July 31, 2023

Mr. Martin Moloney
Secretary General
International Organization of Securities Commissions
C/ Oquendo 12,
28006 Madrid
SPAIN

By email: cryptoassetsconsultation@iosco.org

Dear Sir,

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

The Institute of International Finance (**IIF**) welcomes the opportunity to respond to the International Organization of Securities Commissions' (**IOSCO's**) consultation report containing proposed Policy Recommendations (**Recommendations**) for crypto-assets and digital asset markets, released in May 2023.

We commend IOSCO for tackling these important issues in a timely and consultative way. We welcome IOSCO's thoughtful approach to ensuring a fit-for-purpose regulatory regime that can be expected to strengthen consumer protection, market integrity, and financial stability in crypto-asset markets and among crypto-asset service providers (**CASPs**).

We also welcome IOSCO's close engagement with other international standard-setters engaged in efforts around these topics including the Financial Stability Board (**FSB**) and Committee on Payments and Market Infrastructures (**CPMI**).

In line with our December 15, 2022 submission to the FSB's consultation on crypto-assets and stablecoins, and our earlier submission to the Basel Committee on Banking Supervision (**BCBS**) on the prudential treatment of crypto-asset exposures, we advocate for a measured approach that does not unduly restrict the ability of regulated financial institutions to prudently engage in crypto-asset activities, such that associated risks will be subject to robust, sound risk management practices. This principle was also front and center in our April 30, 2023 submission to HM Treasury and the Bank of England on these topics.

We continue to strongly advocate for **technology neutrality** as a guiding principle for regulation in this space, and agree with the principle of **"same risk, same regulatory outcome"**. Crypto-asset regulation should not bring asset classes that are outside of the scope of financial market regulation into the scope of that regulation merely because of the use of DLT. Similarly, the assessment of operational risk should not include a blanket penalty for use of a particular technology.

We would make additional observations on **articulation and scope** of IOSCO's Recommendations:

1. The **scope of the term "crypto-asset"** as defined in the consultation report is very broad and could cover so-called "utility tokens", cryptographic virtual in-game goods, and loyalty schemes, for example. However, there are many areas in the Recommendations where a narrower scope of application would be appropriate. Many of the Recommendations indeed seem to be relevant only to crypto-assets that economically function similarly to or as a substitute for securities, derivatives, or regulated commodities (such as crypto-assets within Groups 1 and 2 of the Basel Committee prudential standards for bank exposures to crypto-assets). We would also note that tokenized securities, derivatives, and regulated commodities are already covered by securities and derivatives laws and while they do not require an additional layer of regulation, existing regulations

may need to be adapted to take into account potential legal differences in the way tokenized assets may be transferred, exchanged, and traded. We recommend this be made clear in the scope section of the paper.

2. In addition, IOSCO should clarify that for the purpose of its Recommendations, the term "crypto-asset" is not intended to apply to **books and records** systems using DLT or blockchain infrastructure, including internal treasury or other such systems, including those covering affiliates within a financial institution group. Such systems are already under the supervisory oversight of the appropriate regulators for regulated financial institutions. Accordingly, the definition of crypto-assets should exclude tokens that are used solely for the internal bookkeeping records of a financial institution.

3. Bank deposits are one place where extensive regulatory frameworks already exist. **Tokenized bank deposits** are different from stablecoins and crypto-assets, depending on how they are structured, and need to be distinguished as such. We accordingly seek clarification that they would not be within the scope of crypto-assets covered by the Recommendations (at least to the extent they are not freely transferred and traded on a public blockchain). The use of new technology such as distributed ledger technology (**DLT**) to deliver an existing product that is already subject to regulation, which may include deposit tokens, should not change the legal nature of that product or the rules that apply to it.

4. On **cross-border**, in our view, there should be a positive statement that jurisdictions should consider permitting incoming services from other jurisdictions in relation to which determinations have been made that a sufficiently comparable regulatory regime with regard to the risks addressed by the Recommendations has been implemented and that suitable cooperation arrangements with local regulators have been established, in compliance with the IOSCO multilateral memoranda of understanding (**MMOUs**) for supervision and enforcement.

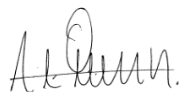
5. On crypto-assets **custody**, we believe it is important to clarify the expectations around stablecoins' underlying reserve assets, and that segregation of client assets from the assets of CASPs and stablecoin issuers is not an end in itself, and must actually achieve remoteness of client assets from the bankruptcy of the CASP or issuer. Safekeeping operations must also be functionally separated from trading and other market activities. It is also important to consider a proportionate approach to crypto-assets liability, given that many risks will be outside the control of the custodian. We note that in some markets, detailed requirements will shortly be in place. These include, for example, requirements to appoint an appropriately regulated custodian to hold and control reserve assets, to provide for client asset segregation, and around the disclosure of risks.

Lastly, we would urge the importance of an approach to regulation that recognizes the **dynamic nature** of this asset class and supports a framework designed to evolve in line with its evolution. Recommendations for crypto-asset markets should not be more prescriptive or restrictive, proportionate to the risks they present, than regulation of traditional financial asset markets.

In the **Annex** we provide detailed answers to selected consultation questions, and additional comments on the wording of the Recommendations or other observations in the consultation report.

