Policy Recommendations for Crypto and Digital Asset Markets

Final Report

THE BOARD
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR11/2023	**16 NOVEMBER 2023**

Copies of publications are available from:
The International Organization of Securities Commissions website: www.iosco.org

Table of Contents

EXECUTIVE SUMMARY

The 18 IOSCO policy recommendations for the regulation of crypto and digital assets (Recommendations) included in this Final Report are designed to support greater consistency with respect to regulatory frameworks and oversight in IOSCO member jurisdictions, to address concerns related to market integrity and investor protection arising from crypto-asset activities. The Recommendations have been developed under the stewardship of the IOSCO Board's Fintech Task Force (FTF) in accordance with IOSCO's Crypto-Asset Roadmap published in June 2022.[1]

The Recommendations are principles-based and outcomes-focused and are aimed at the activities performed by crypto-asset service providers (CASPs).[2] They apply IOSCO's widely accepted global standards for securities markets regulation to address key issues and risks identified in crypto-asset markets. The Recommendations are activities-based and follow a 'lifecycle' approach in addressing the key risks identified in this report. They cover the range of activities in crypto-asset markets that involve CASPs from offering, admission to trading, ongoing trading, settlement, market surveillance and custody as well as marketing and distribution (covering advised and non-advised sales) to retail investors. IOSCO separately consulted on proposed policy recommendations for "decentralized finance" or "DeFi" on 7 September 2023, which will be finalized by the end of 2023.[3] At that time, IOSCO will also publish an umbrella note explaining in more detail the interoperability between the two sets of recommendations.

One of IOSCO's goals is to promote greater consistency with respect to how IOSCO members approach the regulation and oversight of crypto-asset activities, given the cross-border nature of the markets, the risks of regulatory arbitrage and the significant risk of harm to which retail investors continue to be exposed. IOSCO is also seeking to encourage optimal consistency in the way crypto-asset markets and securities markets are regulated within individual IOSCO jurisdictions, in accordance with the principle of "same activities, same risks, same regulation/regulatory outcomes".

---

1 The FTF was established in March 2022 to develop recommendations to the Board of IOSCO and thereafter to oversee the implementation of IOSCO's regulatory agenda for Fintech and crypto-assets. The FTF is prioritizing policy-focused work on crypto-asset markets and activities in its initial 12 to 24 months of operation, while continuing to monitor market developments associated with broader Fintech-related trends and innovation.

2 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 activities such as services relating to lending/staking of crypto-assets and the promotion, marketing and distribution of crypto-assets on behalf of others.

3 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf.

The Recommendations also cover the need for enhanced co-operation among regulators. They aim to provide a critical benchmark for IOSCO members to cooperate, coordinate and respond to cross-border challenges in enforcement and supervision, including regulatory arbitrage concerns, that arise from global crypto-asset activities conducted by CASPs that offer their services, often remotely, into multiple jurisdictions.

In line with IOSCO's established approach for financial market regulation, these Recommendations are addressed to relevant authorities. They look to support jurisdictions seeking to establish compliant markets for the trading of crypto-assets in the most effective way possible.

While the Recommendations are not directly addressed to markets participants, CASPs and all participants in crypto-asset markets are strongly encouraged to carefully consider the expectations and outcomes articulated through the Recommendations and the respective supporting guidance in the conduct of their activities including registered/licensed, and cross-border activities.

INTRODUCTION

IOSCO is issuing these 18 Recommendations to help IOSCO members apply IOSCO's Objectives and Principles for Securities Regulation and relevant supporting IOSCO standards, recommendations, and good practices (hereafter "IOSCO Standards"), as appropriate, to crypto-asset activities within their jurisdictions and, in particular, to respond to widespread concerns regarding market integrity and investor protection within the crypto-asset markets.

The 18 Recommendations cover six key areas, consistent with IOSCO Standards:

1. Conflicts of interest arising from vertical integration of activities and functions,
2. Market manipulation, insider trading and fraud,
3. Cross-border risks and regulatory co-operation,
4. Custody and client asset protection,
5. Operational and technological risk, and
6. Retail access, suitability, and distribution.

Acknowledging the definitional and interpretive jurisdictional differences that currently exist, IOSCO has developed the Recommendations by developing a functional, economic approach to mitigate against the risks, rather than attempting to develop a one-size fits all prescriptive taxonomy.

Accordingly, IOSCO has developed an outcomes-focused, principles-based approach across each key area noted above. This approach is informed by a mapping of IOSCO Standards to relevant elements of the infrastructure, and to the services provided by, and the activities of CASPs.

By doing this, IOSCO has been able to examine and assess how its existing policy framework maps to key identified risks in crypto-asset markets, which IOSCO and its members understand from their expertise as securities markets and conduct regulators.

OVERVIEW OF KEY CONTENTS OF THE REPORT

This Final Report, and the 18 Recommendations contained within, are structured thematically as follows:

- ***Introduction***

  This provides an overview of the key content and structure of the report, along with the broader international regulatory and market context for the development of the Recommendations.

- ***Chapter 1 – Overarching Recommendation Addressed to All Regulators***

  This Chapter lays down an overarching Recommendation and supporting guidance calling upon all IOSCO members, collectively, to apply or adopt these Recommendations in a consistent, outcomes-focused manner.

  As set out in Recommendation 1 (*'Overarching Recommendation Addressed to All Regulators'*), the regulatory frameworks (existing or new) should seek to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those required in traditional financial markets in order to facilitate a level-playing field between crypto-assets and traditional financial markets and help reduce the risk of regulatory arbitrage.

  Regulators are therefore encouraged to analyze the applicability and adequacy of their regulatory frameworks, and the extent to which (1) crypto-assets are, or behave like substitutes for, regulated financial instruments, and (2) investors have substituted other financial investment activities with crypto-asset investment activities. Accordingly, this report focusses on the economic substance of crypto-assets and their substitutability vis-à-vis traditional financial instruments (notwithstanding a crypto-asset's purported potential use case or purpose as stated in supporting marketing and/or distribution materials).

  In adopting this approach, these Recommendations are designed to apply to all types of crypto-assets, including stablecoins. Where further risks are presented by stablecoins, these are explored by way of the supplementary guidance on stablecoins included in box text under Recommendation 6 and the Custody and Client Assets Recommendations.[4]

  Through its preamble (*'Preamble: Intent of the Recommendations'*), Chapter 1 further clarifies the intent of the Recommendations. This operative provision, that ***informs all 18 Recommendations*** while underscoring the need to promote optimal regulatory consistency

[4] The targeted commentary on stablecoins builds on the findings of the March 2020 IOSCO Report on Global Stablecoin Initiatives.

across member jurisdictions, also acknowledges, and provides for, appropriate principles, and outcomes-based flexibility in their domestic implementation.[5]

- ***Chapter 2 – Recommendations on Governance and Disclosure of Conflicts***

  This Chapter includes the Recommendations and supporting guidance to address risks arising, in particular, from vertically integrated CASP business models. Many CASPs typically engage in multiple functions and activities under 'one roof' – including exchange trading, brokerage, market-making and other proprietary trading, offering margin trading, custody, settlement, and re-use of assets – whether through a single legal entity or an affiliated group of entities that are part of a wider group structure. Recommendation 2 (*'Organizational Governance'*) states that CASPs should have effective governance and organizational requirements in place to effectively address and mitigate issues on conflicts of interests arising from vertical integration, including the possible need for measures such as legal segregation of functions and activities, as well as separate registration. Where a CASP engages in different activities and functions in a crypto-asset trading environment, it is important for investors and regulators to understand the precise activities and functions that the CASP is providing, and the capacity in which it is acting, in relation to its clients. Accordingly, Recommendation 3 (*'Disclosure of Role, Capacity and Trading Conflicts'*) states that a CASP should accurately disclose each role and capacity in which it is acting at all times.

- ***Chapter 3 – Recommendations on Order Handling and Trade Disclosures (Trading Intermediaries vs Market Operators)***

  This Chapter includes Recommendations and supporting guidance in the areas of Order Handling and Trade Disclosures. Despite common market parlance of referring to CASPs as "exchanges", a CASP may actually be operating as a trading intermediary (a broker or dealer or both) instead of a market operator (or trading venue). Recommendation 4 (*Client Order Handling'*) addresses inherent conflicts of interests, where CASPs might front-run clients' orders in favor of their own or engage in related party transactions. CASPs are thus expected to

[5] The Recommendations recognize that some jurisdictions have existing regulatory frameworks that encompass crypto and digital assets, while other jurisdictions are in the process of developing regulatory frameworks. Each jurisdiction should implement the CDA Recommendations, as they deem appropriate, within their existing or developing frameworks.

implement systems, policies and procedures that provide for fair, orderly, timely execution that is in the best interest of clients. In the context of a CASP acting as a market operator (or trading venue), it is expected to have resilient systems to effectively support its operation in a fair, orderly and transparent manner. Recommendation 5 (*'Market Operation Requirements'*) sets out transparency requirements in trade disclosures to promote price discovery and competition, which apply to all CASPs and not just those acting as market operators. Transparency requirements and trade disclosure expectations apply to both on-chain and off-chain activity.

- ***Chapter 4 – Recommendations in Relation to the Listing of Crypto-Assets and Certain Primary Market Activities***.

  This Chapter relates to the management of conflicts of interest that may arise from the listing and trading of crypto-assets by CASPs. Many crypto-assets are sold without important disclosures about the crypto-asset and its issuer. There is a lack of accurate and sufficient disclosures to facilitate informed decision-making, a key tenet of traditional financial markets. There also tends to be little, if any, verifiable continuous information provided about or by the crypto-asset issuer. Recommendation 6 (*'Admission to Trading'*) states that CASPs should adopt and disclose substantive and procedural listing and delisting standards pertaining to crypto-assets. The recommendation also specifies the types of disclosures that regulators may consider requiring, including information that may be more relevant to stablecoins. Recommendation 7 (*'Management of Primary Markets Conflicts'*) is concerned specifically with the management of conflicts around crypto-assets issued by crypto-asset issuers in which the CASP has a material interest. Conflict mitigants could include prohibitions on the CASP listing/trading such assets.

- ***Chapter 5 – Recommendations to Address Abusive Behaviors***

  This Chapter provides Recommendations and supporting guidance to address market integrity risks, exacerbated by the fragmented, cross-border nature of the crypto-asset market, such as (1) the lack of effective market surveillance, (2) manipulative market practices (including pyramid and Ponzi schemes, 'pump and dump' schemes, wash-trading, and front-running), (3) insider dealing and unlawful disclosure of inside information; and (4) fraudulent, misleading, or insufficient disclosure. To address such behaviors, Recommendations 8 to 10 (*'Fraud and Market Abuse; Market Surveillance; Management of Non-Public Information'*) set out the critical expectation that there should be effective systems and controls to identify and monitor for manipulative market practices and to prevent leakage and misuse of inside information. Consideration is given to the availability of data ('on-chain' and 'off-chain'), consistent reporting

standards and the existing tools available to regulatory authorities (e.g., intelligence and co-operation) and market participants (e.g., surveillance systems and controls). Alongside ongoing efforts to improve regulatory reporting, regulators should encourage CASPs and the wider industry ecosystem to promote and adhere to international data standards to help improve market transparency and facilitate effective regulatory reporting and market monitoring.

- ***Chapter 6 – Recommendation on Cross-Border Co-operation***

  This Chapter and its supporting guidance respond to the cross-border character of crypto-asset trading by setting out a critical recommendation for how IOSCO members should adopt best practices for international co-operation to help ensure effective supervision and enforcement (*see Recommendation 11 'Enhanced Regulatory Co-operation'*), and to reduce the risk of money laundering. Experience has shown that CASPs often present themselves as operating in a borderless manner and tend to take an ambivalent approach to regulatory compliance. This – in tandem with the global reach of the crypto-asset market, its participants, activities, and some unique characteristics linked to the underlying distributed ledger technology ("DLT") and cryptography, as well as the scale and scope for cross-border regulatory arbitrage – means that investor protection and market integrity issues will persist without coordinated international regulatory action to address them. IOSCO's wide memberships in securities and derivatives markets, with market conduct regulatory expertise and existing information-sharing tools for authorization, supervision and enforcement, are well positioned to achieve investor protection and market integrity objectives.

