July 31, 2023

Via Electronic Submission

General Secretariat
International Organization of Securities Commissions (IOSCO)
C/ Oquendo 12
28806 Madrid
Spain

RE: Public Comment on IOSCO's Consultation Report on Policy Recommendations for Crypto and Digital Asset Markets

Dear General Secretariat:

The Independent Community Bankers of America ("ICBA")[1] appreciates the opportunity to provide comments to the International Organization of Securities Commissions ("IOSCO") Consultation Report of Policy Recommendations for Crypto and Digital Asset Markets.[2] America's community banks have a strong interest in ensuring that digital assets, such as stablecoins issued by non-bank entities, do not harm investors, consumers, or the financial system. ICBA and its members appreciate IOSCOs efforts to (i) advance the potential benefits of cryptoassets while understanding and accounting for potential risks, particularly in light of the growing interconnectedness of such cryptoassets and commensurate risks to financial stability, and (ii) coordinate the efforts of national regulatory authorities as jurisdictions consider how to develop policy standards and solutions to support new technologies within the banking system.

[1] *The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services. With nearly 50,000 locations nationwide, community banks employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding $5.8 trillion in assets, $4.8 trillion in deposits, and $3.8 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at* ***www.icba.org***.

[2] OICU-IOSCO, Policy Recommendations for Crypto and Digital Asset Markets Consultation Report (May 2023), available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf.

WASHINGTON, DC
1615 L Street NW
Suite 900
Washington, DC 20036

SAUK CENTRE, MN
518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

866-843-4222
www.icba.org

General Comments

ICBA and its members support IOSCO's efforts to promote "optimal regulatory consistency" as we recognize that international collaboration and cooperation are vital to address the myriad risks of cryptocurrencies and crypto asset service providers. ICBA and its members support coordination and cooperation both across and within jurisdictions to ensure consistency and harmonization of regulatory and supervisory outcomes for cryptoassets, firms, and activities, with appropriate flexibility for implementation of domestic priorities and to address unique characteristics of national level financial markets and structures. ICBA supports IOSCO playing a leading role in helping to facilitate coordination and communication across jurisdictions to ensure regulatory harmonization and adequately address crypto's unique cross-border risks. Similarly, we have previously expressed support for the Financial Stability Board's ("FSB's") efforts to develop recommendations for the international regulation, supervision, and oversight of cryptoassets and global stablecoins.

We view IOSCO's recommendations as prudent steps to safeguard the financial system against the risks of cryptoassets and increase investor protections. Regarding investor protection, we are particularly concerned with vertical integration within the cryptoasset space. As evidenced by FTX's collapse, the potential for market manipulation and the misappropriation of customer funds increases when a single parent company controls a variety of subsidiaries that act as broker/dealer, exchange, and proprietary trading firm. There must be bright lines and clear disclosure about companies acting as broker/dealers, securities issuers, and exchanges, and when they are doing so in the context of any given transaction.

Finally, we continue to express opposition to the potential ability of cryptoasset companies to access a "Master Account" at the United States Federal Reserve. Federal Reserve Master accounts allow account holders to access the Federal Reserve's wholesale payments systems and other payment services. Access to these accounts must be limited to traditional, regulated financial institutions like banks because granting access to crypto companies could provide a false imprimatur of credibility – for example by implying that the Federal Reserve is endorsing a particular crypto asset or token, or equating its value to that of the US dollar. In addition, access to these services may make it much faster for account holders to translate cryptoassets into dollars, making it more difficult to recover funds in the event of a fraud.

In our view, it is imperative to the stability of the financial system that those who have access to Federal Reserve services are regulated by specialists who can review a financial institution's compliance with laws and generally accepted business practices and thus expect safety and soundness in the participants – cryptoasset companies do not fit that bill.

Most Cryptocurrencies are Securities and Should be Regulated as Such

ICBA supports IOSCO's call for regulators to consider the applicability of their frameworks that they should consider cryptoassets to be regulated financial instruments. As we recently argued in a comment letter to the U.S. Securities and Exchange Commission ("SEC"),[3] most cryptoassets in the United States likely qualify as a security per the criteria established by the Howey Test. ICBA views SEC regulation and enforcement of the crypto sector as critical to protect investors and minimize risks to financial stability.

