort and, as discussed above, responses are not guaranteed.
- Any change to how Controlling Person information is reported should apply only prospectively after sufficient time has been provided to implement new account opening procedures.

- More detailed guidance is necessary regarding how FIs are to implement the FATF Recommendations regarding Controlling Persons with regard to (i) private investment entities that become managed by FIs and (ii) complex trust structures.

Collection of TIN for Preexisting Accounts

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?

- We strongly urge that the CRS not be modified to require the collection and reporting of TINS with respect to Pre-Existing Accounts. Business repeatedly has explained the difficulties that FIs encounter in seeking TINs on these accounts. Moreover, the degree to which Pre-Existing Accounts are "potentially problematic" shrinks each year as customers rearrange their financial affairs and close these accounts and/or must document with a self-certification because of a change in circumstances. In some cases, business would be requesting data that the customer simply does not possess as TINs are not always obligatory.
- Further guidance on the collection of TINs would be welcomed after the initial two-year period of Pre-Existing Accounts where outreach is required on an annual basis once this period has lapsed. Financial Institutions need clarity regarding what is expected to remain compliant—particularly in jurisdictions that have no such requirement—and to mitigate the burden that increases with the number of jurisdictions in which an FI has a footprint. In the absence of clarifying guidance, some FIs have developed their own approaches and started closing such accounts; this action, however, may be subject to legal challenges and, of course, results in a loss of business.
- We suggest aligning the outreach for missing TINs with AML/KYC rules in line with FATF Recommendations—whereby the requirement to review an existing client is done on a risk-based approach (between one and up to three years). This would mitigate the burden for Financial Institutions to operationalise the requirement to obtain missing TINs for Reportable Accounts and also increase the likelihood of receiving a response from the account holder.

Dual-resident Account Holders

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)?

- The removal of the tie breaker for potential dual-resident accounts can create significant compliance issues for FIs:
  - FIs generally do not, and in some countries legally cannot, provide tax advice to customers. Any customer who has obtained independent professional advice likely will have applied the relevant tie-breaker rule. Consequently, if the tie-breaker exception is removed, a conflict will arise in resolving the self-certification's reasonableness. Specifically, the FI will be expecting the customer to provide a pre-tie-breaker position while the customer will be providing a position that already incorporates the tie-breaker's application.
  - The inclusion of the question of dual-residence scenarios in the self-certification and the corresponding information-related systems would require FIs to make substantial adjustments. Therefore, a sufficient transition period of at least two years is necessary. In addition, it is crucial that the rule apply only to financial accounts opened after the transition period. In no case should financial institutions be obliged to obtain a new self-certification if they already received a valid self-certification in the past or were not obliged to obtain a self-certification at all. Because the assessment of dual or multi tax-residencies can be difficult and controversial, the financial institutions should not be obliged to verify the declaration in the self-certification of the account holder.
  - If the tie-breaker rule were repealed retroactively, FIs would have limited ability to review previously accepted self-certifications. FIs do not have the ability to search electronically their recordkeeping systems to determine whether the tie-breaker rules were used previously.
- We strongly support the use of government-issued documentation to resolve dual residence cases.

Integrating CBI/RBI guidance within the CRS

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?

- We acknowledge that CBI/RBI schemes could be used to undermine CRS reporting.
- We urge simple and clear rules for applying the reasonableness test to CBI/RBI holders—as this test often is conducted by frontline staff who typically are not tax specialists—particularly noting that these questions tend towards the tax advice space that FIs are precluded (sometimes by law) from providing. The CRS Commentary includes several examples of how the reasonableness test is applied in other contexts. A self-certification is not reasonable, under the CRS Commentary, if the address on the self-certification conflicts with that contained in the AML/KYC documentation (Sec. VI, para. 14, Example 1). Clear rules such as these allow non-tax specialists to conduct the reasonableness test.