- ***Chapter 7 – Recommendations on Custody of Client Monies and Assets***

  This Chapter provides Recommendations and supporting guidance to deal with custody-related risks and the safeguarding of Client Monies and Assets and to provide clients with clear, concise and non-technical disclosures of the associated risks. These risks relate, for example, to the asset segregation, re-use of assets, liability and ownership considerations. The Recommendations address, amongst other things, the controls that should be embedded within regulatory frameworks to help ensure that where Client Monies and Assets are held by CASPs, they are held safely, and transferred securely, and that inappropriate mixing of assets and other potential abuses are avoided. *(See Recommendations 12 to 16: 'Overarching Custody Recommendation'; 'Segregation and Handling of Client Monies and Assets'; 'Disclosure of Custody and Safekeeping*

Arrangements'; Client Asset Reconciliation and Independent Assurance; Securing Client Money and Assets').

- ***Chapter 8 – Recommendation to Address Operational and Technological Risks***

  This Chapter provides the Recommendations and supporting guidance to address the broad spectrum of operational risks that can arise because of lax controls at CASPs combined with the risks related to DLT and smart contracts. *(See Recommendation 17 'Management and Disclosure of Operational and Technological Risks'*).

- ***Chapter 9 – Recommendation for Retail Distribution***

  This Chapter provides the recommendation and supporting guidance to address the particular issues not covered elsewhere in this report that arise from CASPs' promotions to retail investors of activities and services relating to crypto-assets. Recommendation 18 (*'Retail Client Appropriateness and Disclosure'*) sets out to help ensure that existing or new regulations require CASPs to diligently assess and onboard retail investors who are aware of, and deemed suitable to take on, the greater speculative risks inherent in this market, and to use appropriate measures when promoting crypto-assets to this population, including if crypto-assets are promoted on social media. Indeed, retail investors often would not otherwise hold or trade their own investment portfolios but for the marketing efforts by CASPs to onboard them. Therefore, a particularly acute asymmetry of information arises between CASPs and the retail investor, the significance of which is intensified by the weak market discipline arising in part from the relatively low level of participation of institutional and professional investors, and the unregulated or non-compliant distribution channels that are used to distribute crypto-assets to retail investors, often on a cross-border basis.

Applicability of the Recommendations to Stablecoins

While each of the Recommendations in this Final Report also apply to stablecoins,[6] specific additional guidance in relation to stablecoin disclosures and the custody of reserve assets is included in the box text under Recommendation 6 and the Custody of Client Money Asset

[6] As noted in the preamble to Recommendation 1, particular jurisdictions may allocate responsibility for the regulation and oversight of certain kinds of stablecoins to different Regulators that possess discrete and complementary mandates and objectives, to address investor protection and market integrity risks.

Recommendations.

There are also additional policy recommendations regarding stablecoins, beyond IOSCO's, of which regulators should be cognizant. These include the Financial Stability Board (FSB) Recommendations on the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements and CPMI-IOSCO's report on stablecoin arrangements, noting potential use cases of stablecoins as a payment instrument.

In applying these Recommendations, regulators should consider any unique issues, risks, and conflicts that CASPs have regarding stablecoin arrangements. The Recommendations regarding conflicts of interest, speculation, and disclosure are particularly important (Recommendations 2, 3, 7, 8). For example, a CASP may be directly involved with a stablecoin issuer in creating and redeeming stablecoins and/or maintaining the stablecoin price peg, which creates conflicts and gives rise to potential misuse of inside information, market manipulation and other misconduct. In addition, risks to crypto-asset trading markets and CASPs are directly affected by the credit risk of the stablecoin issuer.

The critical role of stablecoins in crypto-asset markets, and their potential to be used in cross-border activities, highlight the importance of cross-border co-operation (Recommendation 11).

Annex C includes a brief overview of stablecoins, their roles and uses in crypto-asset markets, and describes some of their idiosyncratic features and risks.

Stakeholder Engagement

These Recommendations and guidance take into account feedback from the public consultation, as well as extensive pre-consultation outreach with IOSCO members and external stakeholders. They have also benefited from the advice of IOSCO's Affiliate Member Consultative Committee (AMCC).[7]

Interaction with the FSB and the other Standard Setting Bodies

At a global level, the International Monetary Fund (IMF) and the FSB are calling for more regulation of the crypto-asset market. Acting on IOSCO's investor protection and market

[7] The AMCC is comprised of 68 IOSCO affiliate members, representing securities and derivatives markets and other market infrastructures, self-regulatory organizations (SROs), investor protection funds and compensation funds, as well as other bodies with appropriate interest in securities regulation. There are currently 32 jurisdictions represented in the AMCC which also includes ten regional or international associations."

integrity mandates, these Recommendations look to complement and support the work of the FSB and the sectoral initiatives of other international Standard Setting Bodies (SSBs). Risks to investors and markets arising from market integrity and investor protection concerns can also have a consequential systemic impact within crypto-asset markets, and potentially also on wider financial stability given the lack of transparency and possible growing linkages to the traditional financial sector.

IOSCO is also pursuing its systemic risk mandate for crypto-asset market activities through its engagement with the FSB's agenda on the financial stability implications of crypto-assets. On 17 July 2023, the FSB published its two final reports on the international regulation, supervision and oversight of crypto-assets activities and markets from a financial stability perspective.[8] These FSB reports set out high-level principles for crypto-asset markets. The IOSCO Recommendations set out more granular regulatory expectations to mitigate the market and conduct risks. This helps to ensure alignment and complementarity in the respective regulatory agendas.

Through CPMI-IOSCO,[9] IOSCO also published guidance on the application of the principles for financial market infrastructure (PFMIs) to systemically important stablecoin arrangements used for payments[10] and continues to monitor market developments.

The Basel Committee on Banking Supervision (BCBS) has finalized a standard on the prudential treatment of banks' exposure to crypto-assets. Following the publication of the crypto-asset standard, there are various elements of the standard that are subject to close monitoring and review.

Furthermore, the Financial Action Task Force (FATF) has issued guidance concerning how FATF Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) obligations apply to virtual assets and virtual asset service providers.[11] For example, the Travel Rule requires virtual asset service providers and other financial institutions to share relevant originator and beneficiary information alongside virtual asset transactions. This, combined with the other work

8 See 'High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets (Final Report)' and 'High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangement (Final Report)'.

9 Committee on Payments and Market Infrastructures.

10 See Application of the Principles for Financial Market Infrastructures (PFMI) to stablecoin arrangements.

11 See, e.g., Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

being progressed by global SSBs, illustrates the concerted international effort taking place to develop a coordinated global framework of regulation and supervision for crypto-assets to address the risks associated with crypto-asset activities.

Market Backdrop informing the Need to Develop a Globally Consistent and Coordinated Approach to Crypto-Asset Regulation

Given the global nature and certain unique characteristics of the crypto-asset market, the application of robust regulatory standards alongside international regulatory co-operation will be pivotal to help ensure that any useful innovation can occur while minimizing the risk of regulatory arbitrage and maintaining standards of investor protection and market integrity.

Global retail investor exposure to crypto-assets has grown exponentially in recent years, as have retail investor losses due, not only to market conditions, but also regulatory non-compliance, financial crime, fraud, market manipulation, money laundering and other illegal crypto-asset market practices. The fragility and interconnectedness of the crypto-asset market continues to leave entities and investors exposed to significant losses triggered by all too frequent shock events.[12]

Given the speculative nature driving the demand for many crypto-assets, the lack of intrinsic value in the vast majority of crypto-assets, high levels of retail participation, and the history of losses suffered by retail investors, robust investor protection measures are essential. For example, data from the Bank for International Settlements (BIS) examining CASP activity, calculated on a sample of more than 200 crypto-asset trading apps operating in more than 95 countries, from August 2015 – December 2022, shows that a majority of the users of such apps in nearly all economies experienced losses on their bitcoin holdings.[13]

Many retail investors conduct their trading activities through, and entrust custody of their crypto-assets to, CASPs. There have been many cases where CASPs, including those with the

[12] Examples in 2022 alone include Terra / Luna, Celsius, Voyager, Three Arrows Capital, and FTX.

[13] See BIS Bulletin No. 69: Crypto shocks and retail losses More users trade when the bitcoin price increases…but a large share of users in nearly all economies probably lost money. In nearly all economies in the sample, a majority of investors probably lost money on their bitcoin investment. The median investor would have lost $431 by December 2022, corresponding to almost half of their total $900 in funds invested since downloading the app. Notably, this share is even higher in several emerging market economies like Brazil, India, Pakistan, Thailand and Turkey. If investors continued to invest at a monthly frequency, over four fifths of users would have lost money.

largest market share and highest trading volumes, [14] have demonstrated a lack of willingness to comply with applicable regulatory frameworks that seek to achieve investor protection and market integrity outcomes, and in many cases have structured their operations in a way to evade such frameworks. By not complying with such measures, CASPs profit off retail investors while seeking to avoid the crucial safeguards that come with adherence to regulatory requirements.

[14] According to some data, the three largest CASPs purportedly account for almost three quarters of all trading volume.

CHAPTER 1: OVERARCHING RECOMMENDATION ADDRESSED TO ALL REGULATORS

Preamble: Intent of the Recommendations

The exposure of retail investors across the globe to crypto-assets has grown in recent years, as have retail investor losses amid regulatory non-compliance, financial crime, fraud, market manipulation, money laundering and other illegal crypto- asset market activity. Given the similar economic functions and activities of the crypto-asset market and the traditional financial markets, many existing international policies, standards and jurisdictional regulatory frameworks are applicable to crypto-asset activities.

IOSCO is issuing these Recommendations to help IOSCO members apply relevant existing IOSCO objectives, principles, standards, recommendations and good practices, as appropriate, to crypto-asset activities within their jurisdictions. More specifically, the Recommendations respond to widespread concerns regarding investor protection and market integrity within the crypto-asset markets. The need to address these concerns is evident from repeated instances of market turmoil involving crypto-asset trading, lending and borrowing platforms and other market participants, resulting in significant losses and risks to retail investors due to inadequate protections and safeguards.

Many crypto-asset activities and markets currently operate in non-compliance with applicable regulatory frameworks or are unregulated. These Recommendations recognize that some jurisdictions have existing regulatory frameworks that encompass crypto and digital assets, while some jurisdictions are in the process of developing regulatory frameworks. In addition, in some jurisdictions, the regulatory framework may allocate responsibility for the regulation and oversight of crypto and digital assets to different Regulators that possess discrete and complementary mandates and objectives, to address investor protection and market integrity risks. 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.[15] These Recommendations should be considered by IOSCO

[15] Given the diversity of operating landscapes across different jurisdictions, the application and/or implementation of the 18 Recommendations can take into account the context of specific legal structures prevailing in each jurisdiction, as well as the respective mandates of individual regulators where relevant. This can be met where a regulator, through its given mandate and the regulatory frameworks it applies, sets out clear principles-based expectations for a CASP to meet (which can be supported by regulatory guidance, as appropriate), so as to achieve the same regulatory outcomes articulated in this report.

members as they apply existing regulatory frameworks, or they are granted new powers and/or develop new requirements (such new powers and/or new requirements, together "New Frameworks"), to crypto and digital assets and related activities in a manner that achieves outcomes across jurisdictions consistent with the IOSCO Objectives and Principles for Securities Regulation.

These Recommendations apply to all types of crypto-assets. Accordingly, each of these Recommendations also apply to stablecoins. However, additional guidance in relation to stablecoin disclosures and the custody of reserve assets is included under Recommendation 6 and the Custody and Client Assets Recommendations to clarify how these Recommendations apply additionally to some of the idiosyncratic features or risks presented by stablecoins.

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 principles, 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.

IOSCO Principles supported: 1 – 7.

The IOSCO Standards apply generally to all crypto-assets, their issuers and the provision of services in relation to primary issuance, secondary trading and services and activities linked thereto.