More recently in *Securities and Exchange Commission v. Ripple Labs (SEC v. Ripple)*, 20-civ-10832 (AT), (S.D.N.Y. July 13, 2023) the United States District Court for the Southern District of Texas held that Ripple's sales of its crypto token "XRP constituted the unregistered offer and sale of investment contracts in violation of Section 5 of the Securities Act." In that scenario – where Ripple Lab's XRP token was sold pursuant to written contracts to institutional buyers "who would have understood that Ripple was pitching a speculative value proposition for XRP with potential profits to be derived from Ripple's entrepreneurial and managerial effort" – Ripple Labs failed to show any genuine dispute as to any material fact that it engaged in an unregistered securities offering, entitling the SEC to judgment as a matter of law.

In our view, *SEC v. Ripple,* is a vindication of our view that, when cryptocurrencies are offered for monetary consideration with the expectation that they will appreciate in value due to the entrepreneurial and managerial effort of their offerors, including those who provide the processing power to operate and maintain their distributed ledgers, then they are securities. As such, most cryptoassets should likely be subject to the registration and regulation of more conventional securities instruments.

Response to IOSCO Recommendations

- **Recommendation 1 –** *Regulators should use existing frameworks or New Frameworks to regulate and oversee crypto-asset trading, other crypto-asset services, and the issuing, marketing and selling of crypto-assets (including as investments), in a manner consistent with IOSCO Objectives and Principles for Securities Regulation and relevant supporting IOSCO standards, recommendations, and good practices (hereafter "IOSCO*

[3] Independent Community Bankers of America, "Comment Letter RE: Reopening of the Comment Period: Proposed Amendments to Exchange Act Rule 3b16 [File No. S7-02-22]" (June 13, 2023), (available at: https://www.icba.org/docs/default-source/icba/advocacy-documents/letters-to-regulators/comments-on-rule-3b-16-exchange-definition.pdf?sfvrsn=267ded17_0) (in which we argue that: "Put simply, cryptocurrencies, while novel, should not be exempt from existing legal and regulatory frameworks'… and that , 'ICBA and its member banks believe almost all cryptocurrencies primarily serve as highly volatile investments with identifiable entities responsible for managing the protocol and seeking to increase the value of any related tokens. Accordingly, we believe this activity clearly meets the criteria set forth in the landmark Supreme Court case *Securities and Exchange Commission v. W.J. Howey Co*.'"

Standards"). The regulatory approach should seek to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets.

In general, we agree with this recommendation, particularly to the extent that IOSCO's observation is true that:

(1) cryptoassets are, or behave like substitutes for, regulated financial instruments, and
(2) investors have substituted other financial instrument investment activities with crypto asset trading activities.

If investors view cryptoassets as substitutes for – or even equivalent to – regulated financial instruments like securities, then it is logical for government to apply the same principles of investor protection and market transparency that it does to other financial markets. In the United States, we do not believe this will require the creation of a new regulatory framework or supervisory body, because we believe most cryptocurrencies are securities and can be regulated within the existing framework of securities laws – including registration with the SEC, supervision of brokerages, and exchanges.

- **Recommendation 2 –** *Regulators should require a CASP (crypto asset service provider) to have effective governance and organizational arrangements, commensurate to its activities, including systems, policies and procedures that would, amongst other things, address conflicts of interest, including those arising from different activities conducted, and services provided by a CASP or its affiliated entities. These conflicts should be effectively identified, managed and mitigated.*

  A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions, and may require more robust measures such as legal disaggregation and separate registration and regulation of certain activities and functions to address this Recommendation.

In our view, one of the most apparent risks presented by crypto companies is their tendency to act as vertically-integrated one-stop shops– issuers of a security, broker-dealers that act as their customers' intermediary in trading that crypto security, and exchanges where the crypto security is traded. Regulators should conclude that such clear conflicts of interests are so acute that they cannot be mitigated, and instead should break the cryptocurrency market into its constituent parts. Failure to do so may lead to more failures like that of FTX.

In the United States, that would likely mean that any company or other group that wishes to create a cryptocurrency, including its underlying blockchain and any additional software

development, should register that cryptocurrency as a security with the SEC and file the required periodic disclosure. Companies that facilitate the sale of cryptocurrencies for others should register as broker/dealers. Likewise, those who would act as exchanges for cryptocurrencies should register as national securities exchanges and become subject to SEC oversight.

- **Recommendation 3 –** *Regulators should require a CASP to have accurately disclosed each role and capacity in which it is acting at all times. These disclosures should be made, in plain, concise, nontechnical language, as relevant to the CASP's clients, prospective clients, the general public, and regulators in all jurisdictions where the CASP operates, and into which it provides services. Relevant disclosures should take place prior to entering into an agreement with a prospective client to provide services, and at any point thereafter when such position changes (e.g., if and when the CASP takes on a new, or different, role or capacity).*

In principle, we agree with this recommendation, though as discussed above, not all conflicts of interest may be adequately remedied by disclosure.