The IIF and its members stand ready to engage in additional discussions and consultations on these topics, or to clarify any aspect of our submission.

Yours sincerely,



Jessica Renier
Managing Director, Digital Finance

Andres Portilla
Managing Director, Regulatory Affairs

Annex 1 – IIF responses to individual recommendations / consultation questions

p.	Recommendation or question	IIF response or comment
3	**Introduction**	
3	The proposed recommendations are principles-based and outcomes-focused and are aimed at the activities performed by crypto-asset service providers (CASPs).[1]	We note that crypto-asset issuers would not normally qualify as CASPs within the definition set out in footnote 4 of the consultation report. We would encourage IOSCO to clarify whether the term is intended to refer to issuers in some contexts (for instance, as opposed to exchanges). The Recommendations should therefore ensure that issuers of crypto-assets are subject to proportionate rules that are tailored to the characteristics of the issuer and nature of the issuance. It is likewise important for the Recommendations to differentiate carefully between the activities of a CASP and those of an issuer of crypto-assets, and to properly delineate the handoff of responsibilities between them.
3	The term "crypto asset," also sometimes called a "digital asset," refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "virtual currencies," "coins," and "tokens." To the extent digital assets rely on cryptographic protocols, these types of assets are commonly referred to as "crypto assets."	The scope of the term "crypto-asset" as defined at p. 3 of the consultation report is quite broad and appears to cover so-called "utility tokens", cryptographic virtual in-game goods, and loyalty schemes, for example. There are areas in the Recommendations, however, where a narrower scope of application than inclusion of this full range of possibilities would be appropriate. Many of the Recommendations indeed seem to be relevant only to crypto-assets that economically function similarly to or as a substitute for securities, derivatives, or regulated commodities (such as crypto-assets within Groups 1 and 2 of the Basel Committee prudential standards for bank exposures to crypto-assets). We would also note that tokenized securities, derivatives, and regulated commodities are already covered by securities and derivatives laws and while they do not require an additional layer of regulation, existing regulations may need to be adapted to take into account potential legal differences in the way

[1] [footnote 4 in consultation report.] 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.

p.	Recommendation or question	IIF response or comment
		tokenized assets may be transferred, exchanged, and traded. We recommend this be made clear in the scope section of the paper. Further, the adoption of a distributed ledger or blockchain-based books and records system by a financial institution to record its deposit and custody balances should not change a traditional security, cash, or other asset into a "crypto-asset" or a "digital asset." The design philosophy of an internal record-keeping system should not reclassify an asset when the legal status and the risks associated with the asset do not change. We also consider it potentially unclear whether decentralized "issuer-less" crypto-assets such as Bitcoin and Ether, which may be issued automatically by the operation of decentralized protocols on permissionless blockchains, are within scope of the Recommendations, having regard to the carve-out of decentralized finance or "DeFi" on page 1 of the consultation report.[2] We urge IOSCO to clarify that such crypto-assets are within scope of the final Recommendations. More broadly, we would urge IOSCO to provide further clarity on the term DeFi and what type of crypto-assets / crypto-asset activities will be excluded under this term.
13	**Chapter 1** – Overarching Recommendation Addressed to All Regulators	
13	Each jurisdiction should implement the Recommendations, **as they deem appropriate**, within their existing or developing frameworks considering each Regulator's role within those existing or developing frameworks, and the outcomes achieved through the operation of the frameworks in each jurisdiction.17	We consider that this expression "as they deem appropriate" may leave an undesirable level of optionality. We would suggest "in the manner they deem appropriate" would make it clearer that jurisdictions are urged to implement the Recommendations, but the manner of implementation is a matter of discretion. We would also urge implementation of all Recommendations in a timely manner. The technology is here to stay, and the pace of development has not slackened. Greater clarity in this space is

p.	Recommendation or question	IIF response or comment
		important; it is key to have clear guardrails in place, which IOSCO's Recommendations could either put in place or strengthen.
14	**Recommendation 1** – (Common Standards of Regulatory Outcomes) 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 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.	
15	**Question 1**: – Are there other activities and/or services in the crypto-asset markets which **Recommendation 1** should cover? If so, please explain.	Please refer to our comments on the scope of the Recommendations in response to p. 3 of the consultation paper.[3] The proposals are somewhat vague as to the outer limits of activities that should be regulated, specifying that "The IOSCO Standards apply generally to all crypto-assets, their issuers and the provision of services in relation to primary issuance, secondary trading and ancillary services and activities linked thereto." As such, the danger is that the Recommendations may extend too far, rather than of not extending far enough.
15	**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?	Yes. We continue to strongly advocate for technology neutrality as a guiding principle for regulation in this space, and agree with the principle of "same risk, same regulatory outcome".[4] At the same time, it is important for CASPs who will be providing services for traditional assets and for crypto-assets that the rules be,

[3] See p. 4 of this document.
[4] See also our response to the U.K. authorities dated April 30, 2023.

