

July 31, 2023

International Organization of Securities Commissions
Calle Oquendo 12
28006 Madrid
Spain

By email: cryptoassetsconsultation@iosco.org

Re: PUBLIC Comment of the Association of Global Custodians on OICU-IOSCO Policy Recommendations for Crypto and Digital Asset Markets Consultation Report CR 01/2023 (May 2023) (the “Report”)

The Association of Global Custodians¹ (the “AGC”) is grateful for the opportunity to comment on the International Organization of Securities Commission’s (“IOSCO’s”) “Policy Recommendations for Crypto and Digital Asset Markets Consultation Report” (the “Report”).²

Introductory comments

The AGC broadly agrees with IOSCO’s principles and goals as set out in the Report and supports its overall objectives to set high standards for the provision of crypto-related services while leveraging existing regulatory frameworks. We believe this is important to establish a well-regulated and stable market for the provision of crypto related services. However, we believe the overarching principle of ‘same activities, same risks, same regulatory outcomes’ should be brought into line with principles articulated by other bodies such as the Financial Stability Board (“FSB”) and the European Commission³, which refer to same “regulation” (in the case of the former) or “rules” (in the case of the latter), but not to “outcomes” *per se*. Regulation should be written and enforced so that market participants and service providers have the benefit of predictability regarding the conduct, operations and

¹ Established in 1996, the Association of Global Custodians (the “Association”) is a group of 12 global financial institutions that each provides securities custody and asset-servicing functions primarily to institutional cross-border investors worldwide. As a non-partisan advocacy organization, the Association represents members’ common interests on regulatory and market structure. The member banks are competitors, and the Association does not involve itself in member commercial activities or take positions concerning how members should conduct their custody and related businesses. The members of the Association are: BNP Paribas; BNY Mellon; Brown Brothers Harriman & Co; Citibank, N.A.; Deutsche Bank; HSBC Securities Services; JP Morgan; Northern Trust; RBC Investor & Treasury Services; Skandinaviska Enskilda Banken; Standard Chartered Bank; and State Street Bank and Trust Company.

² OICU-IOSCO Policy Recommendations for Crypto and Digital Asset Markets Consultation Report CR 01/2023 (May 2023) (the “Report”), available at <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf>.

³ See, Financial Stability Board, *Global Regulatory Framework for Crypto-Asset Activities* (17 July 2023), p.1. Available at: <https://www.fsb.org/2023/07/fsb-finalises-global-regulatory-framework-for-crypto-asset-activities/>. See also, Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/193 (“MiCA”), Recital 9. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/>

processes they are expected to perform. “Rule” or “regulation”-based principles do this while a focus on “outcomes” implies the possibility of being held responsible for outcomes without regard to the adequacy of performance or compliance with legal or regulatory conduct requirements. We would caution against a goal of making outcomes the “same” without regard to whether regulated firms comply with appropriate legal and regulatory requirements.⁴

In addition, this overarching principle (albeit referring to “rules” or “regulations” instead of “outcomes”) should apply not only to tokenized traditional financial instruments but also more broadly so that financial services activity in the context digital ledger technology (“DLT”) is addressed and regulated in the same manner as “traditional” financial activity: underlying this premise is that DLT, in effect, is a tool that can be used to achieve effective, efficient and safe outcomes for investors and for financial markets. For example, DLT may be used for a firm’s internal books and records: this does not present the same considerations as *tokenization* of assets using DLT and therefore should not result in assets that are recorded by an intermediary using such technology being treated as “crypto-assets”. What is important is that the firm in this example should be regulated and supervised in such a way as to ensure operations and processes utilizing DLT are as safe and sound as any other operations and processes carried out by the firm. DLT is a means and not an end unto itself and should therefore be treated as such, i.e., regulation of relevant activities, investible instruments and market participants and service providers should be “technology neutral”.⁵ Such a technology-neutral approach is necessary to avoid regulatory arbitrage and to adequately protect consumers’ and investors’ expectations in a way that aligns with broader financial services regulation.