- **Recommendation 5 –** *Regulators should require a CASP that operates a market or acts as an intermediary (directly or indirectly on behalf of a client) to provide pre- and post-trade disclosures in a form and manner that are the same as, or that achieve similar regulatory outcomes consistent with, those that are required in traditional financial markets.*

We agree with this recommendation and believe that CASPs who operate in the manner described should register with the SEC as broker-dealers in the United States.

- **Recommendation 6 –** *Regulators should require a CASP to establish, maintain and appropriately disclose to the public their standards— including systems, policies and procedures— for listing / admitting crypto assets to trading on its market, as well as those for removing cryptoassets from trading. These standards should include the substantive and procedural standards for making such determinations.*

This recommendation is appropriate. It is appropriate for exchanges and other market makers to establish and disclose listing standards for securities in which they make a market. Doing so provides transparency and helps to ensure there is sufficient liquidity and market interest in a given security.

- **Recommendation 7** – *Regulators should require a CASP to manage and mitigate conflicts of interest surrounding the issuance, trading and listing of crypto-assets. This should include appropriate disclosure requirements and may necessitate a prohibition on a CASP listing and / or facilitating trading in, its own proprietary crypto assets, or any crypto assets in which the CASP, or an affiliated entity, may have a material interest.*

In our view, there must be clear disclosure of when crypto companies are engaging in the trading of cryptoassets where they are an issuer. In particular, it is problematic when a crypto company or its affiliated companies trade in the secondary market for a crypto security issued by their own affiliate without disclosure. For example, third party research indicates that, with regards to FTX, up to 86% of the FTX issued FTT token were controlled by FTX and its affiliated proprietary trading firm Alameda Research.[4] With that level of control of the supply of FTT, FTX/Alameda could easily manipulate the price, to the detriment of individual investors in the FTT token. Timely disclosure of this concentrated stake may have limited the investor harm, as might restrictions on Alameda's ability to trade/control a high percentage of a token issued by its affiliated entity.

- **Recommendation 8** – *Regulators should bring enforcement actions against offences involving fraud and market abuse in crypto-asset markets, taking into consideration the extent to which they are not already covered by existing regulatory frameworks. These offences should cover all relevant fraudulent and abusive practices such as market manipulation, insider dealing and unlawful disclosure of inside information; money laundering / terrorist financing; issuing false and misleading statements; and misappropriation of funds.*

ICBA agrees with this statement, but we believe that the United States would have an adequate regulatory and enforcement framework if cryptoassets are deemed to be securities. The SEC's' Division of Enforcement already has the authority to investigate and bring cases against securities fraudsters, including those participating in fraudulent initial coin offerings or ICOs. Additionally, the U.S. Department of Justice has established the National Cryptocurrency Enforcement Team to investigate and prosecute crypto-related crime.

[4] Zhiyuan Sun, Coin Telegraph, "FTX and Alameda likely colluded from the very beginning: Report" (Nov 17, 2022), available at: FTX and Alameda likely colluded from the very beginning: Report (cointelegraph.com).

We believe these resources, as well as other investigative resources that exist within the federal government, are sufficient to bring enforcement actions against offences involving fraud and market abuse in cryptoasset markets and that new regulatory frameworks or regulatory agencies are not likely necessary. However, we acknowledge that additional funding and staffing may be necessary to examine and address fraudulent and abusive practices, especially if the crypto sector continues to grow.

- **Recommendation 9 –** *Regulators should have market surveillance requirements applying to each CASP, so that market abuse risks are effectively mitigated.*

Market surveillance is critical to the function of a market regulator. With respect to crypto markets, regulators should make use of both traditional surveillance methods like reporting by regulated market participants but also surveillance of "on-chain" transactions reported on public ledgers. Purely "on-chain" surveillance may not capture all market activity because some "off-chain" transactions may not be captured. For example, if an individual directly transfers their crypto hardware wallet, that transaction would not be public. Functionally, this is similar to the now uncommon bearer bonds or bearer shares, whose existence made markets somewhat less transparent, but that were not incompatible with regulated securities markets.

- **Recommendation 10 –** *Regulators should require a CASP to put in place systems, policies, and procedures around the management of material non-public information, including, where relevant, information related to whether a crypto-asset will be admitted or listed for trading on its platform and information related to client orders, trade execution, and personally identifying information.*

We agree that crypto companies that handle personally identifying information, and other important financial information about their customers, should be supervised to ensure they take adequate steps to protect that information from theft or misappropriation and that regulators have a role in ensuring such steps are taken.