p.	Recommendation or question	IIF response or comment
		to the greatest extent possible, the same while prioritizing the same outcome. When a service is provided that is similar or the same as existing financial services being provided today, in order to provide such services, CASPs should obtain appropriate licensing that is similar in its objectives and outcomes to existing regimes that are currently applied to those services today, prior to the CASP providing those services.
16	**Chapter 2**: Recommendations on Governance and Disclosure of Conflicts	
16	**Recommendation 2** – (Organizational Governance) Regulators should require a [Crypto-Asset Service Provider or] **CASP** to have effective governance and organisational 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.	We would urge greater clarity in the Recommendation as to the circumstances in which "more robust measures", particularly involving legal disaggregation, would be justified. This is clearly a matter of great concern with regard to the collapses of a number of crypto-assets companies and exchanges in 2022-23, and a simple, clear statement of intent from IOSCO could help to forestall a lengthy period of regulatory migration and ongoing regulatory arbitrage among jurisdictions seeking to attract globally active CASPs and crypto-asset groups.
17	**Recommendation 3** – (Disclosure of Role, Capacity and Trading conflicts) 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	"And into which it provides services": see our response to Question 13 below in relation to the cross-border provision of services by CASPs.

p.	Recommendation or question	IIF response or comment
	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).	
18	**Question 3**: – Does **Chapter 2** adequately identify the potential conflicts of interest that may arise through a CASP's activities? What are other potential conflicts of interest which should be covered?	Chapter 2 generally adequately identifies conflicts that may arise depending on the varied activities of CASPs. Two activities not specifically called out that may give rise to conflicts are issuance of unbacked crypto-assets by a CASP that also trades in those crypto-assets; and involvement of venture capital affiliates in on-market or other trading activities. We have not identified other potential conflicts of interest that should be covered. We note that typically it would be for the firm itself, in or under its conflicts policy, to proactively monitor and identify particular conflicts.
18	**Question 4**: – Do respondents agree that conflicts of interest should be addressed, whether through mitigation, separation of activities in separate entities, or prohibition of conflicts? If not, please explain. Are there other ways to address conflicts of interest of CASPs that are not identified?	Yes. Generally speaking, we see a case for management of conflicts of interest, rather than outright prohibition. As an overall comment, we would not see justification for more onerous rules applying to crypto-asset exchanges than apply to securities, commodities, or derivatives exchanges. Typical measures for the mitigation of conflicts include information barriers, separation of reporting lines, and separation of legal entities within the same corporate group. Identification of all relevant conflicts, both between clients and between the client and the CASP or its affiliates, is another important aspect.
18	**Question 5**: – Does **Recommendation 3** sufficiently address the manner in which conflicts should be disclosed? If not, please explain.	Yes. It would be helpful if the Recommendation were accompanied by some guidance on how disclosures could be tailored to the respective client cohort, e.g. retail vs. institutional clients, to ensure they are fit for purpose. We note the Recommendation would require that relevant disclosures should be updated "at any point thereafter when such position changes." We would suggest there should be a materiality threshold built in such that minor changes in role are not required to be disclosed. There may also be a call for a carve-out where the change of role arises from a corporate reorganization and does not represent an economically substantive change.

p.	Recommendation or question	IIF response or comment
19	**Chapter 3** – Recommendations on Order Handling and Trade Disclosures (Trading Intermediaries vs Market Operators)	
19	**Recommendation 4** – (Client Order Handling) 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, non-technical 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).	
19	Clients also may not understand that the CASP may be front-running client trades.	Front-running of client trades is undesirable and should be permitted only in limited circumstances for pre-hedging and only when acting as principal (in line with the Global FX Code).[5]
20	[R]egulators may consider requiring the CASP to perform the following in accordance with the regulators' authority: … Take reasonable steps to deliver best execution for clients;	Whether best execution is owed to clients is a fundamental aspect of securities regulation. In most jurisdictions, best execution is owed to retail clients for whom an intermediary deals as agent. In some jurisdictions, it may also be owed to wholesale clients and/or when acting as principal in certain circumstances. Where a CASP deals as agent for a client, prima facie, best execution should be owed. At the very least, the circumstances where the client should not expect best execution must be made clear to the client by appropriate, and clear, disclosures.
20	**Recommendation 5** – (Market Operation Requirements) 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	

[5] See Recommendation 11: "A Market Participant should only Pre-Hedge Client orders when acting as a Principal, and should do so fairly and with transparency."

p.	Recommendation or question	IIF response or comment
	consistent with, those that are required in traditional financial markets.	
20	Many CASPs are currently operating in non-compliance or in a manner inconsistent with existing regulations that apply to exchanges. This impedes critical trade transparency for transactions occurring on a CASP trading platform. This lack of information gives rise to a non- transparent market, not only with respect to pricing but also trading activities.	We fully support the objective of pre- and post-trade transparency; that said, we would point out that existing trading platforms do often provide significant transparency, and also that the regulations should be adapted to the limitations of public networks, where relevant. By comparison with securities markets, many crypto-assets exchanges can be seen to deliver a high degree of real-time trading information, and may publish large or block trades sooner than their securities counterparts. Pre-trade transparency may also be good for users of crypto-asset exchanges, depending on the platform. On this score the IOSCO report is in danger of overstating the lack of trade transparency in crypto-assets markets. On the other hand, crypto-asset exchanges may lack formalized procedures for publication of updates about traded crypto-assets, and most will not have procedures for disclosure of substantial holdings. To some extent, these limitations arise from the nature of crypto-assets themselves, the holdings of which are typically pseudonymous at the level of the blockchain.
21	**Question 6**: – What effect would Recommendations 4 and 5 have on CASPs operating as trading intermediaries? Are there other alternatives that would address the issue of assuring that market participants and clients are treated fairly?	It is particularly important that **Recommendation 5** be limited in scope to crypto-assets that perform an economically similar function to securities, regulated commodities, or derivatives. It should be clarified that the term "acts as an intermediary" in **Recommendation 5** refers to dealing as agent for a client, or otherwise where obligations of best execution are owed, and not more broadly such as with regard to the provision of custody or ancillary services. As to the pre- and post-trade disclosures required by **Recommendation 5**, this would be in line with the principle of "same risk, same regulatory outcome". Having said that, regulators should enable CASPs to harness novel advances in technology that can