While, while the goal should achieve as much consistency with existing financial services regulation as possible, IOSCO should also recognize that some important distinctions across types of tokenized investments are inevitable due to different market infrastructures and other differences, resulting in different kinds of access to investments. As we point out in our response to Question 1 below, the risk profiles of different types of DLTs — “private-permissioned” versus “public-permissionless”, for example — can vary significantly. For example, on a private-permissioned network, the use of DLT presents limited, if any, incremental risks that arise in the context of leveraging or improving existing systems and legal frameworks (e.g., a highly regulated Central Securities Depository as a central governance framework utilizing DLT). Where a public-permissionless network is utilized to access an investment, DLT may present different risks. In the latter instances, we believe that, rather than taking a highly inappropriate “one-size-fits-all” approach, regulatory authorities should ensure that firms apply existing and appropriately adjusted risk mitigation practices and technologies to manage and mitigate risk.

Different risk profiles are dependent on types of digital assets, too, and these risks are likely to evolve. Focusing specifically on cryptocurrencies and other tokenised assets that are native to the blockchain, as investment in these types of digital assets are brought more fully into the regulatory ecosystem, they will become integrated into existing regulatory structures that

⁴ We expand on this in our response to Question 2, below.

⁵ See, e.g., UNIDROIT Principles on Digital Assets and Private Law (the “UNIDROIT Principles”), adopted 12th May 2023, Introduction, Part II. Available at: <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/>. See also

address the risks of money laundering, terrorist financing, and sanctions evasion. By permitting highly regulated financial institutions to hold and transfer cryptocurrencies and other block chain native assets, regulatory authorities will bring them from pseudonymous open networks into a regulated regime that requires “Know Your Customer” diligence, anti-money laundering and transaction monitoring diligence and travel rule obligations. Conversely, if regulated financial institutions are prohibited or disincentivized from custodying or transacting these kinds of assets on behalf of their customers, they will be pushed into unregulated or less-regulated environments, increasing the potential for money laundering, terrorist financing, and sanctions evasion.

While the recommendations cover the entire set of services across the entire trade life cycle, the focus of AGC’s submission is on the custody and safeguarding of tokenised financial assets. We direct IOSCO’s attention to submissions of other industry associations for recommendations and questions that we have not focused on, most notably the submission of the Global Financial Markets Association (“GFMA”).

CHAPTER 1: OVERARCHING RECOMMENDATION ADDRESSED TO ALL REGULATORS

Chapter 1 Questions:

Question 1: – Are there other activities and/or services in the crypto-asset markets which Recommendation 1 should cover? If so, please explain.

RESPONSE:

The AGC agrees with IOSCO that the global nature and certain unique characteristics of the crypto-asset market require “the application of robust regulatory standards alongside international regulatory cooperation” to help ensure that “any useful innovation can occur without the risk of regulatory arbitrage and lessening standards of investor protection and market integrity.”

In the context of “custody” services, because we agree that crypto and digital markets can only develop safely and efficiently if rules applicable to CASPs are consistent, we emphasise that high-quality standards should apply equally to any party providing custody-related services in a manner that is similar to “traditional” financial asset custody services today. An adequate balance needs to be struck between allowing innovation and avoiding the potential for misbehaviour and insufficient consumer protection. We therefore welcome the approach of CPSS-IOSCO to develop high, consistent standards.

Global custodians have a long history and much expertise in providing post-trade services for “traditional” financial assets: recommendations should leverage our collective expertise and allow for the provision of crypto custody services by global custodians alongside and on the same terms as other players – premised (again) on the principle of same activity, same risk, same rules. Only by maintaining high standards and by allowing the possibility for established custodians to provide custody services in this market in line with the above principle, can the market grow for the benefit of investors and financial markets

We would add however that these regulatory standards need to take into account broader considerations so that they are integrated as harmoniously as possible into all relevant law and regulation in order to achieve desired outcomes. We emphasise the following two aspects:

- i. The need to take into account other relevant law and regulation: Regulation promulgated by securities regulators should be mindful of other relevant law and regulation – such as banking law and regulation – which may also bear on relevant parties such as CASPs. Such regulation also should reinforce – and are reinforced by – substantive national law such as law bearing on property rights, insolvency, etc. In other words, securities regulation does not and should not operate in a vacuum: inattention to the broader context risks sowing confusion and, worse, risk that securities regulators may not be in a position to anticipate. This is particularly true in the context of banks. For example, custody and ancillary banking services should be offered on consistent terms by regulated and adequately capitalised banking institutions, subject to strict prudential regulatory supervision and controls.