As crypto-assets markets and market participants have grown significantly, with market participants often acting in non-compliance with existing laws or regulations, in consideration of the identified risks in the crypto-asset market and significant ongoing harm to investors, regulators are encouraged to analyze the applicability and adequacy of their regulatory frameworks, and the extent to which:

(1) crypto-assets are, or behave like substitutes for, regulated financial instruments,[16] and

(2) investors have substituted other financial instrument investment activities with crypto-asset trading activities.

Accordingly, these Recommendations focus on the economic substance of a crypto-asset and its substitutability vis-à-vis traditional financial instruments (notwithstanding the crypto-asset's purported potential use case or purpose as stated in supporting marketing and/or distribution materials). Regulators are therefore encouraged to evaluate whether specific requirements address or are needed to address the investor protection and market integrity risks associated with crypto and digital asset activities or certain types of crypto-assets and use existing regulatory and/or New Frameworks to regulate the services and activities.[17]

Application of IOSCO Standards, supported by these Recommendations, will facilitate more effective supervision, enforcement and international co-operation regarding CASPs, with the goal of promoting regulatory compliance. In addition, co-operation and coordination among international bodies such as the FSB and the BIS, and between the SSBs (such as IOSCO, CPMI-IOSCO, the BCBS and FATF) on crypto-assets and crypto-asset regulation are important to achieve greater regulatory harmonization and minimize regulatory arbitrage. This should help facilitate a level playing field between crypto-assets and traditional financial markets and help reduce the risk of regulatory arbitrage arising from any differences in how rules apply to, and are enforced with respect to, crypto-assets and traditional financial markets.

IOSCO as a global membership organization[18] with deep capital markets regulatory expertise is well positioned to achieve these objectives.

16 For these purposes, financial instruments include securities and derivative instruments thereof as well as traded commodity derivatives. Depending on the jurisdiction it would also include traded commodities.

17 As stated in IOSCO Principle 7, the Regulator should have or contribute to a process to review the perimeter of regulation regularly.

18 The IOSCO membership regulates more than 95% of the world's securities markets in more than 130 jurisdictions: securities regulators in emerging markets account for 75% of its ordinary membership.

CHAPTER 2: RECOMMENDATIONS ON GOVERNANCE AND DISCLOSURE OF CONFLICTS

Recommendation 2 – (*Organizational Governance*)

Regulators should require 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 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 segregation of functions and activities, as well as separate registration and regulation of certain activities and functions to address this Recommendation.

IOSCO Principles supported: 8, 23, 31, 33, 34

Although often presenting themselves as "exchanges", many CASPs typically engage in multiple functions and activities under 'one roof' – including exchange services operating a trading venue, brokerage, market-making and other proprietary trading, offering margin trading, custody, clearing, settlement, and services relating to lending and/or staking – whether through a single legal entity or a closely affiliated group of legal entities that are part of a wider group structure.

Conflicts arise from engaging in these activities and functions in a vertically integrated manner. For example, a CASP that operates an order-matching service has a conflict with its users if it is also making markets or otherwise trading as principal against other users in that market. A CASP that allows margin trading may have an incentive to offer margin to an affiliate on terms better than it offers to other users.

Regulators should evaluate whether permitting a CASP to continue to engage in multiple activities in a vertically integrated manner gives rise to conflicts of interest that are not capable of being mitigated and for which disclosure is ineffective to protect markets and investors, in which case they should consider requiring legal segregation of functions and activities. For

example, where a CASP engages in proprietary trading alongside the operation of a trading platform, regulators should consider whether the conflicts of interests presented are unmanageable within the CASP, and address them through requiring legal segregation of these functions and activities, especially where these services are offered to retail clients. This would involve splitting particular CASP functions into separate legal entities, with separate board and management teams, in addition to operating as distinct functions within a given entity.

In addition, if considering New Frameworks, regulators should further consider taking steps to require CASPs to establish effective conflicts of interest policies, procedures and controls and provide public disclosure and reporting, as well as annual effectiveness reviews in light of any new activities or services offered. Regulators may also consider imposing additional independence requirements or de-coupling of functions.

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, 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).

IOSCO Principles Supported: 31, 34, 35 and 37

If a CASP is engaging in different activities and functions in a crypto-asset trading environment, it is important for investors and regulators to understand the precise activities and functions that the CASP is providing, and in what capacity it is acting, in relation to its clients.

The vertical integration and aggregation of different activities and roles of CASPs makes this issue more acute. Recent events have shown that clients do not understand the differing conflicting activities and roles that CASPs are playing in a vertically integrated organization and operational structure. For example, it may not be clear to the client of a CASP the capacity in which the CASP is acting, particularly if the CASP combines multiple functions, within itself and/or through a group of affiliated entities.

The type of disclosure by a CASP that may be important includes –

- The specific legal entity with whom the client is contracting;
- The specific services and activities that are being provided by the CASP and the relevant terms and conditions, and the role of the CASP when handling or executing clients' orders (e.g., whether as a principal or agent) and when holding in custody, moving, or making any use of Client Assets; and
- If the CASP is effecting transactions in crypto-assets on behalf of its clients, the activities that the CASP engages in to effect the transactions, including whether the CASP, or its affiliates, are engaging in market-making activities, whether any client trades will be made with the CASP or its affiliates on a principal basis, and how the CASP protects clients against front running trades;

If permitted to perform multiple functions in a vertically integrated manner (to the extent the regulator permits this combination of activities and functions), a CASP should identify and disclose the conflicts that the CASP has when acting in multiple capacities, the policies and procedures to prevent or mitigate such conflicts, and the risks to clients arising from the vertically integrated operations (including a lack of protection from 'self-dealing' by the CASP, among others).

CHAPTER 3: RECOMMENDATIONS ON ORDER HANDLING AND TRADE DISCLOSURES (TRADING INTERMEDIARIES VS MARKET OPERATORS)

RECOMMENDATION FOR TRADING INTERMEDIARIES

Recommendation 4 – (*Client Order Handling*)

Regulators should require a CASP, when acting as an agent, to handle all client orders fairly and equitably. Regulators should require a CASP to have systems, policies and procedures to provide for fair and expeditious execution of client orders, and restrictions on front-running client orders. Regulators should require that a CASP discloses these systems, policies and procedures to clients and prospective clients, as relevant.

Orders should be handled promptly and accurately recorded.

IOSCO Principles Supported: 29, 31

Despite common market parlance of collectively referring to CASPs as "exchanges" or "trading platforms", a CASP may not in fact be an exchange (or what is commonly known as a market operator). It may instead operate as an intermediary such as a broker or dealer, or both. On the basis of "same activity, same risk and same regulation/regulatory outcomes", specific Recommendations should apply to CASPs based on the role that they undertake.

Information asymmetries and the lack of client disclosures arise due to a number of factors, including a lack of transparency by the CASP, and/or non-compliance with existing requirements concerning the role and capacity in which it is acting (particularly if it combines multiple activities and functions as described in the previous sections).

Clients may not understand that the CASP is trading against them and therefore is not acting in the clients' best interests. Clients also may not understand that the CASP may be front-running client trades, or that it may not be providing the best price or execution for the client's trade. These inherent conflicts can give rise to significant investor harm.

To the extent not already addressed in regulation, regulators should require a CASP to implement systems, policies and procedures that provide for a fair, orderly and timely execution of client orders. Such systems, policies and procedures should be aligned with existing relevant securities and other regulations (e.g., requirements with respect to precedence of client orders and prohibition of front-running). When executing client orders, CASPs should take sufficient

steps to obtain the best possible result for their clients taking into account all relevant execution factors such as price, costs (both the explicit and implicit market impact costs), speed, likelihood of execution and settlement, size, nature or any other consideration relevant to the execution of the order.

When requiring disclosure of such policies and procedures, to the extent not already addressed in regulation, regulators may consider requiring the CASP to perform the following in accordance with the regulators' authority:

- When entering an agreement to provide order execution services to clients, disclose how the execution services will be done (e.g., executed on a principal or agency basis);
- Disclose to regulators and market participants the order-routing procedures and how these are applied fairly (e.g., requirements with respect to precedence of client orders and prohibitions on front-running);
- Disclose any arrangements in place with third parties for routing of client orders, including arrangements concerning payment for order flow (PFOF), or any other forms of inducements;
- Take reasonable steps to deliver best execution for clients;[19] and
- Disclose any significant differences from order handling rules applied to the trading of financial instruments on public markets in the jurisdiction of the client.

RECOMMENDATION FOR MARKET OPERATORS

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 consistent with, those that are required in traditional financial markets.

IOSCO Principles Supported: 33, 34, 35

In many jurisdictions, organized exchanges and trading venues are required to provide public trade transparency, for example, by displaying current bid and offer prices and the depth of

[19] For these purposes, the term best execution should be understood in a manner consistent with a jurisdiction's requirements and, in jurisdictions where regulatory best execution of orders may not be required, to comprise, at a minimum, the 'fair and expeditious' execution of the order by a CASP.

trading interest.

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.

Regulators should require a CASP acting as a market operator to provide market participants/investors with access to an appropriate level of pre-trade and post-trade information to promote transparency, price discovery, and competition. Regulators should consider how to provide investors with useful pre-trade information, including the bids and offers available on the CASP to enable crypto-asset investors to know, with a reasonable degree of certainty, whether and at what prices they can trade the crypto-assets.

Post-trade information on the prices, trade time and the volume of all individual transactions occurring on a CASP should be made publicly and freely available to the fullest extent practicable.

CHAPTER 4: RECOMMENDATIONS IN RELATION TO LISTING OF CRYPTO-ASSETS AND CERTAIN PRIMARY MARKET ACTIVITIES

Recommendation 6 – (*Admission to Trading*)

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 crypto-assets from trading. These standards should include the substantive and procedural standards for making such determinations.

IOSCO Principles Supported: 16, 17

Substantive and procedural listing standards play a key role in investor and market protections in traditional markets. These standards for crypto-assets are just as important, as is the public disclosure of these standards.

As with traditional financial markets, the availability of ongoing information about the financial instrument (in this case, the crypto-asset) and about the issuer is key to informed decision-making and pricing in any trading market.

In the crypto-asset market today, many crypto-assets are sold without important disclosures about the crypto-asset, its main features, the associated risks, and its issuer. Further, there tends to be little, if any, verifiable continuous information provided about or by the crypto-asset issuer. For those jurisdictions where existing rules apply already to crypto-asset issuers, including those relating to disclosures and protections against fraudulent statements, the crypto-assets are being sold in non-compliance with the law.

However, as crypto-asset trading activities implicate the same concerns as traditional financial markets, initial and ongoing information about crypto-assets and crypto-asset issuers is essential to avoid information asymmetries, to help protect against fraud, and to provide transparency to investors trading crypto-assets.

To address these issues from the trading platform standpoint, regulators should require a CASP to adopt substantive and procedural listing standards relating to crypto-assets and their issuers and describe the quantitative and/or qualitative standards that the CASP uses to assess a crypto-asset when approving the admission to trading, permitting it to continue to be admitted to trading, and standards for when its listing may be removed. The disclosures, as relevant, should

also include the procedures used to make those assessments.

In connection with the type of information that should be made available initially, and on an ongoing basis, about the crypto-asset, regulators may consider requiring the types of disclosures that apply when listing any financial instrument for trading on a traditional exchange.

This information would typically include, for example (but is not limited to), a comprehensive description of the crypto-asset, information about ownership and control of the crypto-asset, as well as full information about the issuer and its business, including audited financial statements, and information about the issuer's management team.

Regulators should require a CASP to also adequately disclose relevant information, including (but not limited to):

- The risks associated with the crypto-asset;
- Trading history of the crypto-asset, including volumes and prices;
- Operational description of the crypto-asset, including any incidents of manipulation or security failures;
- Token ownership concentration and any options and/or lock-ups for insiders and affiliates;
- Protocols for transfers; and
- The CASP's treatment of the client crypto-assets and their respective rights and entitlements when events such as, but not limited to, hard forks and airdrops occur.

These disclosures should apply and are important, even where there is no clearly identifiable entity issuing a crypto-asset.