p.	Recommendation or question	IIF response or comment
		help provide disclosures automatically, including through blockchain analytics. See further our comments on pre- and post-trade transparency on p. 10 above. As to Recommendation 4, see our observations on front-running and best execution, on p. 9 above.
21	**Question 7**: – Do respondents believe that CASPs should be able to engage in both roles (i.e. as a market operator and trading intermediary) without limitation? If yes, please explain how the conflicts can be effectively mitigated.	Engaging in both roles (i.e. as market operator and trading intermediary) can give rise to significant conflicts of interests. The Recommendation on conflicts of interest already addresses such conflicts. As such, there is already a limitation on this dual role. It is noted that in many jurisdictions, an intermediary acting as agent owes obligations of a different kind to a client than one acting as principal. As such, conflicts among these different roles are of a different nature.
21	**Question 8**: – Given many crypto-asset transactions occur “off-chain” how would respondents propose that CASPs identify and disclose all pre- and post-trade “off-chain” transactions?	We do not believe that CASPs should be obliged to identify all pre- and post-trade “off-chain” transactions. The wholesale or “upstairs” market in securities markets is typically not as transparent as a central limit order book (CLOB), and in many jurisdictions is not transparent. Where there is a system of market makers operated by a crypto-asset exchange, trading by those market makers should as a first approximation be disclosed by the exchange in a similar manner as by a securities exchange. The term “pre-trade off-chain transaction” is not clear. Presumably this refers to pre-trade orders or indications of interest. Again, it is not considered appropriate to require the disclosure of such orders, at least if they are not being placed by market makers on a particular exchange.
22	**Chapter 4** – Recommendations in Relation to Listing of Crypto-Assets and Certain Primary Market Activities	

p.	Recommendation or question	IIF response or comment
24	**Question 9**: – Will the proposed listing/delisting recommendations in **Chapter 4** enable robust public disclosure about traded crypto-assets? Are there other mechanisms that respondents would suggest to assure sufficient public disclosure and avoid information asymmetry among market participants?	See below for our comments specifically on **Recommendations 6 and 7**. There are many crypto-asset market information services, aggregators and analytics tools which crypto-assets investors should be encouraged to understand and utilize, which may not be affiliated with particular exchanges. Exchanges and indeed regulators could be encouraged to take some responsibility for bringing these to the attention of investors, through the use of fact sheets, without necessarily being seen to endorse the contents of these services. Recommendation 6 In the crypto-asset space, there is usually no distinction between "listing" and admission to trading (ATT), given that the concept of "primary listing" (or home exchange) of most crypto-assets does not exist. However, there are exchanges that of course issue their own crypto-asset token, and to that extent there may be an analogy with the idea of listing. IOSCO is encouraged to explore these concepts further and whether the ATT concept can completely supplant the listing concept for crypto-assets that are not regulated as securities, commodities or derivatives. Recommendation 6 – guidance on disclosures As we say above, it is potentially unclear whether decentralized "issuer-less" crypto-assets such as Bitcoin and Ether, which may be issued automatically by the operation of decentralized protocols on permissionless blockchains, are within scope of the Recommendations, having regard to the carve out of decentralized finance or "DeFi" on page 1 of the consultation report. We urge IOSCO to clarify that such crypto-assets are within scope of the final Recommendations. If IOSCO provides further clarity on this by stating they are within scope, some of the proposed information mentioned on p. 23 of the

p.	Recommendation or question	IIF response or comment
		consultation report would not be relevant. For example, in the case of Bitcoin and Ether, and other similarly decentralized cryptocurrencies, it is not apparent which entity is the "issuer" concerned, in respect of which the CASP should disclose "full information about the issuer and its business, including audited financial statements". It is also noted that, for many issuers of crypto-assets, if they are not public companies at present, providing audited financial statements publicly may be a significant change in their mode of operation. Recommendation 7 While we are supportive in principle, we would urge that the appropriate groundwork be laid in terms of accounting and auditing standards governing crypto-assets. Accounting for crypto-assets is also an issue that should be considered at the national and international levels. Where crypto- assets providers have assets in one denomination (such as ETH) and liabilities in another (such as USD), there should be an expectation that the assets denominated in non-fiat should be marked to market daily, to avoid liability mismatches. The failure to mark crypto-assets to market has indeed been alleged as a factor in the collapse of Celsius, and accounting and governance failures were also prominent in the collapse of FTX. In relation to accounting, we are of the view that more clarity on the international accounting standards applicable to the activity of safeguarding of crypto-assets is desirable and should be referred to the International Accounting Standards Board (IASB) as an urgent issue. Further, as we state above, regulators should enable CASPs to harness novel advances in technology which can help provide disclosures automatically, including through blockchain analytics. While we are supportive of the Recommendation, we note also that Recommendation 2 requires a CASP 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