We discuss these risks in more detail in our responses to questions asked in Chapter 7 below.

- ii. The need to take account of the distinction between tokenised securities and other instruments that are subject to existing legal frameworks versus those crypto-assets that are not: The differentiation between regimes applicable to security tokens⁶ and those applicable to other crypto-assets⁷ appears to be already recognized/implemented in certain countries and regions.⁸ More “traditional” assets that are tokenised have generally been brought into alignment with similar assets that have not been tokenised, while those that present different or novel risks have required different approaches.⁹ As a result, addressing tokenised securities and similar “traditional” assets and all other crypto assets in the same way could raise difficulties and potential incompatibilities with regional and national law approaches.

⁶ For example, traditional MiFID financial instruments being tokenized, tokenised “securities entitlements” under UCC Article 8 in the United States or tokenised securities treated as choses in action under existing English law.

⁷ For example, crypto-assets under the European Union (EU) Markets in Crypto-Assets Regulation (MiCA), “controllable electronic records” (“CERs”) under UCC Article 12 in the United States or “digital objects” as proposed by the UK Law Commission as a new form of property right under the law of England and Wales.

⁸ Examples include (i) the differentiation between assets subject to MiCA versus those that will be subject to the DLT Pilot Regime in the EU, (ii) the emerging difference in the UK between tokenised assets treated as intangible property (“choses in action”) following existing English law principles versus those to be considered a new form of property to be called “Digital Objects”; and (iii) the difference in the United States between tokenised assets to be treated as “securities entitlements” under UCC Article 8 versus those considered “controllable electronic records” under UCC Article 12. Recently approved “Principles” by UNIDROIT defer to “other law” where the distinction emerges. Available at: <https://www.unidroit.org/instruments/capital-markets/geneva-convention/>

⁹ See, Basel Committee on Banking Supervision, *Prudential Treatment of Crypto asset Exposures*, (Bank for International Settlements, December 2022) (“BCBS Standards”). Available at: <https://www.bis.org/bcbs/publ/d545.htm>

Question 2: – Do respondents agree that regulators should take an outcomes-focused approach (which may include economic outcomes and structures) when they consider applying existing regulatory frameworks to, or adopting new frameworks for, crypto-asset markets?

RESPONSE:

It is crucial that any approach to be implemented by regulatory authorities coheres with other relevant law and regulation, especially those bearing on prudential banking regulation, property rights and insolvency. We appreciate that IOSCO’s Recommendation 2 recommends achieving regulatory “outcomes” for investor protection and market integrity that are “the same as, or consistent with, those that are required in traditional financial markets”, however, we strongly emphasise the need to take into account all relevant areas of law and regulation, especially if deference to these other areas may be the better course depending on the nature of a particular asset, the activity being undertaken, the size or sophistication of the parties involved or whether and the extent to which existing market structures and legal frameworks already address relevant risks. As we point out in our response further below, certain distinctions may need to be made that suggest deference to other areas of law and regulation – particularly as they relate to “traditional financial markets”. An “outcomes-focused” approach that seeks to reinvent the wheel where other, more relevant law and regulation already fully applies could create confusion.

Considerations that bear on the extent to which an outcomes-focused (or alternative) approach can or should be adopted include:

1. Liability of the CASP: elements relating to the liability of the custodian are not addressed in IOSCO’s Report. While it is possible this may be left to divergent national law approaches, harmonisation would likely be beneficial to investors and service providers alike by providing for greater predictability of outcomes. This is a crucial element as the decision to engage in the provision of services is driven in part by the applicable liability regime (to assess the exposure of the service provider in case of a loss). In doing so, the right balance needs to be struck between ensuring adequate investor protection and allowing the provision of custody services on reasonable terms.

The European Union has embarked on such an approach under the Markets in Crypto Assets (MiCA) Regulation¹⁰ by clarifying that custodians cannot be held liable for elements which are outside of their control. We support clarifying in similar terms that a CASP providing custody services is not liable for incidents that are not attributable to them/under their control. Liability should be capped to the amount of the market value of the assets lost at the time such loss occurred. This is especially relevant for public permissionless networks where market infrastructure is not owned or operated by a single, highly supervised entity such as a CSD

¹⁰ MiCA was adopted by the European Parliament 20th April 2023.