- We are concerned that the current proposal suggests that FIs should ask four questions (that may be perceived as tax advice) to persons claiming residence in a jurisdiction offering a potentially high-risk CBI/RBI scheme. The FI then is required to consider the client's answers when finally applying the reasonableness test without any instruction to the client that may be perceived as tax advice. To apply such an "ask-follow-up-questions" approach in the mass market, there would need to be a clear rule such as "if the answer to question X is 'yes', the self-certification fails the reasonableness test" or "if the answer to question Y is 'no' and the answer to question Z is 'yes, the self-certification passes the reasonableness test." Furthermore, clear guidance needs to be provided in resolving any reasonableness failures in this context, e.g. if the client states that he/she paid personal income taxes in Jurisdiction X in the past year, must the RFI instruct the client to include Jurisdiction X in the self-certification to resolve the failed reasonableness? This instruction would impact the integrity of a *self*-certification and could require the FI to violate local laws prohibiting it from providing tax advice. The "common" reporting standard will become fragmented to the extent (i) of any uncertainty regarding the rules' application or (ii) that judgment-based rules are adopted that cannot be incorporated into electronic systems.
- With respect to the specific questions:
  - Even if the client affirms that he/she obtained residence rights under a CBI/RBI scheme, this does not necessarily mean that he/she is also resident in another jurisdiction.
  - Asking the client whether he/she also holds residence rights in another jurisdiction in our view is obsolete because the client is clearly instructed when completing the self-certification that all countries of residence must be listed (and that the incorrect completion of a self-certification is subject to penalty).
  - Even if the client affirms that he/she spent 90 days in another jurisdiction, this does not necessarily mean that he/she is also resident in that other jurisdiction. There are numerous jurisdictions with exceptions and higher thresholds and jurisdictions may apply different counting mechanism—none of which an FI cannot be expected to know and verify. This analysis also ventures into the tax advice arena—which FIs generally are prohibited by company policy or local law from entering.
  - Even if the client affirms that he/she filed a tax return in another jurisdiction in the previous year, this does not mean that he/she still is tax resident there. Equally likely, this could simply be the result of a move of domicile or because the tax filing obligation was due to certain investments or real property in that jurisdiction.
- Thus, the proposed wording should not be incorporated into the CRS Commentaries as it is unlikely to achieve the CRS policy objective and might create tax advice difficulties for FIs. We strongly recommend that the OECD and the Global Forum continue to solve the matter of CBI/RBI schemes with the relevant jurisdictions directly (particularly since all of the currently listed jurisdictions participate in the CRS). FIs will of course continue to apply the existing due diligence requirements and, where a client claiming residence under a CBI/RBI scheme would e.g. provide a residence address in a different jurisdiction, the FI will trigger either a reasonableness test failure (at account opening) or a change in circumstances process (if identified during the course of the client relationship).

Transitional Measures

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?

- The transitional measures are too narrow to support the work effort required by FIs to implement all of the proposed changes (as Section X provides relief currently only for the requirements under subparagraph A(1)(b) of Section 1).
- A very substantial timeline (e.g. 3 years) would be needed as many Financial Institutions presently lack sufficient capacity to respond effectively to new mandates—particularly those of this magnitude.
- Specifically in relation to the requirements under subparagraph A(1)(b) of Section 1, should a manual review of accounts be required, the review should be risk-based and narrowly tailored. As manual reviews are required currently only for high value pre-existing accounts in very specific circumstances, any new obligation to review accounts deemed "problematic" (such as accounts without TINs) likewise should be targeted to those of sufficiently high value.
- Adding new reporting fields means that the financial institutions need to update electronic reporting systems to accommodate these fields. These system changes can take 24 to 36 months after the final text and schema have been agreed and enacted in each country's local law. A phased implementation, with "soft landing" penalty relief, will be necessary because of complexities within specific organizations or industries. Updating legacy systems can be particularly problematic.

Other comments

1. Are there any other measures that could be taken to ensure the seamless integration of the CRS with the Crypto-Asset Reporting Framework?

- We are concerned about duplicative due diligence and reporting obligations that could arise for CRS Financial Institutions with respect to Crypto-Assets. We would make the following policy recommendations to eliminate duplication:
    - Align the scope of CRS and CARF due diligence and onboarding requirements – i.e. align both the types of documentation and indicia-based due diligence required as well as the timing requirements for obtaining documentation or performing due diligence. Alternatively, for Financial Institutions that are already Reporting FIs under CRS, align due diligence and onboarding requirements across both CRS and CARF reporting. In either case, reporting FIs should be permitted to rely on the outcomes of CRS due diligence to determine customers' tax residency for purposes of the CARF in the case where the reporting FIs have already specified their tax residency under the CRS and the customers also trade Crypto-Assets. Principally, we make this recommendation due to the considerable investment and operational burden already borne by Financial Institutions in the context of CRS and FATCA. If such institutions were required to adopt another similar, but slightly

different, regime and effectively build a new set of due diligence procedures particularly for Crypto-Assets—some of which might be maintained within the same account architecture as CRS Financial Accounts—this would represent a significant challenge and cost.