CASP Disclosures about Stablecoins

CASPs that list stablecoins should consider additional information that should be disclosed to customers. To address this, **Recommendation 6** should be read with the following guidance in relation to stablecoins. Regulators should consider requiring a CASP to disclose, as relevant:

1. The terms of the stablecoin including:

(a) what the stablecoin represents, including the reserve assets, how the stablecoin is pegged and the reference asset for the peg (e.g., to a single fiat currency, a basket of currencies, etc.);

(b) the mechanism to support the peg, including whether the stablecoin is fully backed or

supported by a reserve of assets or specific types of assets;

(c) the mechanisms for creating and redeeming the stablecoin;

(d) the rights of any and all stablecoin holders to present the stablecoin for redemption to the issuer, to the CASP or to other third parties, and any potential or existing claims against the stablecoin issuer and/or against the reserve assets;

(e) whether a stablecoin holder has an enforceable direct claim against the issuer of the stablecoin and/or its reserve assets; and

(f) whether and how the stablecoin holder can exchange their stablecoin, in a timely manner, for underlying fiat currency, and any fees that may be levied in respect of this.

2. Risks relating to the stablecoin and stablecoin issuer including:

(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;

(b) how the reserve assets are safeguarded, who is holding the reserve assets and in what capacity, whether reserve assets are invested in other assets and the investment policy, along with other disclosures set out in Recommendation 14;

(c) what potential or actual conflicts of interest exist between the CASP and the stablecoin issuer and how those conflicts of interest are addressed;

(d) the regulatory status of the stablecoin in jurisdictions in which it is used;

(e) public transparency about the stablecoin issuer's reserve; and

(f) whether the issuer has provided an independently audited and complete set of financial statements that includes the reserve assets.

Recommendation 7 – (*Management of Primary Markets Conflicts*)

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.

IOSCO Principles Supported: 29, 31, 33, 34

Currently, CASPs engage in a multitude of activities in a vertically integrated manner, many of which are being done in non-compliance with applicable law. Among the activities that CASPs currently engage in are listing and trading crypto-assets that they issue or those of crypto-asset issuers in which they have, or acquire, a material interest. In these cases, CASPs have both a strong incentive and opportunity to influence the price discovery process, particularly when also acting as a market maker in the relevant crypto-asset. Such activities pose significant conflicts of interest and can give rise to significant investor harm.

A CASP engaging in these activities can have a significant economic interest in the success of the trading and related activities involving the crypto-asset. A CASP or an affiliate that has invested in a prospective enterprise and owns and trades the crypto-assets issued by that enterprise could have access to material non-public information and could have an incentive to use this information when engaging in trading activities. Even absent the misuse of any material inside information, the CASP may have an incentive to promote trading of the crypto-asset even if doing so might not be suitable for or in the best interests of its clients.

Regulators should consider requirements designed to mitigate these effects. The approach could include, for example, prohibitions on the CASP listing and/or trading crypto-assets in which the CASP has a material interest.

CHAPTER 5: RECOMMENDATIONS TO ADDRESS ABUSIVE BEHAVIORS

Recommendation 8 – (*Fraud and Market Abuse*)

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.

IOSCO Principles Supported: 31, 33, 34, 35, 36

Regulation of traditional financial markets prohibits abusive practices that undermine market integrity. Three commonly observed types of abusive practices include (but are not necessarily limited to):

i. ***Unlawful disclosure of material, non-public information*** – Disclosing or 'tipping' inside information, except where strictly necessary and under appropriate conditions, allows those individuals to profit from this information and gives certain market participants an unfair advantage over others.

ii. ***Insider dealing*** – Trading based on 'inside' or material non-public information creates an unfair advantage due to the insiders privileged position at the expense of others.

iii. ***Market manipulation*** – Behaviors that create a false or misleading signal as to the supply, demand or price of a financial asset or otherwise impacts trading in the asset though any other form of deception or contrivance.

Crypto-asset markets should be regulated in a manner consistent with the aim of preventing the same (as well as any idiosyncratic) types of fraudulent and manipulative practices that exist in traditional financial markets. In some jurisdictions, these types of fraudulent and abusive practices in crypto-asset markets may already be covered by existing regulatory frameworks. New Frameworks should explore ways to impose such prohibitions, seeking alignment and consistency of outcomes when tackling market abuse in both traditional financial markets and crypto-asset markets.

Regulators should review their offence provisions and apply them as needed to deal with any potential gaps and new market developments.[20]

Recommendation 9 (*Market Surveillance*)

Regulators should have market surveillance requirements applying to each CASP, so that market abuse risks are effectively mitigated.

IOSCO Principles Supported: 31, 33, 34, 36

Market surveillance is an important tool for deterring and detecting fraudulent or manipulative activity in traditional financial markets, and market surveillance for crypto-asset markets should provide a similar level of protection.

As with traditional financial markets, regulators should consider – to the extent that existing frameworks do not already apply – the following when evaluating market surveillance tools, systems and controls that should apply to CASPs:

- The timeliness of surveillance of transactions and orders to deter and detect market abuse.
- Controls to take prompt remedial actions upon discovery of market abuse on their platform (e.g., suspension of trading).
- Systems for sharing information related to suspected market abuse between relevant crypto-asset markets.
- Systems to detect and report suspicious transactions and orders to the relevant body.
- Systems to identify malicious actors from a cyber, financial crime and market integrity standpoint.
- Requirements, in line with FATF recommendations for AML-CTF, including (amongst other things) Customer Due Diligence Requirements.

Regulators should consider requiring proportionate additional systems and controls, based on the nature, scale and complexity of the CASP's business. This could, for example, include the development of appropriate systems by CASPs to effectively monitor media (including social

[20] It is worth noting here that while offence provisions will apply to CASPs, social media personalities or so-called 'finfluencers' and those providing investment recommendations will generally also come within the scope of relevant market manipulation provisions and therefore potentially be liable, both civilly and criminally, when engaging in these types of abusive practices.

media) for manipulative practices (i.e., information sharing on prospective listings on telegram, signal, etc.). As appropriate, regulatory authorities should also consider monitoring relevant media, including social media.

In evaluating whether market surveillance tools are effective, regulators should consider how to assure, amongst other things, oversight and verification of on-chain and off-chain transactions, including those transactions occurring directly on a CASP through the internal recordkeeping of ownership changes in omnibus accounts.[21] Regulators should evaluate different ways to engage in such oversight and verification, including requiring the detailed reporting of so-called 'off-chain activity' or settling of transactions on the internal books and records of the CASP, not reflected on the public ledger or blockchain.

Moreover, effective market surveillance requires greater oversight of on-chain and off-chain data across platforms. Regulators should make efforts to improve cross-market data transparency and regulatory reporting, supported by high-quality and comparable data, similar to the data that is now available in traditional financial markets.[22] As this is currently a continuing challenge in crypto-asset markets, regulators should consider how to address this issue, which may include market-led solutions and/or regulatory requirements placed on CASPs to report relevant data. In addition, IOSCO intends to (1) conduct work amongst its members going forward to promote the development of data standards that could help to improve the availability, and improved access to better and more homogenized international data sets,[23] and alongside this (2) encourage its members to develop appropriate solutions within their jurisdictions to help further these objectives.

---

21 For the avoidance of doubt, this should apply to transactions arranged or executed by CASPs that provide custodial wallets as well as to those that do not.

22 For example, the same pre- and post- trade price transparency, where appropriate, transaction reporting data, number of accounts, value of the crypto-assets held in the accounts.

23 Consideration could be given to existing approaches like the efforts of LEI and IOSCO, FSB, LEI ROC, and CPMI-IOSCO post financial crisis that aimed at data standardization in traditional financial markets.

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 platform and information related to client orders, trade execution, and personally identifying information.

IOSCO Principles Supported: 31, 34, 36

As in traditional financial markets, a lack of controls on material non-public and market sensitive information, and a lack of restrictions on inappropriate use of such information, may result in manipulative market practices or insider trading.

This may be exacerbated by the cross-border nature of the crypto-asset market, for example, where a particular crypto-asset may be admitted on several trading platforms across jurisdictions, heightening the risk of regulatory arbitrage.

Regulators should thus require a CASP to put in place systems, policies and procedures around the management of material non-public information and to restrict inappropriate use of such information.

These could include the following:

- A process for the CASP to identify and classify information that is material non-public and market sensitive. Examples include, but are not limited to, information regarding the CASP's client orders and the planned listing of a particular crypto-asset;
- System and controls to restrict the access of material non-public and market sensitive information to a controlled list of persons on a 'need-to-know' basis, for example, via the use of ethical walls or information barriers;
- Periodic review of the list of persons who have access to material non-public and market sensitive information;
- Restrictions against the sharing and the use of material non-public and market sensitive information by the CASP and list of persons;
- Processes for monitoring for potential breach of the CASP's systems, policies and

procedures policies regarding material non-public and market sensitive information, including, processes to facilitate whistleblowing and the reporting of potential breaches to the relevant authorities.

CHAPTER 6: RECOMMENDATION ON CROSS-BORDER CO-OPERATION

Recommendation 11 – (*Enhanced Regulatory Co-operation*)

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 co-operation 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.

IOSCO Principles Supported: 13, 14, 15

Many CASPs offer services from offshore financial centers. CASPs often structure and present themselves as having little or no visible substantive presence within any jurisdiction, thus exacerbating supervisory and enforcement challenges that may arise. The provision of services into a jurisdiction by a CASP may nevertheless implicate that jurisdiction's laws.[24]

The differing approaches as well as the attempt by CASPs to avoid regulation or operate in non-compliance with existing regulation raise significant issues. These issues significantly increase the risk of regulatory arbitrage, reduce the ability of jurisdictions to enforce their laws, and depending on the laws of particular jurisdictions, potentially raise the prospect of jurisdictional borders hindering the effectiveness of the authorization and supervision process. They also enable money laundering risks and facilitate financial crime, and reduce the ability of regulators to effectively detect and enforce against these activities.

IOSCO is already active in tackling issues related to day-to-day cross-border co-operation between authorities. Crypto-asset related information requests are already captured by IOSCO's Multilateral Memorandum of Understanding (MMoU) and Enhanced Multilateral Memorandum of Understanding (EMMoU), premised on the underlying principle of "same activity, same risk, same regulation/regulatory outcomes". In tandem with the overarching MMoU and EMMoU, regulators should take proactive steps, bilateral or multilateral, to enable

[24] It is recognized that the issues of international co-operation between regulators in view of the cross-border provision of crypto-asset services overlaps with issues being addressed in the separate proposal for a 20th anniversary review of the effectiveness of the IOSCO MMOU and the IOSCO Retail Market Conduct Task Force recommendations for further work on unauthorised provision of financial services.

sharing of information for effective supervision and enforcement.

Beyond the MMoU and EMMoU, regulators should also share information with one another and, where relevant, with law enforcement authorities, and work together to stop abusive and criminal behaviors, including financial crime and money laundering, and to mitigate risks to investors.

In addition, amongst wider measures to enhance cross-border supervision of the market, regulators should consider bilateral and/or multilateral co-operation arrangements beyond the enforcement context, as appropriate, such as supervisory colleges[25] or networks,[26] or regional arrangements,[27] or other forms of cross-jurisdictional co-operation, to support rigorous and effective ongoing supervision of CASPs operating across multiple jurisdictions.

[25] For example, IOSCO has mentioned potential consideration of supervisory colleges in connection with crypto-asset platforms. See: Lessons Learned from the Use of Global Supervisory Colleges, Final Report, IOSCO (January 2022), pp. 28-30, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD696.pdf.

[26] See: Principles Regarding Cross-Border Supervisory Co-operation, Final Report, IOSCO (May 2010), pp. 31, 36-37, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD322.pdf.

[27] For example, IOSCO APRC (Asia-Pacific Regional Committee) established the APRC Supervisory MMoU, which is the first IOSCO framework undertaken as part of efforts to strengthen supervisory co-operation in the Asia-Pacific region. The APRC Supervisory MMoU enables signatories to exchange broader supervisory information than under the MMoU, that is enforcement-focussed.

CHAPTER 7: RECOMMENDATIONS ON CUSTODY OF CLIENT MONIES AND ASSETS

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.

The proper custody of Client Assets[28] is reliant on the strength of a service provider's systems, policies and procedures as well as the legal arrangements governing the custody relationship. Regulators should require a CASP to ensure that Client Assets are adequately protected at all times, including when placed with a third party chosen by the CASP, specifically aiming to minimize the risk of loss or misuse.