2. Definition and scope of CASP activities: Page 1 of the Report provides the following definition of a CASP:

CASPs are service providers that conduct a wide range of activities relating to crypto-assets, including but not limited to, admission to trading, trading (as agent or principal), operating a market, custody, and other ancillary activities such as lending / staking of crypto-assets and the promotion and distribution of crypto-assets on behalf of others.

There are two main problems with this approach which derive from (i) using a single concept of a CASP, and (ii) only regulating CASPs, and not regulating parties that are not CASPs.

The first problem is that the scope of the definition of a CASP is too limited, so that there is the possibility that some relevant parties, including, notably, issuers, are not treated as CASPs and are therefore potentially entirely outside the purview of regulation even where they provide some elements of activities defined as CASP activities in the Report. Unregulated entities could carry out relevant activities, creating extra burdens on CASPs in order to compensate for the risk associated with the unregulated entities.

The second problem is that, even if not comprehensive, the concept of a CASP will, nonetheless, cover many different types of activities, and individual CASPs may carry out only one or two of these activities (for example, just custody activities). What this means is that generic obligations on CASPs, - for example, to provide certain types of information – may be inappropriate to the particular scope of a CASP’s service offering or otherwise unnecessarily burdensome. Further distinctions therefore should be made, leveraging existing regulatory frameworks that are tailored to the nature of the services provided by the CASP.

3. Risk of double regulation: The obligations placed on CASPs may create the risk of double – and possibly or inconsistent or contradictory - regulation, as some jurisdictions may already have rules in place covering entities other than CASPs. One example of this problem in the Recommendations is the text regarding stablecoins, and the proposed obligations on CASPs relating to stablecoins (see question 21): in the EU, MiCA contains detailed rules relating to stablecoin issuers.

Another example is the way in which banks operate and are regulated and supervised: prudential regulatory authorities typically impose stringent requirements regarding custody of customer assets, which would include any crypto assets. Just as securities regulators have had to do, these bank regulatory authorities have had to adapt to new technology such as DLT. One set of rules imposed by securities regulators that conflict or are inconsistent with another set of rules imposed by bank regulators may sow confusion and increase operational risk if banks are forced to balkanise their processes due to different, incompatible regulatory pressure points. Recognition by securities regulators of the adequacy of regulation in these other areas – where other authorities have “primary” authority – has long been adopted as an approach for

resolving potential incompatibilities.¹¹ This of course assumes that bank regulatory authorities indeed conduct the necessary assessment and promulgate the necessary regulation themselves, which we have already started to see¹² and encourage. We see no reason why a similar approach should not be adopted by securities regulators as it would relate to CASPs.

CHAPTER 7: RECOMMENDATIONS ON CUSTODY OF CLIENT MONIES AND ASSETS

Chapter 7 Questions:

Question 14: – Do the Recommendations in Chapter 7 provide for adequate protection of customer crypto-assets held in custody by a CASP? If not, what other measures should be considered?

RESPONSE:

As alluded to above in our response to Question 1, the Recommendations in Chapter 7 need to take into account broader considerations so that they are integrated as harmoniously as possible with all relevant law and regulation in order to achieve desired outcomes. Regulation promulgated by securities regulators should be mindful of other relevant law and regulation – such as banking law and regulation – which may also bear on relevant parties that may act as CASPs. Such regulation also should reinforce – and are reinforced by – substantive national law such as law bearing on property rights, insolvency, etc.

As stated in the introduction, the AGC supports a robust, well-structured regime for the protection of client assets generally. A regime focused on crypto/digital assets should align where possible with current requirements and practices that have proven their value over a long period of time in the custody space. Custody and safeguarding services should be performed by adequately licensed, capitalised entities, which are subject to prudential regulatory supervision. Such an approach would seem even more important with respect to “custody” of crypto-assets made available over public/permissionless networks, where there

¹¹ For example, “equivalence” – as opposed to wholesale extraterritorial imposition of domestic requirements - as a means of gauging the adequacy of foreign legal, regulatory and supervisory approaches. As the European Commission has explained:

EU equivalence has become a significant tool in recent years, fostering integration of global financial markets and cooperation with third-country authorities. The EU assesses the overall policy context and to what extent the regulatory regimes of a given third country achieves the same outcomes as its own rules. A positive equivalence decision, which is a unilateral measure by the Commission, allows EU authorities to rely on third-country rules and supervision, allowing market participants from third countries who are active in the EU to comply with only one set of rules.