p.	Recommendation or question	IIF response or comment
		affiliated entities. These conflicts should be effectively identified, managed and mitigated." We understand that CASPs engaged in issuance, trading and listing of crypto-assets would also be covered by Recommendation 2. If that is not the intent, it should be clarified. We note that Recommendation 7 differs in some ways from the wording of Recommendation 2. For instance, it requires conflicts of interest to be managed and mitigated but not identified. It also does not refer to "governance and organisational requirements." If there are policy reasons for the Recommendations to be different, then they should be articulated.
24	**Question 10**: – Do respondents agree that there should be limitations, including prohibitions on CASPs listing and / or trading any crypto-assets in which they or their affiliates have a material interest? If not, please explain.	The proposed prohibition on a CASP listing and/or facilitating trading in its own proprietary crypto-assets, or any crypto-assets in which it may have a material interest, may not be justified. Many crypto-asset exchanges today have proprietary tokens. IOSCO is encouraged to make it clear that a CASP may self-list its own token, just as many securities exchanges globally do self-list, subject of course to appropriate governance and conflicts management procedures being in place, in line with the Recommendations. This should recognize risks associated with the use of the token as collateral, lending with the token, and market manipulation with regard to the price or trading volume of that asset. Separately, we would observe that the consultation report indicates that a primary concern is that CASPs may have a strong incentive to influence the price discovery process, and that this requirement would seem less applicable to stablecoins.
25	**Chapter 5** – Recommendations to Address Abusive Behaviors	
27	**Recommendation 10** (Management of Material Non-Public Information) 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	

p.	Recommendation or question	IIF response or comment
	platform and information related to client orders, trade execution, and personally identifying information.	
28	**Question 11**: – In addition to the types of offences identified in **Chapter 5**, are there: a) Other types of criminal or civil offences that should be specifically identified that are unique to crypto-asset markets, prevention of which would further limit market abuse behaviors and enhance integrity? b) Any novel offences, or behaviors, specific to crypto-assets that are not present in traditional financial markets? If so, please explain.	While there is already quite a long list of behaviors – such as rug-pulls and the like – that could be deployed in answer to this question, most of these can be analyzed in terms of more traditional offences, including fraud and market manipulation. Given also the speed at which crypto-assets markets have evolved, it is not desirable to "bake in" detailed descriptions of abusive behavior into the law which may quickly go out of date. It could be effective for regulators to disseminate typologies of new behaviors which may be abusive – similar to how money laundering regulators disseminate information about money laundering typologies.[6] Some of the more challenging edge cases relate to DeFi protocols where there may be no legal entity actually operating the protocol involved, other than in some cases a collective of individuals associated with a Decentralized Autonomous Organization (if one exists). It is assumed that IOSCO's DeFi workstream will tackle this issue in its forthcoming paper.
28	**Question 12**: – Do the market surveillance requirements adequately address the identified market abuse risks? What additional measures may be needed to supplement **Recommendation 9** to address any risks specific to crypto-asset market activities? Please consider both on- and off-chain transactions.	We agree that market surveillance for crypto-asset markets should provide a similar level of protection as applies in traditional financial markets. We do not believe additional measures are required. Indeed, with regard to **Recommendation 9**, with regard to off-chain transactions, as these are not published anywhere, the scope of the obligation should be limited to transactions to which the CASP is a party, as principal or as agent, or is aware of in the ordinary course of providing its services (such as because it operates an exchange). We also believe that the scope of **Recommendation 9** should be limited only to certain CASPs. Broadly speaking, those CASPs that

[6] For example, see Council of Europe (2023), Money Laundering and Terrorist Financing Risks in the World of Virtual Assets: Typologies Report; FinCEN (2021), FinCEN Ransomware Advisory; AUSTRAC (2023), Typologies paper: AUSTRAC money laundering and terrorism financing indicators.

p.	Recommendation or question	IIF response or comment
		operate exchange-like entities should be subject to market surveillance requirements. CASPs such as crypto-asset custodians or other intermediaries need not have such requirements imposed on them. It is worth noting that the more that crypto-assets are brought into the regulated ecosystem, the safer crypto-assets can be expected to become, reducing the risks of money laundering, terrorist financing, and sanctions evasion. Conversely, if regulated financial institutions are prohibited or disincentivized from custodying or transacting crypto-assets on behalf of their clients, crypto-assets will be pushed into unregulated liquidity pools, increasing the potential for money laundering, terrorist financing, and sanctions evasion.
29	**Chapter 6 – Recommendation on Cross-Border Cooperation**	
29	**Recommendation 11** – (Enhanced Regulatory Cooperation) 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 authorisation and on-going supervision of regulated CASPs, and enable broad assistance in enforcement investigations and related proceedings.	
30	**Question 13**: – Which measures, or combination of measures, would be the most effective in supporting cross-border cooperation amongst authorities? What other measures should be considered that can strengthen cross-border co-operation?	We endorse global coordination to avoid fractured frameworks and regulatory arbitrage. IOSCO should take the opportunity to clarify the basis on which CASPs are entitled to provide services from outside a jurisdiction. Crypto-asset markets are global in nature, enabled by technology that has allowed global participation from inception. Maintaining investor access to global liquidity is important, while recognizing that supervision takes place at the jurisdictional level. While providing