  - CRS Financial Institutions should be allowed to discharge all CARF reporting obligations for any Crypto Assets held on behalf of clients that they treat as part of a custodial account.
  - Alternatively, if specific incremental data points are of particular interest to government and are not required under custodial account reporting, or governments would like specific data points concerning Crypto Assets to be segregated from other products, the CRS XML schema should be amended to include these specific data points so that CRS Reporting FIs may provide this reporting as part of their usual CRS reporting. It should be noted that any such additional fields must be optional within the schema as many CRS RFIs may not have any reporting obligations under CARF.
  - RCASP entities that are also CRS Financial Institutions should only report under CARF for assets that are not Financial Accounts under the CRS.
- We welcome the guidance provided by the OECD suggesting that certain deployments of blockchain technology would not be caught *per se* within the scope of Crypto-Asset reporting. As this is a developing area, we would strongly recommend OECD consults with business on the various uses of blockchain and other similar technology and how this might interact with any Crypto-Asset reporting. In particular, we would note that traditional financial institutions should be included in these discussions as, even if they do not actively participate in the trading or holding of crypto assets (and may have no plans to do so), they nonetheless may have an interest in using blockchain technology for internal purposes.
- Differences between CARF and CRS definitions should be limited to situations supported by clear and sound tax policy considerations. Having similar, but slightly different, definitions will be confusing to clients and financial entities and lead to inefficiencies for tax authorities. A few examples of these differences are provided below:
  - The CARF Excluded Person definition (page 17 E 1.) treats listed and regularly traded entities as non-reportable entities. CRS restricts this non-reportable Active NFE type to listed corporations. It would be useful to align the CARF and CRS rules for consistency and clarity.
  - CRS requires reporting and documentation for the Controlling Persons of a Passive NFE. The CARF due diligence rules for Controlling Persons (page 13, B 2.) do not appear to have a defined term equivalent to Passive NFE; instead, these rules apply to an entity that is not an Excluded Person and not an Active Entity. It would be preferable, from an operational perspective, to define the equivalent entity as a "Passive Entity" and align with the CRS definition.
- Finally, we would like to bring to your attention the exploration of possible uses of distributed ledger technology (DLT) for financial asset issuance and settlement activity. Going forward, it may become possible for financial assets to be primarily issued in a private, permissioned DLT network with oversight by a Financial Market Infrastructure (FMI) or other financial institution. The CRS and CARF must remain sufficiently flexible to address evolutionary developments.

- Such FMI or other financial institution, in the example above, may be viewed both as a CRS Financial Institution and as a CARF Reporting Crypto-Asset Service Provider.
- The current CRS framework could be adapted to broaden the scope of CRS Financial Accounts/Account Holders to include 'wallets' and 'wallet holders' and to require the CRS Financial Institution that operates a private, permissioned DLT to include the 'wallets' in scope of its CRS reporting, in which case they are discharged from all CARF reporting obligations to avoid double reporting under both CRS and CARF. Such exclusion is consistent with OECD's policy objective to have CARF applicable to blockchain technology used in a *"decentralised manner, without the need to rely on traditional financial intermediaries or central administrators"*, which is different from a private, permissioned DLT network operated by a CRS Financial Institution.

2. *Comments are also welcomed on all other aspects of amendments to the CRS.*

- Several proposed amendments to the CRS would impose substantial burdens on FIs and provide, at best, very limited benefits to governments.
- A robust and accessible Government Verification Service—implemented by all Participating Jurisdictions—would provide very substantial benefits by:
    - promoting consistency across RFIs within a single jurisdiction; and
    - ensuring more complete and accurate information (as it would have been validated by the local regulator).
- <u>Status of Account as Pre-Existing or New</u>
    - We do not expect many Financial Institutions to have designations as to pre-existing accounts vs. new accounts stored in an electronically searchable format. To the extent that systems record the date on which they treat an account as opened, some indication would exist as to whether an account is "new" or "pre-existing." Any manual search requirement or system update necessitated to ensure accurate pre-existing or new account designations seems overly broad and would have limited value with respect to a fully documented account.
    - Moreover, this additional information might create more confusion than it resolves such as if a customer has multiple accounts to which different due diligence procedures had been provided or when there has been a change of policyholder of a cash value insurance contract.
    - Finally, if an FI reports under the aggregated account reporting option, a differentiation into new and pre-existing accounts might not be possible since an account holder could hold e.g. cash value insurance contracts that qualify as pre-existing accounts while other contracts would have to be reported as new accounts. For reporting purposes, however, only one aggregated account value (i.e. sum of all reportable contracts) will be reported. At least for FIs applying the aggregated account reporting, this new requirement should not be transposed into the Standard or the corresponding Commentary.