European Commission, *Financial services: Commission sets out its equivalence policy with non-EU countries*, (29th July 2019). Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4309.

¹² See, BCBS Standards and recent proposals under discussion in the EU under the Capital Requirements Directive (“CRD VI”).

may not be a centralised, highly regulated governance framework (such as a CSD) to the holding of the assets.

While the provision of custody services is an essential part of the package provided by CASPs, IOSCO should consider whether the safeguarding of these assets should be entrusted to specifically licensed institutions such as custody banks. Especially if the services entail the provision of settlement and asset servicing, where cash and liquidity management is an integral part of the service offering (e.g., to support DvP settlement), it is important to ensure that the taking of deposits and the provision of settlement liquidity, necessary currency conversion services and cash management services are provided through adequately capitalised banks, subject to banking rules and capital requirements, and under the supervision of prudential banking authorities (see also our comment below regarding treatment of money).

It is essential that in prescribing requirements to segregate Client Assets or place them in trust – as for example set out in **Recommendation 13** – that there is a distinction made between CASPS which are not adequately regulated as banks, and CASPS which have a full banking license and are strictly regulated and supervised as such. All global custodians today are regulated banks and as a result they are subject to high standards and levels of control, supervision and prudential regulatory oversight, including where they provide custody services to clients. Investors benefit from this when entrusting financial assets to such providers for safekeeping.

Question 15: –

(a) Should the Recommendations in Chapter 7 address the manner in which the customer crypto-assets should be held?

RESPONSE:

(a) We address crucial elements that we believe IOSCO must take into account in addressing the manner in which customer crypto-assets should be “held”:

- i. Treatment of money: We note that OICU-IOSCO describes “Client Assets” as both money and crypto-assets held for, and on behalf of, a client.¹³ Cash should **not** be treated in the same way as crypto/digital assets for purposes of recommendations relating to digital/crypto assets. The reason for this lies in what distinguishes cash from other assets held or maintained as “property” of customers: cash deposits maintained with banks are subject fully to bank prudential regulation and are maintained on bank balance sheets as deposits (“as banker”) and therefore are liabilities of banks to customers.

While it is already standard practice for custodians to segregate client assets such as securities and other non-cash assets - in order to ensure that the assets are bankruptcy remote from the custodian – this is **not** the case with respect to cash balances maintained by bank custodians.

¹³ See, Report, footnote 26, p. 31.

Whether or not “money” is considered a part of “Client Assets” subject to IOSCO’s recommendations, there needs to be recognition – as is the case today in many jurisdictions - that CASPs which are licensed and operate as banks are not required to segregate money if it held by them on deposit (i.e., as “banker”), subject to disclosure requirements of the risks of deposits in the event of the bank’s insolvency. As is the case today, non-bank custodians can be required to open up segregated cash accounts on the books of adequately regulated and capitalised banks (ensuring that client cash is bankruptcy remote from the non-bank custodians), but those banks should - as they do today- be allowed to maintain this cash as a general deposits and use it for general banking purposes. This is important for custody banks to operate efficiently in the provision of services (such as currency conversions, liquidity management, etc.) and to fulfil their core economic functions as banks. Given that they are subject to high prudential regulatory standards, investors can derive comfort by keeping their cash with such banks, without imposing unnecessary and costly requirements for segregation, which would prohibit established custody banks from providing custody services for crypto assets and which would be fundamentally inconsistent with the role of banks in the financial system.