p.	Recommendation or question	IIF response or comment
		adequate consumer protection, authorities should bear in mind the risk of effectively requiring local customers to use less liquid local venues. This regulatory arbitrage would not achieve IOSCO's desired ends. To the extent possible, uniform standards would help to avoid a fractured global framework and unnecessary barriers. That said, jurisdictions should consider permitting incoming services from other jurisdictions in relation to which determinations have been made that a sufficiently comparable regulatory regime with regard to the risks addressed by the Recommendations has been implemented and that suitable cooperation arrangements with local regulators have been established, in compliance with the IOSCO MMOUs for supervision and enforcement. Those MMOUs should be reviewed to ensure they remain fit for purpose for dealing with issues relating to crypto-assets and CASPSs. There may be a case for reviewing domestic arrangements to ensure that information sharing gateways are also aligned with the MMOUs. The principle that jurisdictions and regulators should be able to defer to each other when it is justified by the quality of their respective regulatory and enforcement regimes, based on similar outcomes, in a non-discriminatory way, paying due respect to home country regulation regimes, should be fully respected and reflected in the Recommendations.[7]
31	**Chapter 7 – Recommendations on Custody of Client Monies and Assets**	
31	**Recommendation 12** – (Overarching Custody Recommendation) Regulators should apply the IOSCO Recommendations Regarding the Protection of Client Assets when considering the application of existing frameworks, or New Frameworks, covering CASPs that hold or safeguard Client Assets.	See response to **Question 14** below.

[7] C.f. G20 leaders' declaration, September 6, 2013, paragraph 71 (with regard to OTC derivatives regulation).

p.	Recommendation or question	IIF response or comment
32	**Recommendation 13** – (Segregation and Handling of Client Monies and Assets) Regulators should require a CASP to place Client Assets in trust, or to otherwise segregate them from the CASP's proprietary assets.	See response to **Question 14** below.
36	**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?	Recommendation 12 We support the application of the IOSCO Recommendations Regarding the Protection of Client Assets. These are intended to apply to intermediaries performing a range of custodial services for a client, including where holding client assets in a chain of custody through multiple jurisdictions or placing assets with an affiliate in the same group or with a third party, regulated outside the intermediary's home jurisdiction. However, we think it is essential that the special characteristics of the underlying assets in the case of crypto-assets are always carefully considered in how the IOSCO Recommendations Regarding the Protection of Client Assets are applied. At the same time, to allow for a level playing field with the regulation of traditional financial assets, the policy Recommendations for crypto-asset markets should not be more prescriptive or restrictive, proportionate to the risks presented, than existing regulation for traditional financial assets. In some places, the IOSCO requirements around custody look to be more prescriptive than is common in the traditional space. For example, the Recommendation to disclose details of the contractual agreements with a third-party custodian look to go beyond what is current market practice. IOSCO should justify such special treatment or disapply the requirement. Recommendation 13 The objective to be achieved – which is bankruptcy remoteness, in other words the continued availability of client assets to clients in the event of the bankruptcy of the CASP – should be clearly spelled out to guide the application and understanding of the segregation requirement.

p.	Recommendation or question	IIF response or comment
		Even if client assets are segregated, they may not necessarily be bankruptcy remote. We suggest "arrange for them to be held in a bankruptcy remote manner" instead of only "segregate". With regard to client cash, this should be held with a prudentially-regulated institution such as a bank; in such a case the bank should not be required to custody the cash separately. Non-cash client assets should be held by an appropriately regulated custodian.[8] We also agree that rules governing the ownership of customer digital assets following insolvency of an intermediary should be made as clear as possible. Safekeeping operations must also be functionally separated from trading and other market activities.
36	**Question 15**: – (a) Should the Recommendations in **Chapter 7** address the manner in which the customer crypto-assets should be held? (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? (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? (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.	**Sub-question (a) (manner of holding) and (c) (books and records):** Crypto-asset custody should be regulated on par with traditional custody. We therefore welcome IOSCO's proposed approach of using existing regulatory frameworks for traditional finance custodians as a basis for developing a crypto-asset custody framework. Final regulatory standards for crypto-asset custody should be based on the following principles: i) segregation of client assets from firm/principal assets; ii) adherence to regulatory requirements and best practices for client asset safety and recordkeeping; and iii) identification and mitigation of risk across the end-to-end lifecycle, with security central to design architecture and operations of technical infrastructure. **Sub-question (b) (new technologies):** we consider that the activities of staking and lending are different, and the regulatory treatment should distinguish them. We would also point out that in some forms of staking, title is transferred and the underlying staked crypto-assets form part of the bankruptcy estate of the custodian or