As is the case with traditional financial assets, regulators should set out expectations that the CASP maintain accurate and up-to-date records and accounts of Client Assets that readily establish the precise nature, amount, location and ownership status of Client Assets and the clients for whom the assets are held. The records should also be maintained in such a way that they may be used as an audit trail.

A number of different methods and structures can be used by a CASP to hold Client Assets taking into account risk management, liquidity and efficiency considerations and trade-offs.

IOSCO is not prescribing specific expectations or thresholds regarding, for example, the holding of crypto-asset private keys in "hot" vs "cold" vs "warm" wallets.[29] When considering the maintenance of private keys, safety of Client Assets should be prioritized. For the purposes of this Recommendation, non-custodial wallets are not considered.

Ultimately, sufficient, reliable and clear information should be made available to clients and any third parties (for example insolvency practitioners, regulators and the courts) to enable them to understand the rights to any Client Assets, including the ability for clients to receive their Client Assets back, or an equivalent value thereof, should they suffer losses, for instance, due to the CASP entering an insolvency process.[30]

---

28 For these purpose, "Client Assets" cover both money and crypto-assets held for, and on behalf of, a client.

29 Further operational and technological considerations are set out under Recommendation 17.

30 The outcomes for clients' rights to their assets depend on jurisdictional application of custody and trust arrangements; a CASP should therefore provide its clients with appropriate and accurate disclosure on their respective rights upon the CASP entering into an insolvency process.

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.

IOSCO Principles Supported: 31, 32, 38

Taking into account the technological means by which crypto-assets are created and held, laws and court decisions, and jurisprudence in certain jurisdictions might not yet have evolved in ways that provide CASP clients with legal certainty regarding protection of their crypto-assets.

Regulators should nonetheless require a CASP to segregate Client Assets from their proprietary assets, as well as the assets of any affiliate or service provider held by the CASPs, and place Client Assets in trust or in segregated bankruptcy remote accounts (or provide equivalent protection through legal or accounting mechanisms recognized in the relevant jurisdiction), so that they are separate and distinct from the CASP's own assets/estate.

Regulators should require a CASP to specify how Client Assets are protected against loss or misuse and how such assets are segregated as Client Assets that are not subject to the claims of the CASP's creditors.

Where the CASP expressly takes legal and/or beneficial title to Client Assets (for purposes, e.g., of lending, re-use or re-hypothecation of the crypto-assets), the CASP will cease to hold those Client Assets in trust for the client. The CASP should obtain the client's explicit prior consent to such arrangements. The CASP should provide clear, concise and non-technical disclosure of these arrangements, sufficient for the client to understand that Client Assets are not held in custody and might not be returned should the CASP enter insolvency.

Regulators should impose specific measures in situations where the CASP takes legal and/or beneficial ownership of Client Assets. These requirements should include, for example:

- receiving prior explicit consent from the client for the assets, for example, to be lent out, re-used or re-hypothecated;
- providing clients with clear, concise and non-technical, prior disclosure about the risks of these types of activities, including the potential loss of their entire crypto-asset holdings;

In all cases, whether a CASP is acting as a custodian holding Client Assets in trust, or in another

segregated arrangement, regulators should consider requiring CASPs to:

- maintain accurate and up-to-date records and accounts of Client Assets at all times that readily establish the precise nature, amount, location and ownership status of the assets, and identify the clients for whom they are held; and
- maintain records and accounts that enable it, on a frequent and regular basis, to specify each client's rights and the CASP's obligations to each client with respect to Client Assets.

Recommendation 14 – (*Disclosure of Custody and Safekeeping Arrangements*)

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.**

IOSCO Principles Supported: 31, 32, 38

Where a CASP is providing custody services to a client, regulators should require the CASP to clearly disclose, as relevant, all terms and conditions attached to the custodial activity being provided, such as the safeguards in place to provide for adequate protection of Client Assets from losses or insolvency of the CASP.[31] Regulators also should require the CASP to identify how the

[31] With respect to this recommendation, regulators should carefully consider how to ensure that the disclosure requirements do not require a CASP to reveal technical information that exposes it to heightened cybersecurity risks.

CASP protects the Client Assets, including from the claims of the CASP's creditors.

Where the CASP enters into a sub-custody arrangement with a third party, the disclosure should also detail the terms of these contractual arrangements and any additional risks that these might create for the client, as relevant.

For example, the regulator should require the CASP to disclose to its clients whenever Client Assets are to be held or placed in a foreign jurisdiction, as well as the name of such jurisdiction, and thus may become subject to the client asset protections and/or insolvency regimes of that foreign jurisdiction.

Custody for reserve assets of stablecoins

How reserve assets are held by the stablecoin issuer or others is of paramount importance, as is the fact that these reserve assets remain sufficient at all times to cover redemption of all outstanding stablecoins. The custody and client asset Recommendations should therefore be read, as relevant, as referring to custody of reserve assets backing stablecoins, in addition to Client Assets. Given that a large part of the market for stablecoins is conducted through CASPs, the disclosures set out above in **Recommendation 14,** as relevant, should be included in any disclosures to clients by CASPs.

Recommendation 15 – (*Client Asset Reconciliation and Independent Assurance*)

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.

IOSCO Principles Supported: 31, 32, 38

To support Recommendation 13 on the segregation and handling of Client Assets, a CASP should maintain appropriate books and records to track and record transactions and ownership of Client Assets. The CASP should conduct regular and frequent reconciliation of Client Assets on a client-by-client basis, to identify and resolve any discrepancies in a timely manner. In doing so, CASPs should also take into account both relevant off-chain and on-chain records.

Regulators should require that each CASP implement measures to support reconciliations of

Client Assets, which may include (but not be limited to):

- policies and procedures governing the process and controls for Client Asset reconciliation;
- conducting reconciliations on a regular and frequent basis;
- procedures to reconcile off-chain and on-chain records;
- providing clients with a statement of account, comprising information on their Client Assets and transactions;
- engaging an independent auditor, on an annual basis,[32] to:
    - conduct an independent audit of the CASP's Client Asset environment; and
    - issue an internal control report, including an opinion as to whether the CASP's controls related to custodial services—including the systems, processes and procedures for safeguarding of Client Assets —are designed and operating effectively; and
    - conduct an independent review of the adequacy of CASPs' policies and procedures.

Regulators should have procedures to evaluate audits and independent reviews, investigate instances where these reviews contain qualifications and/or adverse findings, and take such action as they deem appropriate.

Recommendation 16: (*Securing client money and assets*)

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

IOSCO Principles Supported: 31, 32, 38

Where a CASP does not have appropriate arrangements to safeguard Client Assets, this can increase the risk of loss, misuse, and delay in returning Client Assets, particularly in the case of

[32] These engagements should be performed by an independent auditor to obtain reasonable assurance about whether the subject matter information is free from material misstatement (e.g., with respect to the audit), or whether the CASP complied with the specified requirements, in all material respects (e.g., with respect to the internal control report).

an insolvency.

CASPs ostensibly operating as custodians have been hacked in the past and/or have lost the means to access Client Assets they were responsible for safeguarding. In particular, loss of a private key or wallet could mean that recovery of the corresponding Client Assets becomes extremely difficult, if not impossible.

Proper custody of Client Assets is reliant on the strength of a CASP's policies, procedures and controls, including the means of access (such as private keys and wallets). However, a CASP is holding Client Assets, it should maintain adequate policies, procedures and arrangements to minimize risk of loss, theft or inaccessibility to Client Assets.

These policies and procedures should recognize the risks associated with different wallet types (e.g., hot, warm and cold).

Regulators should consider whether and how a CASP can compensate its clients under applicable law, in the event of theft or loss of Client Assets. Depending on the jurisdiction, this could include requiring a CASP to hold sufficient assets to compensate clients (e.g., additional own funds and/or guarantee).

CHAPTER 8: RECOMMENDATION TO ADDRESS OPERATIONAL AND TECHNOLOGICAL RISKS

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.

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.

IOSCO Principles Supported: 31, 32, 33, 34, 38

A CASP faces operational and technological risks similar to those faced by traditional financial institutions.[33]

However, crypto-asset activities may introduce some unique and additional operational and technological risks, including those arising from the underlying DLT used for the issuance, trading and provision of services related to crypto-assets and the deployment of smart contracts, forks and use of cross-chain bridges. The disclosures contemplated by this Recommendation should address these risks, which are idiosyncratic to CASPs.[34] Regulators should require a CASP to put in place sufficient measures to address cyber and system resiliency. These measures should be reviewed at least annually and updated to help ensure that they remain strong and robust. Such measures could include:

- identifying the relevant operational and technological risks which the CASP faces and requiring the CASP to adopt appropriate processes and procedures to address such risks.
- implementing operational and technology risk management framework and

33 For example, see IOSCO (2019), Cyber Task Force Final Report and see CPMI-IOSCO (2016), Guidance on cyber resilience for financial market infrastructures (FMI).

34 With respect to this recommendation, regulators should carefully consider how to ensure that the disclosure requirements do not require a CASP to reveal technical information that exposes it to heightened cybersecurity risks.

conducting at least an annual independent audit from a reputable third party.

- implementing frequent, rigorous code audits to mitigate cyber security risks.

CHAPTER 9: RETAIL DISTRIBUTION RECOMMENDATION

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, or work with other relevant authorities to require, that all promotions and marketing of crypto-assets to retail clients accurately and sufficiently disclose the product and service provided as well as the associated risks in a manner that is fair, clear, and not misleading.

Regulators should require a CASP to implement adequate systems, policies and procedures, including for providing disclosures, in relation to onboarding new clients, and as part of its ongoing services to existing clients. This should include assessing the appropriateness and/or suitability of particular crypto-asset products and services offered to each retail client.

IOSCO Principles Supported: 16, 17, 23

Crypto-asset markets differ significantly from traditional financial markets in having a high proportion of retail participants directly accessing CASP trading platforms. Many crypto-assets and CASPs are operating in non-compliance with applicable law in some jurisdictions, where important retail client protections already exist.

Notwithstanding the applicability of existing regulatory frameworks – considering the cross-border nature of these activities and direct access business models – there are significant additional risks of mis-selling and exposure to fraud in crypto-asset markets, including difficulty in seeking recourse against CASPs and other market participants.

In developing New Frameworks, regulators should ensure, where within their remit, that promotions of crypto-assets are appropriate for retail clients. Similarly, where within their remit, they should impose requirements on CASPs covering suitability/appropriateness assessments of clients and potential clients.[35] Further, regulators should consider how to

[35] If a prospective client does not demonstrate sufficient knowledge, the CASP should not permit trading of crypto- assets.

evaluate CASP marketing materials and advertising about crypto-asset trading generally or for particular crypto-assets.

Promotions to retail clients, where allowed, must not be misleading when relating to the crypto-asset or service being promoted, and any statement made about the crypto-asset or service must be accurate and verified by the CASP. Promotions should be designed to promote a clear understanding by retail clients of what they are buying, such as the key facts and relevant risks around the crypto-asset or service provided (including, for example, the rate of return, or the mechanism for maintaining stability in the case of a stablecoin). This should apply irrespective of how, or on which platform, the promotion is made, which includes traditional, online and social media, as well as digital engagement practices used for targeted marketings, gamification and digital nudging.

If suitability/appropriateness assessments are used by a CASP, regulators should require that the assessments are well constructed and robust. In particular, such assessment should not mislead clients into believing that they sufficiently understand the operations of crypto-asset markets and the related risks.

In addition to clear, concise, non-technical and accurate disclosures that should be provided on the key features and risks related to the crypto-assets and services offered by a CASP, any fee, commission or incentive, directly or indirectly charged to the client, should also be clearly disclosed.

Regulators should consider requiring CASPs to disclose any commercial arrangements with legal or natural persons providing investment advice on crypto-assets admitted to trading on their platform or in which they have a material interest. This extends to any individuals who may be commissioned to recommend investment in particular crypto-assets on media (including social media). In some jurisdictions, the investment advice frameworks apply to recommendations made by service providers, including so-called 'finfluencers' and other intermediaries.