- ii. Importance of deference to national law on property rights: “custody” fundamentally speaks to the maintenance of property interests on behalf of customers. It has been widely noted by legal bodies such as UNIDROIT, the UK Law Commission and the U.S. Uniform Law Commission¹⁴ that this tends to be a crucial consideration in the context of insolvency of either an intermediary or relevant market infrastructure such as a central securities depository (CSD) or other FMI. A recent decision of the General Division of The High Court of Singapore clarified that crypto assets can be “held on trust” as “choses in action”¹⁵: this is similar to the approach recommended by the UK Law Commission, with similar advantages for rightful owners.

¹⁴ The UNIDROIT Principles, *e.g.*, provide that proprietary rights that have been made effective against third parties are generally effective against an insolvency representative. *See*, UNIDROIT Principles, Principle 19. The UK Law Commission, providing a detailed assessment of insolvency aspects in its recently published report, explained that in the event of the custodial holding intermediary entering an insolvency process, “entitlements would ordinarily not form part of the holding intermediary’s estate and would not be available to meet the claims of its general creditors”, but the explained further:

In a custodial intermediated holding arrangement involving segregated assets held in their totality on trust for (or otherwise subject to the superior title of) a third-party beneficiary or superior title holder, a custodial holding intermediary’s general creditors will have no claim to those assets at all. However, where more complex structures are deployed, such as funds of commingled holdings held on behalf of a number of third parties and the intermediary itself, a portion of the value of such holdings representing the holding intermediary’s co-ownership entitlement can fall into the bankruptcy estate and be subject to claims of general creditors.

UK Law Commission, *Digital Assets: Final Report*, Law Com No. 412 (2023), Para. 7.26, p. 153. Available at: <https://www.lawcom.gov.uk/project/digital-assets/>. The AGC fully agrees with this assessment and notes that it is in accord with our views on effective segregation arrangements articulated in this response.

¹⁵ *See, ByBit Fintech Limited V Ho Kai Xin & Ors.* [2023] SGHC 199. It should be noted, however, that the approach taken in the UK will make a further distinction between “choses in action” and “data objects”, with

Whether and to what extent a CASP can protect a customer's property rights through appropriate custody arrangements must draw on whether the relevant legal framework under which the CASP operates supports rights in such assets as right *in rem*. This should be distinguished from situations in which the customer has contract rights – rights *in personam* – which are not covered in the same way by national law frameworks. In the latter case, a custodian may maintain a record as an accommodation to the client – or it may be required to do this under sectoral law or regulation – but the custodian would not be in a position to intermediate the rights to these assets or to ensure an outcome designed to achieve insolvency remoteness with respect to contract rights running between a client and a third party such as an issuer. Indeed, assets that represent rights *in personam* by their nature inherently involve risk that the customer/investor will be an unsecured creditor *vis a vis* an insolvent counterparty who has not performed its obligations under the arrangement (except to the extent the arrangement is secured with collateral).

Moreover, in cases of assets involving rights *in personam*, the custodian cannot control disposition of a customer's rights, since the customer itself – or its designated agent (such as an investment manager) – would retain sole instruction authority *vis a vis* the counterparty (see, e.g., OTC derivatives). There is no reason why this premise would change solely because of the technology used to connect investors to counterparties who may utilise digital ledger technology (in particular smart contracts) in place of existing document-based approaches.

This distinction between rights *in rem* and rights *in personam* is a fundamental precept of traditional finance as well as the legal (including insolvency) frameworks under national law: there is no reason why this would change in the context of crypto assets.

- iii. Linked assets: we believe securities regulators should carefully consider situations in which underlying assets are “linked” or “tethered” crypto assets: such situations create the prospect of an electronic record associated with the crypto asset being accorded property rights under national law, but rights in the underlying (“linked”) asset not necessarily flowing with them.¹⁶ Whether and to what extent a link to underlying rights is sufficiently established may vary by legal jurisdiction.
- iv. Omnibus accounts: Recommendation 14, sub(iii), would require disclosure of the extent to which Client Assets are “aggregated or pooled within omnibus client accounts, the rights of individual clients with respect to the aggregated or pooled assets, and the risks of loss arising from any pooling or aggregating activities”. The AGC fully supports transparency and disclosure of risks to clients and also strongly

different attributes for each and the latter constituting a “new” form of property right (which the Singapore court rejected in dictum).