[8] The definition of client assets set out in footnote 26 of the consultation report refers to both money and crypto-assets held for, and on behalf of, a client, and Recommendation 13 says that CASPs (whether banks or not) must segregate client assets. Either all bank deposits must be taken out of the scope of the definition of client assets, or there must be a specific exclusion from the segregation requirement for bank deposits.

p.	Recommendation or question	IIF response or comment
		the service provider of the staking activity. This form of staking should also be treated differently from staking where title is not transferred and where the underlying staked crypto-assets are protected for the beneficial owner even in the bankruptcy of the custodian or the staking service provider. **Sub-question (d) (valuation):** accounting for crypto-assets is an issue that should be considered at the national and international levels. Where crypto-assets providers have assets in one denomination (such as ETH) and liabilities in another (such as USD), there should be an expectation that the assets denominated in non-fiat should be marked to market daily, to avoid liability mismatches. The failure to mark crypto-assets to market has indeed been alleged as a factor in the collapse of Celsius, and accounting and governance failures were also prominent in the collapse of FTX. In relation to accounting, we are of the view that more clarity on the international accounting standards applicable to the activity of safeguarding of cryptoassets is desirable and should be referred to the International Accounting Standards Board (IASB) as an urgent issue.
36	**Question 16**: – Should the Recommendations address particular safeguards that a CASP should put in place? If so, please provide examples.	**Custodial liability** A key issue that arose during the legislative consideration of the European Union's Markets in Crypto Asset Regulation (MiCA) was the need to clearly establish the extent of custodial liability for the loss of client assets. Making custodians liable for losses outside of their control (e.g. DLT hacks and malfunctions) would make crypto-asset custody unviable for regulated entities and prevent qualified custodians from entering the market. We would therefore support jurisdictions taking a proportionate approach that may not impose full, uncapped liability on the custodian in the event of a malfunction or hack that was not within the custodian's control. Other aspects of the MiCA regime, as just one potential point of reference as IOSCO considers Recommendations, that might be instructive are requirements that CASPs providing custody of crypto-assets on behalf of clients:

p.	Recommendation or question	IIF response or comment
		- enter an agreement with their clients to specify their duties and their responsibilities; - keep appropriate records of client positions and their value and report on those positions and value to clients periodically; - maintain a custody policy with internal rules and procedures to ensure the safekeeping or the control of such crypto-assets and their return to clients; - facilitate the exercise of the rights attached to the crypto-assets, where applicable. The rules that apply to CASPs acting as custodians should clearly differentiate between rules applicable to assets under custody and those applicable to assets that are not in custody (i.e. where the custodian is providing a reporting service on "not-in-bank" assets). **Prudential aspects** It is important that existing rules for non-crypto custody, which work well, are not disturbed or changed in the process. In relation to the future development of prudential rules, we believe policymakers should take an off-balance sheet approach to custody of crypto-assets. It is essential that any capital and liquidity requirements associated with crypto-asset custody do not make custody unfeasible at scale for banks and prevent qualified institutions such as custodians from providing institutional-grade solutions that addresses identified risks of this novel asset class.
37	**Chapter 8 – Recommendation to Address Operational and Technological Risks**	
37	**Recommendation 17** – (Management and disclosure of Operational and Technological Risks) 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.	

p.	Recommendation or question	IIF response or comment
	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.	
38	**Question 17**: – Are there additional or unique technology/cyber/operational risks related to crypto-assets and the use of DLT which CASPs should take into account? If so, please explain.	Some of the key additional or unique risks relate to the heightened risk of client asset theft or loss from hacks, exploits and similar cyber attacks. Inter-protocol "bridges" have been a particular source of loss, with the bridge hack share of total stolen funds running well over 50% in 2022.[9] Some protocols retain "admin keys" alongside governance tokens as a means for project controllers to exercise overall control over the protocol. These admin keys can be a source of cyber risk or insider fraud risk.[10]
38	**Question 18**: – Are there particular ways that CASPs should evaluate these risks and communicate these risks to retail investors? If so, please explain.	We believe that risks to be disclosed to retail investors should be identified at an appropriate level of granularity, having regard to the nature and maturity of the token and the sophistication of the target market. Risks around token performance in adverse scenarios, and risks pertinent to governance or regulation material to investors' decisions, should be identified and disclosed. In some cases, particular operational or cyber risks may be important, including around issues related to smart contracts, oracles, or bridges.
39	**Chapter 9** – Recommendation for Retail Distribution	
39	**Recommendation 18** – (Retail Client Appropriateness and Disclosure) Regulators should require a CASP, to operate in a manner consistent with IOSCO's Standards regarding interactions and dealings with retail clients. Regulators should require a CASP to implement adequate systems, policies and procedures, and disclosure in relation to onboarding new clients, and as part of its ongoing services to existing clients. This should include assessing the appropriateness	

[9] Chainalysis (2022), Cross-Chain Bridge Hacks Emerge as Top Security Risk, August 2.
[10] IIF (2022), Decentralized Finance: Use Cases, Challenges and Opportunities, p. 7.