Regulators should require CASPs to have an efficient and effective mechanism to address client complaints. Regulators should also take steps to tackle the risks posed to retail investors by the prevalence of poor marketing practices. This should be done directly where a particular IOSCO member has that mandate, or otherwise in coordination with other domestic regulators who are responsible for issues related to media and advertising (such as advertising standard setters and

consumer watchdogs).

Annex A – Glossary of Relevant Terms and Definitions

This Glossary applies to this report only. It uses technical, non-legal definitions included in the body of this report and (other relevant IOSCO publications). For a small sub-set of terms (not defined in IOSCO publications), the Glossary definitions of other Standard Setting Bodies have been employed for consistency. The Glossary is of limited scope and in no way attempts to set out legal definitions that could create opportunities for regulatory arbitrage, and which remain matters for individual jurisdictions to decide upon.

Blockchain

A form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerized process by which transactions are validated.

Crypto-asset

An asset, sometimes called a "digital asset," that is issued and/or transferred using distributed ledger or blockchain technology. Crypto-assets include, but are 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."

Crypto-Asset Service Provider (CASP)

A service provider that conducts 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 activities such as services relating to lending/staking of crypto-assets and the promotion and distribution of crypto-assets on behalf of others.

Smart Contract

Code deployed in a distributed ledger technology environment that is self-executing and can be used to carry out certain "if/then" type computations. The execution of a smart contract is triggered when that smart contract is "called" by a transaction on the blockchain.

Stablecoin

A crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

Wallet

An application or device for storing the cryptographic keys providing access to crypto-assets. A hot wallet is connected to the internet and usually takes the form of software for the user, while a cold wallet is a hardware that is not connected to the internet and stores the cryptographic keys.

Custodial wallet

A crypto-asset service where a user's crypto-assets and/or means of access (e.g., private keys or a shard of a private key) are kept under custody by a service provider on behalf of the user. The user interacts with the service provider, rather than the blockchain, to manage its crypto-assets. A custodial wallet is also known as a "hosted wallet".

Non-custodial wallet

Software or hardware that stores cryptographic keys for a user, making the user's crypto-assets accessible only to the user, and allowing the user to interact directly with the blockchain and the blockchain-based finance applications. A non-custodial wallet is also known as an "unhosted wallet".

Annex B – Feedback Statement

On 23 May 2023, IOSCO consulted on a set of 18 policy recommendations. The feedback period closed on 31 July 2023, with a total of 80 responses received from a range of stakeholders falling into these broad categories:

1. Industry Association (28)
2. CASP (11)
3. Regulatory Authority (9)
4. Traditional Finance Entity (8)
5. Blockchain Analytics and Intelligence (7)
6. Blockchain Governance (5)
7. Think Tank (4)
8. SRO (3)
9. Natural Person (2)
10. Payments Provider (2)
11. Legal Advisor (1)

The IOSCO Board is grateful for the responses and took them into consideration when preparing the Final Report with Policy Recommendations for Crypto and Digital Asset (CDA) Markets (Final Report). The rest of this section summarizes the replies received on the consultation questions.

Policy Recommendations for Crypto and Digital Asset Markets:

1. Chapter 1 – Overarching Recommendation Addressed to All Regulators

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.

Risk based classification and scope - Taxonomy

There is a general consensus from respondents that taking an outcomes-focused approach is appropriate when applying or developing regulatory frameworks for CASPs.

Several respondents suggested that IOSCO should consider adopting a globally consistent taxonomy for crypto-assets to provide clarity as to the legal character of such assets and a differentiated treatment of a crypto-asset according to its token classification and risk profile.

Respondents highlighted the need for IOSCO to clarify the outer limits of activities that IOSCO principles should be applied to. Suggestions regarding outer limits of activities included clarifying which DLT-based financial products and services are specifically covered by the separate DeFi consultation report, and taking account of the distinction between tokenized securities and other instruments that are subject to existing legal frameworks.

Several respondents asked for clarification on the scope of "ancillary services and other activities" and whether the provision of investment, portfolio management, NFTs and crypto-asset transfer are covered. Several respondents highlighted the need for including additional activities.

IOSCO's response:

Substance over form

Sufficient clarification is already set out covering the applicability of the Recommendations and how they apply. The application of the Recommendations is predicated on economic substitutability and a substance -over -form approach as clearly laid out in the explanatory guidance to Recommendation 1. In applying or developing regimes to cover crypto-assets, IOSCO members should arrive at consistent regulatory outcomes with those expected in traditional finance. However, IOSCO does not regulate the use of particular crypto-asset market acronyms (ICOs, IEOs, NFTs, DAOs, etc.) or particular labels or naming conventions (so-called "exchanges" or so-called "stablecoins") which may be seeking to portray legitimacy and compliance with traditional finance regulations. Instead, the approach focuses on economic substance and substitutability as outlined above. This allows the regulatory approach to adapt and apply to future developments. To strengthen this message further, some additional draft has been added to the preamble of Chapter 1 to further emphasise that the report focusses on the economic substance of crypto-assets and their substitutability vis-à-vis traditional financial instruments (notwithstanding a crypto-asset's purported potential use case or purpose as stated in its supporting marketing and/or distribution materials).

In addition, a short glossary providing generic definitions to aid interpretation of common terms used in the CDA Recommendations has been included by way of Annex A to the draft Final Report. This Glossary uses technical, non-legal definitions that were included in the body of the CDA consultation report (and other IOSCO publications). Annex A includes a clear disclaimer that the Glossary is of limited scope and in no way attempts to set out legal definitions that could create opportunities for regulatory arbitrage, and which remain matters for individual jurisdictions to decide upon.

In relation to the respective scope and interaction between the CDA and DeFi Recommendations, IOSCO will publish an umbrella note explaining in more detail the interoperability between the two sets of Recommendations

2. Chapter 2 – Recommendations on Governance and Disclosure of Conflicts

Recommendation 2 (Organizational Governance): Regulators should require 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 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 segregation of functions and activities, as well as separate registration and regulation of certain activities and functions to address this Recommendation.

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, 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).

Addressing specific conflicts of interests - Functional Segregation

Most respondents were supportive of Recommendation 2 and of the view that Chapter 2 covered adequately the types of conflicts of interest that should be covered.

However, for the purposes of legal certainty, a couple of respondents requested further details and guidance regarding which activities are permissible or potentially problematic.

One respondent asserted that vertically integrated CASPs' activities should be prohibited to combat unmanageable conflicts of interest within CASPs, or alternatively, CASPs should be required to set aside a certain level of capital to ensure the protection of investors in cases of

conflicts of interest.

Another respondent requested further guidance specifically on acute conflicts of interest that cannot be mitigated solely by disclosures, and what kinds of conflicts of interest would require more robust measures to mitigate.

Some respondents mentioned the following other types of conflicts of interest that they think should be covered by a CASP's conflicts of interest arrangements (e.g. commingling of funds, Prohibition on CASPs issuing so-called native or platform tokens, etc.).

One respondent suggested including additional detail in the recommendations on activities/products/services which CASPs, particularly vertically integrated CASPs, must not offer under the same legal entity to avoid conflict of interest.

Some respondents were of the view that it was preferable to leave CASPs the option to manage conflicts of interest through governance, and internal and external control mechanisms and not necessarily to impose more stringent rules such as legal segregation.

Some respondents stressed that while good disclosure was vital, it cannot be the sole measure to address conflicts of interest.

Some respondents recommended introducing disclosure requirements to enhance transparency and mitigate risks, such as implementing robust transaction reporting, establishing a regulatory framework for off-chain transactions, enhancing security and privacy measures, and requiring proportionate obligations for CASPs.

IOSCO's response:

The guidance will be strengthened and tied back to the language in Recommendation 2.

The guidance highlights certain combinations of activities (i.e., acting as market operator and trading intermediary) as an example of a conflict. In order to strengthen the guidance and tie back to the language in Recommendation 2, the guidance now explains that regulators should consider whether the conflicts of interests presented are unmanageable within CASPs and address them through requiring legal separation of these activities, especially where these services are offered to retail clients. This new guidance retains some flexibility for regulators

to require appropriate mitigants for CASPs to manage conflicts, while providing a stronger message around an area of acute potential conduct risk (particularly where retail clients are involved), as illustrated by high-profile firm failures such as FTX. Minor further adjustments have been made to the guidance to further reflect that a jurisdiction can evaluate whether the prohibition on unmanageable conflicts should be instituted in situations where these conflicts cannot be effectively managed by other available conflict management measures (i.e., in a manner that minimizes harm to investors and/or markets to an acceptable level).

Specific disclosures regarding any commercial relationships between CASPs and third parties have been included in the Recommendation 18 setting out that CASPs should also disclose any commercial arrangements with legal or natural persons providing investment advice on crypto-assets admitted to trading on their platform or in which they have a material interest. This extends to any individuals who may be commissioned to recommend investment in particular crypto-assets on media (including social media). In some jurisdictions, the investment advice frameworks apply to Recommendations made by service providers, including so-called 'finfluencers' and other intermediaries.

3. Chapter 3 – Recommendations on Order Handling and Trade Disclosures (Trading Intermediaries Vs Market Operators)

Recommendation 4 (Client Order Handling): Regulators should require a CASP, when acting as an agent, to handle all client orders fairly and equitably. Regulators should require a CASP to have systems, policies and procedures to provide for fair and expeditious execution of client orders, and restrictions on front-running client orders. Regulators should require that a CASP discloses these systems, policies and procedures to clients and prospective clients, as relevant. Orders should be handled promptly and accurately recorded.

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 consistent with, those that are required in traditional financial markets.

Best execution and disclosure

Respondents agreed that the same standards should be applied to the crypto-asset market as that applied to traditional financial markets, including around best execution and disclosure.

Several Traditional Finance Entities and Industry Associations believed that Recommendations 4 and 5 would have a positive impact on price discovery, market integrity, transparency in the market, the management of conflicts of interest, and improved fairness which would then help investors to make informed decisions.

Nuances between market operators and intermediaries

Several respondents also suggested that attention should be paid to the nuances between market operators and intermediaries that act as principal or act as agent due to the fact there are differences in the way they operate and the obligations that they are subject to in traditional financial markets.

Respondents were broadly in favor of CASPs engaging in both roles (i.e., as a market operator and trading intermediary), however, not without limitations in place to manage potential conflicts of interest.

Respondents suggested that CASPs performing both roles should be subject to appropriate controls to ensure effective management of potential conflicts of interest, as is the case in traditional financial markets. This could include implementing best execution and disclosure obligations as well as adhering to robust governance standards and being subject to regulatory oversight.

Furthermore, an Industry Association noted that market participants in traditional finance can engage in dual roles when subject to effective regulation and oversight, therefore, the same regulatory principle should apply to CASPs.

Two Traditional Finance Entities expressed skepticism around CASPs engaging in both roles i.e., acting as both a market operator and trading intermediary.

Data Availability, Reporting and Information Sharing

Respondents agreed with the importance of introducing disclosure requirements regarding off-chain transactions as doing so would improve transparency and market integrity.

Respondents provided several suggestions regarding how CASPs could identify and disclose data related to off-chain transactions. Ranging from the creation of an event notification message system, the real-time logging of order book activity, the mirroring of traditional finance practices to internal record keeping.

However, a Think Tank stated that Recommendation 5 should not prescribe a particular method or procedure for identifying and disclosing pre- and post-trade transaction data for transactions that occur off-chain due to ongoing technological developments in this space.

Some feedback items are about the importance of bringing transparency to off-chain transactions, impediments to data collection on a cross-jurisdictional basis arising from different data protection standards, disclosure and regulatory reporting by CASPs to relevant authorities, acknowledgement of key concepts and mechanisms for international co-operation (e.g. bilateral mechanisms).

IOSCO's response:

Additional guidance under Recommendation 4

With respect to calls for further clarity on how to deliver best, or fair and expeditious, execution, we are including additional guidance under Recommendation 4 on the best execution factors that jurisdictions may require CASPs to take into account (i.e., the execution factors to be assessed and the costs to be considered when executing orders, such as explicit trading costs and implicit market impact costs).

Certain combinations of activities already highlighted.