In the United States, financial institutions, brokers, dealers, and people providing insurance services, including investment companies and investment advisors, must comply with the Privacy and Safeguards Rules of the Gramm-Leach Bliley Act ("GLBA"). The Privacy Rule requires financial institutions to provide particular notices and to comply with certain limitations on disclosure of nonpublic personal information. The Safeguards rule requires these institutions to "implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards

that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[5]

Financial institutions are defined broadly, including but not limited to any institutions that engage in activities that are financial in nature such as "Lending, exchanging, transferring, investing for others, or safeguarding money or securities."[6] In our view, most if not all, crypto companies meet this definition of financial institution.

We believe that adherence to the Privacy and Safeguards Rules – to which crypto companies should already be subject as financial institutions – should be sufficient to protect client personally identifying information. Depending on the characteristics of their business, most crypto companies should be supervised for compliance to GLBA either by the SEC or Federal Trade Commission (FTC).

- **Recommendation 11 –** *Regulators, in recognition of the cross-border nature of crypto-asset issuance, trading, and other activities, should have the ability to share information and cooperate with regulators and relevant authorities in other jurisdictions with respect to such activities. This includes having available cooperation arrangements and/or other mechanisms to engage with regulators and relevant authorities in other jurisdictions. These should accommodate the authorization and on-going supervision of regulated CASPs, and enable broad assistance in enforcement investigations and related proceedings.*

From their creation, cryptocurrencies have been a favored tool of money launderers and those who engage in cross-border crime. The lack of intermediaries and pseudonymous nature of cryptocurrencies have made them the go to asset for money laundering and cross-border blackmail. Furthermore, crypto companies have often participated in regulatory arbitrage, attempting to domicile themselves in jurisdictions with relatively fewer investor protections or disclosure requirements.

Enhancing international information sharing and cross-jurisdictional cooperation in enforcement is absolutely critical to address cryptoassets' unique cross-border risks. This should include an agreed upon set of approaches for involving a nation's securities' regulator when its laws are implicated or consumers in its jurisdiction are impacted, notwithstanding that crypto companies being domiciled in a foreign jurisdiction (or not being domiciled in any discernible jurisdiction).

---

[5] 16 C.F.R. Part 314.
[6] 12 U.S.C. 1843(k)(4)(A).

Additionally, through its development of the Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU), IOSCO has established itself as a key facilitator of international cooperation. We encourage IOSCO to continue its efforts to increase the number of signatories and consider new ways to use the MMoU to support cross-border investigations and enforcement actions, particularly with respect to cryptoassets.

- **Recommendation 13 –** *Regulators should require a CASP to place Client Assets in trust, or to otherwise segregate them from the CASP's proprietary assets.*

We agree that certain regulated investment advisors who hold cryptoassets on behalf of clients should be required to hold those assets in trust – segregated from their own proprietary assets and in the custody of a qualified custodian. For more information about our position regarding this issue, please see our comment letter in response to revisions to the SEC's Safeguarding Rule where we recommend expanding the scope of the rule from "funds or securities" to all assets, including cryptoassets.[7] We also note that technical challenges and legal uncertainties related to custody of crypto may make it difficult to find a willing and able custodian.

- **Recommendation 14 –** *Regulators should require a CASP to disclose, as relevant, in clear, concise and non-technical language to clients:*
    - *i. How Client Assets are held, and the arrangements for safeguarding these assets and/or their private keys;*
    - *ii. The use (if any) of an independent custodian, sub-custodian or related party custodian;*
    - *iii. 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;*
    - *iv. Risks arising from the CASP's handling or moving of Client Assets, whether directly or indirectly, such as through a cross-chain bridge; and*
    - *v. Full and accurate information on the obligations and responsibilities of a CASP with respect to the use of Client Assets, as well as private keys, including the terms for their restitution, and on the risks involved.*

We believe the recommended disclosure requirements a crypto company acting as a custodian are appropriate.

[7] Independent Community Bankers of America. "Comment Letter RE: Safeguarding Advisory Client Assets Proposed Rule [Release No. IA-6240; File No. S7-04-23; RIN 3235-AM32]". (May 8, 2023), (available at https://www.icba.org/docs/default-source/icba/advocacy-documents/letters-to-regulators/comments-on-sec-safeguarding-rule.pdf?sfvrsn=2daed17_0).

- **Recommendation 15 –** *Regulators should require a CASP to have systems, policies, and procedures to conduct regular and frequent reconciliations of Client Assets subject to appropriate independent assurance.*

This recommendation is appropriate, and we strongly support the recommended requirement of independent audits of any crypto company with custody of client assets.