p.	Recommendation or question	IIF response or comment
	and/or suitability of particular crypto-asset products and services offered to each retail client.	
40	**Question 19**: – What other point of sale / distribution safeguards should be adopted when services are offered to retail investors?	Regulators could consider imposing design and distribution obligations such as a requirement to provide target market determinations. In the traditional space, suitability is typically attached to the type of investment service as opposed to the specific type of asset included in the service. We would stress that suitability requirements should take the same approach for the crypto-asset space where it is based on the type of service (be it digitally native or traditional) built around the assets.
40	**Question 20**: – Should regulators take steps to restrict advertisements and endorsements promoting crypto-assets? If so, what limitations should be considered?	No comment.
41	**Chapter 10** – Box Text on Stablecoins	
46	**Question 21**: Are there additional features of stablecoins which should be considered under **Chapter 10**? If so, please explain.	It is worth noting that versions of the same stablecoin that may be traded on different blockchains may have differing risk profiles, for example if one blockchain has different characteristics, or if the issuers only arrange market-making or redemption arrangements on one or some chains and not others. Client documentation should clearly distinguish between the native token and various derived forms or "wrappers" in which economic exposure to a stablecoin may be available, including as to risk disclosures and economic performance in various scenarios. **Additional comments on the Additional Recommendations on stablecoins** If IOSCO is to issue recommendations on stablecoins, it is suggested they be firm recommendations. Suggesting that a regulator "consider requiring" is not a firm recommendation and may open up undesirable regulatory arbitrage. We would suggest that IOSCO provide greater clarity around the prohibitions on CASPs listing affiliated digital assets, and whether this

p.	Recommendation or question	IIF response or comment
		extends to stablecoins. Given that the consultation report indicates that a primary concern is that CASPs may have a strong incentive to influence the price discovery process, this requirement would seem less applicable to stablecoins. There seems to be some duplication with the recommendations of the Financial Stability Board concerning so-called "global stablecoins". We note that potential inconsistencies between the IOSCO Recommendations and those of the FSB would create challenges to regulation and conflicts for compliance, if both sets of recommendations are intended to apply to global stablecoins. For example, the proposed disclosure of "whether there is segregation of reserve assets from the stablecoin issuer's own assets" implies choice, while the FSB's high-level recommendations seem to require segregation, at least for reserve-backed global stablecoins and stablecoins that have the potential to become global.[11] If the FSB's recommendations are intended to apply to the exclusion of IOSCO's to global stablecoins, this should also be made clear. Further, bank deposits are one place where extensive regulatory frameworks already exist. Tokenized bank deposits are different from stablecoins and crypto-assets, depending on how they are structured, and need to be distinguished as such.[12] We accordingly seek clarification that they would not be within the scope of crypto-assets covered by the Recommendations (at least to the extent they are not freely transferred and traded on a public blockchain). The use of new technology such as DLT to deliver an existing product that is already subject to regulation, which may include deposit tokens, should not change the legal nature of that product or the rules that apply to it.

[11] See e.g. FSB (2023), "Regulations and oversight should require the adequate safeguarding of customer assets and private keys, as well as appropriate risk disclosures and adequate protection of the users' ownership rights, including through prudent segregation and record-keeping requirements that minimise the risk of loss, misuse of or delayed access to assets." (p. 5) and "authorities should require reserve-based stablecoins to ensure safe custody and proper record-keeping of reserve assets and that ownership rights of reserve assets are protected at all times, including through segregation requirements from other assets of the GSC, members of its group and the custodian's assets." (p. 10)

[12] Our view is that they are digital representations of commercial bank money.

p.	Recommendation or question	IIF response or comment
		Additional Recommendation of custody for reserve assets of stablecoins Noting that crypto-asset issuers would not normally qualify as CASPs on IOSCO's definition on p. 3 of the consultation report, but that the Additional Recommendation states that **Recommendations 12 – 16** should be read, as relevant, as referring to reserve assets backing stablecoins as well as client assets, there is a need to clarify whether and, if so, how **Recommendations 12 – 16 are** intended to apply to stablecoin issuers. This is because issuance of a crypto-asset is not included in the list of activities set out in footnote 4 of the consultation report which defines a CASP Assuming that the intention is that **Recommendations 12 – 16** are to apply to stablecoin issuers themselves, the proposed disclosure 2(a) "whether there is segregation of reserve assets from the stablecoin issuer's own assets, protecting the stablecoin holder in event of the issuer's insolvency or bankruptcy" seems to contradict **Recommendation 13** ("Regulators should require a CASP to place Client Assets in trust, or to otherwise segregate them from the CASP's proprietary assets"). As to the proposed disclosure 2(b), it is suggested that a CASP should not be providing services with regard to a stablecoin if it does not know who is holding the reserve assets and in what capacity. Also, it is not clear if the expression "if known" is intended to qualify only who holds the reserve assets or also how they are held.
51	**Additional issues**	
51	**Question 22: –** IOSCO also welcomes views from stakeholders on potential additional issues for consideration	Although financial crime and money laundering are noted as risks in the consultation report, they do not appear on the 6 key risks areas, nor in the Recommendations, which focus more on fraud perpetuated by a CASP rather than where a well-intentioned CASP's systems are abused for the purposes of money laundering. While we acknowledge this is mainly the domain of FATF, we would suggest a stronger articulation between these Recommendations and that issue.