As currently drafted, the guidance highlights certain combinations of activities (i.e. acting as market operator and trading intermediary) as an example of an inherent conflict.

Recommendations 4 and 5 set out the expectation that CASPs provide post-trade disclosures or transaction reporting of off-chain transactions and an obligation for intermediaries to ensure best execution. These types of disclosures and obligations are likely to provide more information to clients regarding the impact conflicts of interests may have on their order execution. However, conflict disclosure is not a substitute for public price disclosures or for obligations of CASPs to their customers to give the best price on trades. Data transparency and regulatory reporting is integral to effective market surveillance. The Guidance to Recommendation 9 has been expanded in this regard acknowledging the importance of homogenizing data standards.

4. Chapter 4 – Recommendations in Relation to Listing of Crypto-Assets and Certain Primary Market Activities

Recommendation 6 (Admission to Trading): 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 crypto-assets from trading. These standards should include the substantive and procedural standards for making such determinations.

Recommendation 7 (Management of Primary Markets Conflicts): 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.

Expectations surrounding trading admission processes

Respondents generally supported Recommendation 6 on listing and de-listing crypto assets.

Many respondents provided suggestions for further detailed guidance relating to the systems, procedures, policies and disclosures to be put in place by CASPs.

However, some respondents were concerned that it may be challenging, onerous, or irrelevant for CASPs to disclose issuer-related information relating to crypto-assets where are decentralized or which do not have a clearly identifiable issuer.

Some expectations surrounding trading admission processes are conducting due diligence on prospective listing of crypto-assets CASPs to examine the smart contract of any prospective token for malicious code and make certain assurances.

Several respondents (predominantly CASPs) did not support prohibitions on a CASP listing and/or trading any crypto-assets in which they or their affiliates have a material interest.

These respondents commented that there are effective mitigants, such as governance arrangements, polices and disclosures, without needing to enact prohibitions.

IOSCO's response:

There were calls for further guidance regarding the systems, procedures and policies that CASPs should have. This would, to a certain extent, depend on the relevant jurisdictional framework. Therefore, IOSCO will not provide further elaboration on this point.

A question arises as to whether CASPs should be permitted to admit to trading crypto-assets in which they have a material interest. This could involve requiring further disclosures around admission practices and stronger measures around taking proprietary positions in the crypto-assets. After consideration, it was decided that Recommendation 7 (Management of Primary Market Conflicts) is sufficiently robust as drafted, and that additional IOSCO guidance is not needed at this juncture.

5. Chapter 5 – Recommendations to Address Abusive Behaviors

Recommendation 8 (Fraud and Market Abuse): 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.

Recommendation 9 (Market Surveillance): Regulators should have market surveillance requirements applying to each CASP, so that market abuse risks are effectively mitigated.

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 platform and information related to client orders, trade execution, and personally identifying information.

Capturing abusive practices and offences

Overall support from respondents who considered that the draft Recommendations and supporting guidance capture most of the offences occurring in crypto-asset markets. Nevertheless, respondents indicated that specificities of crypto-markets (e.g. on-chain and off-chain data, market fragmentation, direct retail access, etc.) should be taken into account in order to effectively prevent and mitigate market abuse risks. To that end, respondents highlighted some of the novel offences that are bespoke to crypto assets (e.g. private key theft, 51% attacks, MEV, etc.) and then provided a few specific examples of fraudulent behaviors that can be or have been observed in crypto markets.

While some respondents seem to encourage regulators not to perceive the crypto-asset ecosystem as inherently riskier than traditional finance, other respondents provided evidence of rates of insider dealing occurring ahead of crypto-assets listing which are significantly higher than those observed for traditional financial instruments.

Separately, respondents suggested that the definition of inside information and market

manipulation can be broader than in traditional markets and it may need to be adapted to take into account abusive practices that may not yet currently exist in traditional markets. Finally, as abusive behaviors often take place via social media platforms, a couple of respondents suggested covering influencer marketing practices in the Recommendations to ensure that any communication and advertising of crypto assets is not misleading.

Overall support from respondents who considered that market surveillance is a critical element to mitigate market abuse risks within the crypto ecosystem. There was also support for placing increased responsibility on CASPs for preventing, detecting and combating market abuse on their own trading platforms.

However, respondents suggested considering several additional elements to supplement Recommendation 9 as to address risks specific to crypto-asset markets, including adequate monitoring of illicit activities (such as sanction violations, money laundering and terrorism financing), integration of off-chain and on-chain data for market surveillance purposes, development of systems to analyze data contained in news releases and social media posts, improved collaboration among regulators, as well as the adaption of the market surveillance approach depending on the CASP/crypto-activities conducted.

In addition, respondents generally suggested that market surveillance requirements must be updated and amended on a regular basis to address novel risks and trends, also considering that continuous monitoring of market developments, supported by future-proofed regulatory principles, is required to ensure that detection methods remain successful.

IOSCO's response:

Additional details about monitoring social media has been included.

The categorization of abusive practices such as fraud, market manipulation and market abuse are arguably broad enough to also capture these 'bespoke' detrimental market integrity practices on display in crypto-asset markets.

Additional detail by way of a footnote has been included in the guidance to Recommendation 8 to identify expectations on CASPs to monitor media (including social media) for manipulative practices (i.e., information sharing on prospective listings on telegram, signal,

etc.). Feedback suggested that the guidance could also call on regulatory authorities to build appropriate expertise and consider conducting social media monitoring.

Further commentary on data has been included.

Data transparency and regulatory reporting is integral to effective market surveillance. The Guidance to Recommendation 9 has been expanded in this regard acknowledging the importance of homogenizing data standards. As part of this, consideration has been given to whether the data standards should be the same as in traditional markets, such that they could support the same pre- and post-trade price transparency obligations (where appropriate) and the ability of jurisdictions to surveil and examine markets for pricing information. Notwithstanding the fact that the non-compliance of CASPs is a contributing factor to these data challenges for regulators, it must nonetheless be acknowledged that the market itself is still teething its way through some of these data challenges. Accordingly, the explanatory guidance to Recommendation 9 has been supplemented to note that IOSCO and its members intends to (1) conduct work amongst its members going forward to promote the development of data standards that could help to improve the availability, and improved access to better and more homogenized international data sets, and alongside this (2) encourages its members to develop appropriate solutions within their jurisdictions to help further these objectives.

6. Chapter 6 – Recommendation on Cross-Border Co-operation

Recommendation 11 (Enhanced Regulatory Co-operation): 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 co-operation 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.

Concepts and Mechanisms for International Co-operation

Comments overwhelmingly agree that international co-operation is critical to the goals of cross-border co-operation.

The various concepts in approaching international co-operation include comments referencing a harmonized regulatory approach, others to global or cross-border alignment, equivalence regimes, substituted compliance regimes, passporting, notification requirements, and still others, a focus on regulatory outcomes.

A number of responses urge focusing on, leveraging, and using the full power of, the mechanisms of international co-operation, including the IOSCO MMoU and EMMoU, as well as the other mechanism set forth in the consultation report, such as bilateral or multilateral co-operation arrangements, supervisory colleges or other networks.

One comment noted that the MMoU and EMMoU are limited because they are too sector-specific as they relate to activities in the securities sector, but not to the enforcement of off-chain transactions. However, the majority of respondents see the IOSCO MmoU and EMMoU as key facilitating mechanisms for advancing international co-operation.

Data Sharing for International Co-operation

Some comments requested clarification as to the nature of the information to be shared.

Some comments noted that impediments to data collection such as different jurisdictions having different data protection standards could affect cross-border co-operation.

Some comments were concerned about data confidentiality and would like to see data sharing for international co-operation be limited solely to regulatory ends, while another comment believed that data should be shared as necessary to maintain fair orderly and transparent markets and that authorities should have access to relevant data for supervisory and regulatory purposes wherever the data is located.

On balance, respondents recommended targeted approaches regarding data sharing for international co-operation purposes, with regulators working to identify the data that is the most meaningful from a supervisory perspective, take an incremental approach to avoid the risks of data overcollection, and collect and process data that is needed for defined purposes and that the various information sharing mechanisms set forth in the consultation report could be used to share data as needed.

IOSCO's response:

The Recommendations promote international co-operation.

IOSCO agrees with the benefits of international co-operation as many of the respondents have set forth. The need for international co-operation is immediate. The IOSCO Recommendations promote international co-operation and provide jurisdictions with a broad range of mechanisms by which international co-operation can be achieved. Acknowledging the importance of homogenizing data standards, additional supplementary text has been included under Recommendation 9.

7. Chapter 7 – Recommendation on Client money and assets

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.

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.

Recommendation 14 (Disclosure of Custody and Safekeeping Arrangements): Regulators should require a CASP to disclose, as relevant, in clear, concise and non-technical language to clients:

1. How Client Assets are held, and the arrangements for safeguarding these assets and/or their private keys;
2. the use (if any) of an independent custodian, sub-custodian or related party custodian;
3. 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;
4. Risks arising from the CASP's handling or moving of Client Assets, whether directly or indirectly, such as through a cross-chain bridge; and

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.

Recommendation 15 (Client Asset Reconciliation and Independent Assurance): 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.

Recommendation 16 (Securing client money and assets): Regulators should require a CASP to adopt appropriate systems, policies and procedures to mitigate the risk of loss, theft or inaccessibility of Client Assets.

Minimum requirements and risk management

Respondents generally agreed that the recommendations provide adequate protection of customer crypto-assets held in custody by CASPs.

There was also consensus for the intended outcomes proposed in Chapter 7.

Respondents agreed with using traditional finance requirements as a starting point, but one industry association strongly felt that new custody laws were required due to the profound differences between traditional finance asset holdings and the holding of private keys. Although the response did not offer specific policy recommendations or solutions.

Respondents sought clarification on the proportion of crypto-assets which could be held in hot/warm/cold wallets.

Several respondents commented that CASPs should be required to disclose their proof of reserves/liabilities to clients (in a manner which could be independently verified) on a periodic basis. As part of the process/procedures, CASPs should include robust risk management tools, particularly for credit and liquidity risks.

Several respondents felt that legal separation of client assets and proprietary assets should be mandatory, however others felt this suggestion would be impractical, especially in instances such as when the mixing of assets arises from a collection of fees or is beneficial for technological execution efficiencies.

A number of respondents referred to MICA as a benchmark for defining minimum requirements and highlighted specific provisions which could be incorporated, for instance, Articles 70 ('Safekeeping of clients' crypto-assets and funds) and 75 ('Providing custody and administration of crypto-assets on behalf of clients').

Respondents emphasized their desire that recommendations remain technologically neutral.

An industry association sought acknowledgment CASPs already subject to custody regulation would not have additional requirements imposed on them. There was a split between respondents who felt that IOSCO should keep their recommendations principle based to allow for new technology to come into scope as developments happen, and respondents who sought to have specific recommendations included.

A traditional finance entity suggested that the term 'custodian' be clearly defined in the recommendations as there is a variation of understanding of this term outside of traditional finance. They felt a clear definition would ensure that requirements are drafted and applied as consistently as possible.

An industry association requested that the recommendations outline specific prudential, governance and operational resilience requirements, and insolvency policies to strengthen the resilience of custodial activity and protect investors.

IOSCO's response:

We welcome the strong agreement from the respondents with Recommendations 13 (Segregation and Handling of Client Monies and Assets) and 15 (Client Asset Reconciliation and Independent Assurance).

The responses have highlighted some challenges, for example, lack of skilled providers for audits, but note that the industry is continually developing and maturing and should overcome these challenges.

In relation to limits placed on hot/warm/cold wallets, we note the feedback received and consider that any limits should be within the remit of regulators within the relevant jurisdictions. We do consider that customers should be aware of the respective risks of the different types of wallets and choose the right service for them.

8. Chapter 8 – Recommendation to Address Operational and Technological Risks

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.

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.

Additional or unique technology/cyber/operational risks

The additional and unique risks mentioned are mostly technological and cybersecurity risks that are native to crypto-assets and their underlying technology, which include the use of DLT and smart contracts, forks in the protocol, storage and safekeeping of the crypto-asset, as well as cross-chain bridges.