¹⁶ See, UNIDROIT Principle 4, which provides that law other than the Principles (e.g., relevant national law) will determine the contractual and proprietary effects (if any) of the link to another asset. Principles law takes a neutral stance as to whether this link is sufficiently established and what, if any, the legal effect of the link may be. These matters are instead left to the other law of the State, including its regulatory law, to determine.

supports full segregation of client positions so that their rights and entitlements in custodied assets are adequately identified in relevant books and records of custodians and FMIs. However, there needs to be a proper understanding of the role of so-called omnibus accounts and the manner in which they are utilised safely and efficiently. “Pooled” accounts should not be confused with “omnibus” accounts where the latter are utilised properly. Omnibus accounts in traditional finance are used extensively by intermediaries as essential tools for connecting “many” investors to “many” investments in which they invest (typically, book-entry securities) where the investments typically are immobilised and dematerialised at central market infrastructures such as CSDs. In other words, full and proper segregation of client assets (both from proprietary assets and also assets of other customers) can and do exist *at the same time* as omnibus accounts maintained by intermediaries further up the chain of custody.¹⁷ This does not mean that client accounts are “pooled” since segregated positions are maintained for each client on the books of the custody bank, with custody records reflecting this: the full amounts of these segregated positions mathematically correlate to omnibus accounts up the chain, with positions reconciled as required among intermediaries and any FMIs through the chain.

(b) How should the Recommendations in Chapter 7 address, in the context of custody of customer crypto-assets, new technological and other developments regarding safeguarding of customer crypto-assets?

RESPONSE:

We agree with other authorities that regulation should strive for “technology neutrality” and that existing legal and regulatory frameworks should be utilised wherever possible (see, e.g., UK and U.S.).

Regarding the use of cold vs hot wallets and the management of private keys, regulations should not be overly prescriptive regarding the way in which assets are held so long as the service providers adhere to high standards regarding the protection of client assets, and leverage the technological progress which is constantly made in these areas.

(c) What safeguards should a CASP put in place to ensure that they maintain accurate books and records of clients’ crypto-assets held in custody at all times, including information held both on and off-chain?

RESPONSE:

We encourage the application of standards on regular and frequent reconciliation between the CASPS own books and the holdings and transactions on crypto platforms for as long as CASPS maintain their own independent set of books and records. It is also important to have clarity on when transactions are deemed final and irreversible (“settlement finality”) and base reconciliation on these final and undisputed records.

¹⁷ We add, however, that omnibus accounts should not contain proprietary assets of the CASP anywhere in the chain.

(d) Should the Recommendations in Chapter 7 include a requirement for CASPs to have procedures in place for fair and reliable valuation of crypto-assets held in custody? If so, please explain why.

RESPONSE:

No. Custodians can provide indicative values based on available pricing sources, but that valuation is not a core service of custodians and investors should employ their own valuation methods (as they do today). Custodians should disclose that values that are provided are indicative and not to be relied upon for pricing and valuation purposes (which the client can source from specialised providers or market makers).

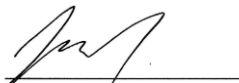
Question 16: – Should the Recommendations address particular safeguards that a CASP should put in place? If so, please provide examples.

RESPONSE:

We agree with GFMA that regulators should require a CASP, as relevant based on the services provided by the CASP, to adopt appropriate systems, policies and procedures to mitigate the risk of loss, theft or inaccessibility of Client Assets. Regulations should take into account existing operational risk capital requirements and provide for limitations on liability, including that: (1) a CASP acting as custodian should not be liable for losses incurred due to events outside of the CASP's control; (2) any compensation for loss should be capped at the market value of the lost crypto-asset at the time of the loss; and (3) CASPs and professional or institutional clients should be able to negotiate limitations on liability, subject to appropriate minimum requirements.

The members of the AGC welcome IOSCO's efforts to ensure a harmonised global framework for digital assets is established so that investors receive necessary certainty and protections in line with standards that have long been in place for "traditional" financial services activities and assets. We look forward to engaging with IOSCO throughout its deliberations and would welcome any dialogue. Please do not hesitate to reach out to the association with any questions or comments regarding this submission.

Sincerely,



John Siena

Chair, European Focus Committee, on behalf of:
ASSOCIATION OF GLOBAL CUSTODIANS
john.siena@bbh.com
www.theagc.com