- Whether a valid self-certification has been obtained
  - CRS implementation processes vary across financial institutions. From a systems architectural standpoint, there generally is separation between (i) the customer follow-up/case management and (ii) reporting systems (as these fundamental architectural positions were taken based on the law and obligations at the CRS' commencement). Significant systems rebuild would be required to revisit such a foundational aspect of the FI's solution architecture.
  - Information regarding whether a valid self-certification has been obtained, in the majority of instances, is not stored in a searchable format. While some FI's may have added these features into their databases for CRS due diligence and reporting purposes, this information generally is captured only for new accounts. Many systems simply flag an account as reportable. Other financial institutions have a separate system for reportable accounts. Once the information has been inputted into the system, as noted above, the manner in which it was gathered will not necessarily be stored in an electronically searchable format.
  - Even for those FIs that have recorded this information electronically, technical and/or procedural enhancements most likely will be necessary for the information to be retrieved and reported. In all other cases, manual reviews would be required.
  - The costs of revising systems and/or undertaking a manual review will be substantial and outweigh any benefit to tax authorities. Knowing whether a self-certification is on file will provide no additional value if the customer already has been identified as reportable and the relevant information to perform the risk assessment has been reported.
  - Finally, we ask tax authorities to recognize that situations will arise in which an FI has complied fully with its obligations even though something appears amiss. One example illustrating this point involves an account holder who was validly documented at account opening. Following a change in circumstances, the client does not provide a new tax self-certification as per request and therefore reporting is amended to include new indicia. In that case, the original self-certification no longer is valid, and the report would show that no valid self-certification is held. In this situation, however, the FI has complied fully with its obligations.
- Joint Account Information
  - Information regarding joint accounts often will not be available in an electronically searchable format.
  - Financial Institutions, of course, will know whether an account is a joint account. With significant effort and substantial re-work, Financial Institutions may be able to flag and report these accounts. Significant difficulties may arise, however, in extracting the number of joint account holders. Difficulties certainly will arise, for example, in the case of (i) life insurance contracts with a multitude of persons identified as heirs and (ii) an account owned by a Joint Venture between two Passive NFEs with multiple Controlling Persons.
  - Finally, the value of the information is limited—particularly since the relative ownership interest of each joint owner may be well beyond the FI's remit.

- Type of Financial Account
    - It generally should be obvious to the reporting tax authority what type of financial account has been reported by virtue of the entity reporting it. As a regulated industry, an entity will need to be regulated and licenced to provide certain types of accounts. Therefore, we do not see the value of this additional field being added to the reporting schema.
    - If authorities are attempting to use the type of Financial Account to validate the type of income reported, further guidance may be required. For example:
        - Tax laws differ between countries; what is a dividend in the reporting country may be interest in the receiving country(ies) or vice versa. Thus, perfect matching can never be achieved.
        - With respect to a non-custodial/non-depository account, it is not clear whether redemption payments should be reported as Other Income (as would generally be the case for FATCA purposes) or as Gross Proceeds/Redemption payments.
        - Finally, if an FI reports under the aggregated account reporting option, a differentiation into account types might not be possible since an account holder could hold e.g. cash value insurance contracts while other contracts held with the same insurance company are mandatorily to be treated as depository accounts under the current rules (e.g. guaranteed investment contracts, payout-plans etc.). For reporting purposes, however, only one aggregated account value (i.e. sum of all reportable contracts) will be reported. At least for FIs applying the aggregated account reporting, this new requirement should not be transposed into the Standard or the corresponding Commentary.
    - Consequently, if this information is required, we would suggest that the manner in which the information is categorised for each account should be further clarified to ensure consistency of the information reported.
- Temporary Application of Pre-Existing Account Rules for the opening of new accounts without a self-certification
    - While relief for situations in which an account is opened without a self-certification is appreciated, FIs also should be permitted to rely on fallback procedures adopted by their governments to obtain the self-certification after account opening.
- Numbering
    - In general, we suggest using the numbering convention that is used in other OECD publications (e.g., Model Tax Convention). For example, proposed paragraph "6bis" would become "6.1".
- Look-through requirements in respect of Controlling Persons of publicly traded entities
    - We suggest not limiting the exclusion to publicly listed Companies, but expanding it to publicly listed Entities, as the same rationale applies to any publicly listed Entity, such as publicly listed trusts, which in certain jurisdictions may be the only type of Entity entitled to qualify for a particular tax treatment (e.g, real estate investment trust).
- Treatment of corporate trustees and SPV custodians
    - We suggest revisiting the professional accounting/law firm example to clarify that whilst the firm may have received the payment in its own name, it needs to have

done so for the benefit of the corporate trustee for the latter to include such payment as income—as not every payment received by another Entity (e.g., a firm) should be treated as income received by an Entity (e.g., a corporate trustee) for purposes of the gross income test, but only a payment received for its benefit.

- Related Entity definition in case of indirect ownership
    - We suggest revisiting the example as under international tax law (and in a number of jurisdictions under domestic tax law) the indirect ownership of the common parent Entity would typically not be treated as exceeding 50% and, even though Entity A and Entity C would be considered to be connected through the chain of ownership, they would not be treated as Related Entities.