Disclosure of risks

Several respondents commented on what should be disclosed, mainly information related to crypto-asset trading decisions, as well as technical, cyber and operational risks.

Others pointed to the disclosure of the CASPs' risk management framework, the results of risk assessments, and the results of external audits

Some respondents pointed to the need for investor education, taking into account that a certain level of knowledge is required to understand the information disclosed.

Some respondents mentioned methods of communication with retail investors, with the majority calling for transparent and clear disclosure in non-technical language.

IOSCO's response:

It is not proposed to make any changes to Recommendation 17.

9. Chapter 9 – Recommendation for Retail Distribution

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, or work with other relevant authorities to require, that all promotions and marketing of crypto-assets to retail clients accurately and sufficiently disclose the product and service provided as well as the associated risks in a manner that is fair, clear, and not misleading.

Regulators should require a CASP to implement adequate systems, policies and procedures, including for providing disclosures in relation to onboarding new clients, and as part of its ongoing services to existing clients. This should include assessing the appropriateness and/or suitability of particular crypto-asset products and services offered to each retail client.

Having clear disclosure requirements

Respondents generally supported Recommendation 18 and agreed that IOSCO's Standards and regulatory measures used in the financial markets broadly continued to be relevant to the context of CASPs and crypto-asset activities.

Many respondents highlighted that a key regulatory measure would be disclosure requirements by CASPs to ensure that retail clients have clear and accurate information to make informed decisions.

On requiring CASPs to assess the appropriateness and/or suitability of crypto-assets products and services offered to each retail customer, several respondents were of the view that such requirements were not necessary and that customers (retail or otherwise) should be given access to crypto-asset products and services.

Not banning or prohibiting advertisements/promotions

Respondents were against the outright prohibition of advertising or endorsements of crypto-asset but agreed that regulatory safeguards were needed given widespread instances of consumer harm.

The safeguards should be in line with current safeguards that were applicable to traditional financial services on a "same activity, same risk, same regulation/regulatory outcome" basis.

The guidance note would be enhanced to include the additional regulatory safeguards suggested in the feedback.

Several respondents have made reference to the need for greater accountability by parties other than CASPs (such as social media personalities and "finfluencers").

IOSCO's response:

Additional text has been added to Recommendation 18 setting out that regulators should require, or work with other relevant authorities to require, that all promotions of crypto-assets to retail clients accurately and sufficiently disclose the product and service provided as well as the associated risks in a manner that is fair, clear, not misleading.

Additional guidance has been included under Recommendation 18 setting out that CASPs should also disclose any commercial arrangements with (legal or natural) persons providing investment advice on crypto-assets admitted to trading on their platform or in which they have a material interest. This extends to any individuals who may be commissioned to recommend investment in particular crypto-assets on media (including social media). In some jurisdictions, the investment advice frameworks apply to recommendations made by service providers including so-called 'finfluencers' and other intermediaries.

Additional detail by way of a footnote has been included in the guidance to Recommendation 8 to identify expectations on CASPs to monitor media (including social media) for manipulative practices (i.e., information sharing on prospective listings on telegram, signal, etc.). Feedback suggested that the guidance could also call on regulatory authorities to build appropriate expertise and consider conducting social media monitoring.

Guidance has been incorporated setting out that Regulators should require CASPs to have an efficient and effective mechanism to address client complaints. Regulators should also take steps to tackle the risks posed to retail investors by the prevalence of poor marketing practices. This should be done directly where IOSCO members have the mandate or in coordination with other domestic regulators who are responsible for issues related to media and advertising (such as advertising standard setting and consumer watchdogs).

10. Box Text Commentary on Stablecoins

Stablecoins' different use cases as a store of value, medium of exchange or bridge

Referring to the potential use case of stablecoins as a medium of exchange and taking note of FSB publications, certain respondents suggested that Stablecoins are more suited to prescriptive prudential regulations and IOSCO principles, unless binding, may open the way to regulatory arbitrage.

Certain respondents, especially Blockchain Industry Associations, advocated for self-regulation or a bespoke regulatory regime, suggesting that the recommendations are burdensome on issuers or the CASP.

Some respondents provided specific modifications to the framework proposed in the consultation paper. These range from adjustments to the definition of a stablecoin, clarification on interaction with other frameworks (notably FSB Recommendations and European Markets in Crypto-Assets Regulation or "MICA"), additional clarification on custody arrangements and counterparty risks, to enhancing reporting requirements.

Some respondents also suggested considering the risk profile of the asset and related activity to calibrate regulatory requirements and distinguish stablecoins from other non-referenced assets.

Quite a few commenters invited IOSCO and its members to continue collaborating in this area as use cases emerge and to coordinate efforts with prudential authorities, central banks, and other relevant entities in each jurisdiction.

IOSCO's response:

The Recommendations apply to all crypto-assets including so-called stablecoins in seeking to deliver regulatory outcomes of investor protection and market integrity. The unique characteristics and idiosyncratic considerations presented by stablecoins are sufficiently addressed in the proposals and these have been maintained without amendment.

Annex C – Overview of Stablecoins, their Roles and Uses in Crypto-Asset Markets

What is a Stablecoin?

As defined by the FSB[36], a stablecoin is "a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets".

Stablecoins represent a large portion of the total market value for crypto-assets, and as a result there is a renewed focus on stablecoin arrangements. While stablecoin arrangements seek to achieve a particular characteristic (i.e., a stable value, in most cases tied to a fiat currency (e.g., the U.S. Dollar)), they are not technologically different from other types of crypto-assets. Stablecoins generally purport to be pegged or linked to one or more assets, in many cases fiat currency ("reference assets").

Despite claims by some stablecoin[37] issuers that the arrangements are "backed" or "collateralized" by reserve assets, it should be noted that several currently traded stablecoins are not in fact fully "backed" or "collateralized" by reserve assets. Therefore, stablecoin holders may not be entitled to any redemption right (at face value or otherwise) from the issuer of the stablecoin.

Stablecoin arrangements can take many forms and can reference one or more of the following asset types, or a combination of these asset types:

- Fiat currencies: stablecoins can reference one or more fiat currencies. The fiat currencies, or assets with equivalent fair value, may or may not be safeguarded by a custodian.
- Other real-world assets: stablecoins can reference other real-world assets, for example, securities, commodities, derivatives, real-estate, and/or other financial instruments and assets.

Finally, some stablecoins can also be pegged to and backed by other crypto-assets and/or market themselves as algorithmically controlled. An algorithmically controlled stablecoin is one that typically uses an algorithm to maintain price stability relative to the identified reference

36 See FSB, High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final report, Final Report, July 17 2023.

37 Generally, the issuer of a stablecoin is the entity responsible for designing the stablecoin, and managing the minting, issuance, redemption and supply of tokens. The stablecoin issuer also may manage the reserve assets. The trading price, and therefore maintenance of the peg, occurs with respect to fiat-based stablecoins through trading activities and the ability of certain market participants to acquire newly minted stablecoins in exchange for fiat currency and to put stablecoins to issuers for redemption. Algorithmically controlled stablecoins use a different mechanism to maintain the peg.

asset by adjusting the supply of tokens as needed. These types of arrangements are not covered in this Annex.

Uses of Stablecoins

Stablecoins are predominantly used to facilitate trading, lending and borrowing of crypto-assets, and are used as a perceived stable leg of a crypto-asset trading pair and as collateral in lending and borrowing arrangements, both on crypto-asset platforms and in DeFi applications and protocols. As such, stablecoins can play an important role in a CASP's operations.

Some have said that stablecoins may have the potential to be used for payments, outside of trading, lending and borrowing activities. At the same time, stablecoins may constitute a financial instrument. Issues involving stablecoins have been considered by a number of global organizations and standard setting bodies, including the FSB, IOSCO and CPMI-IOSCO because of the potential systemic impact they could have if used globally as a means of payment in commerce and because of their potential impact on investors and markets.

Risks of Stablecoins

Risks presented by crypto-assets are also relevant to stablecoins. In particular, there are risks addressed by these Recommendations, such as conflicts of interest, abusive behaviors, lack of operational resilience, information asymmetry, poor governance, lack of financial resilience and increased concentration risk.

However, stablecoins also present specific risks that differ from other crypto-assets due to their purported "stability" in relation to reference assets. These risks include those that flow from a lack of transparency, lack of verification of underlying reserve assets and potential for a "bank run" on the stablecoin.[38]

Reserve Assets

There are risks that the reserve assets supporting a stablecoin might either be insufficient, or unavailable, to fund redemption requests, either when the issuer is a going concern, or when it is insolvent. The particular risks relating to reserve assets is enhanced in stablecoin arrangements in which the reserve assets are not held in a segregated manner and investors and

[38] Recent studies suggest that stablecoins are vulnerable to runs in times of stress, in a similar way to money market funds.

other holders of stablecoins do not have a direct right of redemption from the issuer from dedicated and segregated reserve assets. The credit risk of the issuer in this scenario, which is the most common currently is significant given the lack of segregation of reserve assets from other creditors of the stablecoin issuer. The particular risks relating to the sufficiency and/or viability of the reserve assets themselves could arise as a result of mismanagement of the reserve assets by the stablecoin issuer or due to market conditions. Even where the reserve assets are segregated, liquidity is a key risk in relation to the reserve assets as the reserve assets must be sufficiently liquid to enable issuers to use the reserve to fund redemption requests. A failure to fund such requests or loss of confidence could result in a "run" on the stablecoin. If the stablecoin issuer becomes insolvent, even stablecoin holders that have a direct right of redemption from an issuer may not be able to redeem their stablecoins, thus facing loss of their entire value. Stablecoin holders are subject to the credit risk of the stablecoin issuer if the reserve assets are not segregated and held for the crypto-asset holders in a way that protects the assets from other creditors of the stablecoin issuer. In this case, there may be no legal claim by the stablecoin holder as against the issuer or reserve.

Reserve assets of a financial nature, including deposits with banks or assets held with custodians, create an interdependence channel with traditional finance. This poses two-way risks – a run on a stablecoin may threaten the viability of an institution that holds the reserve assets as, for example, deposits. Similarly, the failure of a bank or custodian will mean that those reserve issues may become either illiquid or diminished for a period – and there is a risk of destabilizing the stablecoin, the stablecoin issuer and the wider crypto-asset market.

Rights of Holders

The use of stablecoins is dependent upon a holder having a direct right against the stablecoin issuer to obtain the fiat value of the stablecoin. However, many issuers of stablecoins place restrictions on the types of persons that can request redemptions or place a minimum value for redemptions. In many stablecoin structures, the stablecoin issuer will allow only larger institutions and crypto-asset trading platforms to interact directly with the stablecoin issuer to create and to redeem stablecoins. Other persons interested in holding stablecoins must acquire them in trading or similar activities from these third parties and may only look to these third parties, including crypto-asset trading platforms for repurchase or redemption of the stablecoins. As a result, stablecoin holders are subject to counterparty risk of the crypto-asset trading platforms in order to redeem their stablecoins. The rights of holders may not be clearly

disclosed, whether by the issuer of the stablecoin or other parties, and holders of stablecoins do not have any rights relating to the operation of the stablecoin arrangement.

The majority of stablecoin distributions and trading occurs on secondary markets through CASPs and clients may not be aware of what rights they have and do not have against a stablecoin issuer. Further, a holder of a stablecoin may not understand that they are dependent on the continued viability and desire of CASPs to purchase stablecoins from them in order for them to sell or otherwise dispose of their stablecoin. Related to this issue is the fact that the pricing and, therefore, value of the stablecoin in the hands of the stablecoin holder is determined by secondary market trading and market sentiment. For example, the secondary market price of a stablecoin can "de-peg" due to market conditions, including sentiment, even if the issuer is fulfilling redemptions of certain market participants at par.

Money Laundering/Fraud/Scams

As with other crypto-assets, stablecoins may appeal to money launderers and criminals who do not wish to subject the proceeds of crime to traditional financial system oversight. Stablecoins are also likely to be perceived as more stable than other crypto-assets, so are more attractive to money launderers and criminals who do not wish to be as exposed to crypto-asset market volatility.

In light of the price instability of crypto-assets, because of their relatively more stable nature scammers have turned to stablecoins and are soliciting stablecoins from their victims.