- **Recommendation 16 –** *Regulators should require a CASP to adopt appropriate systems, policies, and procedures to mitigate the risk of loss, theft, or inaccessibility of Client Assets.*

In principle, we agree with this recommendation. However, it is not immediately clear what systems and policies are appropriate to prevent loss and theft. At a minimum, a crypto company that acts as a custodian of client assets should "physically" safeguard those assets through proper maintenance of cryptographic keys. It may also be appropriate to require such custodians to purchase insurance for crypto assets in their custody or to maintain cash balances with a separate custodian to be paid to the custodians' client in the event the asset is lost by the custodian.

- **Recommendation 17 –** *Regulators should require a CASP to comply with requirements pertaining to operational and technology risk and resilience in accordance with IOSCO's Recommendations and Standards. Regulators should require a CASP to disclose in a clear, concise and non-technical manner, all material sources of operational and technological risks and have appropriate risk management frameworks (e.g., people, processes, systems, and controls) in place to manage and mitigate such risks.*

This recommendation is appropriate and commensurate to the financial and cybersecurity risks posed by crypto companies.

Comment Regarding Chapter 10: Box on Stablecoins:

We agree that IOSCO is correct in pointing out the risk of stablecoins including that they may be backed by insufficient reserve assets or that they may be used to facilitate money lauding or fraud. To this end, it is important for the stablecoin ecosystem to be properly supervised, and it is perhaps appropriate to limit the issuance of stablecoins that track the value of a currency 1-to-1 to regulated banks. In general, we agree with the applicability of the report's recommendations to stablecoins.

As we have commented previously, ICBA and its members have a strong interest in ensuring that stablecoins do not create systemic, investor, or consumer risk and that risks created by unregulated or loosely regulated nonbank firms operating in this sector do not spill over into the traditional banking system. One of the defining characteristics of a global stablecoin ("GSC") is its potential reach and adoption across multiple jurisdictions. This reach—without a strong, internationally-consistent floor—introduces the potential for regulatory evasion or arbitrage, potentially allowing a stablecoin to gain substantial market influence without the regulatory or supervisory oversight or prudential requirements commensurate with the risks posed.

Consistent with the principle of "same activity, same risk, same regulation," we strongly support international and domestic efforts to bring all stablecoins—not only GSCs—within the existing regulatory perimeter. Any regulatory or supervisory regime applicable to stablecoins should be comparable to a functionally similar product offered by a bank or other traditional financial services provider.

However, bringing stablecoins within the regulatory perimeter is a necessary, but not sufficient, step. As the 2022, collapse of the TerraUSD stablecoin demonstrated stablecoins' unique characteristics can introduce new and difficult to assess risks, such as the potential for weaknesses in stabilization mechanisms to ensure a strong peg to the stablecoin's reference asset to cause rapid destabilization. We support the FSB's revised recommendation that authorities require a GSC to maintain an effective stabilization mechanism, clear redemption rights and to meet prudential requirements. Indeed, ICBA and its members encourage authorities to apply these requirements to all stablecoins, not only GSCs, and to limit issuance activities to banks or other supervised financial institutions subject to capital adequacy, reserve and other prudential requirements.

Conclusion

ICBA appreciates the opportunity to provide comments in response to IOSCO's Consultation Report of Policy Recommendations for Crypto and Digital Asset Markets. America's community banks have a strong interest in ensuring the protection of their customers, and that includes an interest in insuring that the market for cryptoassets is transparent and well-regulated. As this report observes, "investors have substituted other financial instrument investment activities with crypto asset trading activities" and have treated cryptoassets as the functional equivalent of securities. We believe that most cryptoassets are – in fact – already securities under U.S. law. In light of these realities, we believe it is not only appropriate but necessary for securities regulators to provide the same investor protections regarding disclosure, transparency, and protection from conflict of interest in crypto markets to which investors have become accustomed.

Implementing these protections will not only serve the important purpose of investor protection but will promote the stability of the overall financial system and pave the way for regulated institutions to participate in crypto markets.

Please feel free to contact us at Brian.Laverdure@icba.org and Mickey.Marshall@icba.org if you have any questions about the positions stated in this letter.

Sincerely,

/s/
Brian Laverdure, AAP
Vice President, Payments and Technology Policy

/s/
Mickey Marshall
Assistant Vice President and Regulatory Counsel

WASHINGTON, DC
1615 L Street NW
Suite 900
Washington, DC 20036

SAUK CENTRE, MN
518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

866-843-4222
www.icba.org