3 June 2022

Alp Eroglu
International Organization of Securities Commissions (IOSCO)
Calle Oquendo 12
28006 Madrid
Spain

By email: consultation-03-2022@iosco.org

CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

Dear Mr Eroglu,

Submission on the Retail Market Conduct Task Force Consultation Report

CPA Australia is a professional accounting organisation representing the diverse interests of more than 170,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

While we consider the increased involvement of retail investors in financial markets as positive, we highlight potential societal risks, as well as investor risks, stemming from the limited financial literacy of many retail investors, unregulated new asset classes such as crypto assets and unlicensed 'finfluencers' providing investment advice on social media platforms.

Our key recommendations are:

- Provide education material and stronger investor protection measures targeted at minors investing in crypto assets.
- Include crypto gaming in the important retail trends to be monitored and assessed by IOSCO and regulators.
- Urge regulators to understand stablecoins, monitor their development and develop regulatory requirements/safeguards.
- Consider regulating gamification investing such as crypto games such that they are available only to individuals of legal age.
- Clarify the regulatory treatment of crypto gaming tokens.
- Develop harmonised reporting and disclosure standards for crypto assets applicable across jurisdictions.
- Initiate targeted international initiatives involving regulators across jurisdictions to narrow data gaps related to crypto assets.
- Consider including finfluencers in the scope of financial services legislation and provide stronger regulatory oversight of social media channels providing platforms to finfluencers.
- Issue (automated) warnings and educational material to protect retail investors and enhance their financial literacy.
- Encourage regulators to build an online presence on social media platforms.
- Consider identity theft as a fraud type and encourage crypto asset service providers to implement more robust identity verification methods.
- Consider introducing product intervention powers for the crypto asset market.

Responses to the Issues Paper questions are included in the Attachment.

If you have any questions about this submission, please do not hesitate to contact Dr Jana Schmitz, Digital Economy Policy Lead at jana.schmitz@cpaaustralia.com.au.

Yours faithfully

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy
Encl.

Attachment

Q1: In their risk analysis, should regulators specifically consider/target specific demographic profiles/groups for additional or enhanced investor protection measures? If so, should greater attention be focused on younger age groups or older age groups? Is there a tipping point in behaviors beyond which regulators should become concerned?

In our view, the same investor protection measures should apply across different groups of investors. However, we note that certain demographic groups, such as underaged investors, are exposed to significant risks they may not understand. Apart from investor protection measures, regulators should consider investor education as a key responsibility for them. Investor education should be tailored to different demographics. Regulators must put additional effort and resources into educating and protecting minors.

Considering the aggressive promotion of crypto assets to the public, including through social media, and the growing number of underaged crypto retail investors, regulators should do more to educate investors about this new investment class and warn them that many crypto assets are highly risky and speculative. Regulators should alert retail crypto investors, particularly minors, to the fact that they:

- face the very real possibility of losing all their invested money if they buy these assets;
- should be alert to the risks of misleading advertisements, including via social media and finfluencers; and
- should be particularly wary of promised fast or high returns, especially those that look too good to be true.

See also our responses to **Q2** and **Q3**.

Recommendation 1:

Provide education material and stronger investor protection measures targeted at minors investing in crypto assets.

Q2: Does the consultation report capture accurately the important retail trends and the reasons for increased retail trading? Are there any missing concerns or issues and other potential risk magnifiers? What may be the current and potential long-term implications of increased retail participation in markets in your view?

Overall, we consider growing retail participation in financial markets as positive. However, we note that this development may come with increased societal risks (e.g., inexperienced investors losing their life savings). Whilst the increased retail investor participation does not necessarily pose a systemic risk to the stability of the financial system, it could lead to deeper societal issues and impact the broader community's trust in markets and regulators in the event of a major event such as the collapse of a popular crypto currency.

Further, we note that crypto gaming is not mentioned in the issues paper although it is widely considered as one of the main retail investor trends. "Play-to-earn" crypto games blend entertainment with financial speculation. Amid the hype around non-fungible tokens (NFTs) and the metaverse, these games attract millions of players and billions of US dollars from investors who see the games as a way to introduce more people to cryptocurrency and other crypto asset classes.

Players can use crypto gaming tokens to earn rewards by winning games and creating new tokens. Gaming tokens can be traded with other players on the platform and sold via centralised and decentralised cryptocurrency exchanges. We understand that most crypto gaming platforms are not regulated by securities regulators and are not compliant with AML/CTF and age verification requirements (see also our comment on **Q3**).

Adding layers of complexity, unofficial financial networks have emerged around these games as some players leverage their in-game possessions for further gains: players form gaming groups often referred to as "guilds", allowing other players who want to play for free, without investing in crypto assets, to use the guild's NFTs to play in exchange for a percentage of the gains/rewards.

Given the market capitalisation of major crypto gaming tokens, we urge the IOSCO to monitor this growing unregulated market segment. We understand that southeast Asian countries such as Thailand and Philippines have emerged as some of the fastest growing crypto gaming hubs.

Recommendation 2:

Include crypto gaming in the important retail trends to be monitored and assessed by IOSCO and securities regulators.

Noting that the issues paper refers to stablecoins, in light of the latest collapse of LUNA and terraUSD, we emphasise the need for regulators to address the ongoing development of stablecoins, with particular focus on algorithmic stablecoins. The stability of a stablecoin's peg to its reference value is a central issue. While a range of stablecoin-related issues may be resolved with appropriate institutional safeguards, regulations, and technical advancements, sustained growth in stablecoins in circulation would ultimately impact the traditional financial system in significant ways that are important to understand.

Recommendation 3:

Urge regulators to understand stablecoins, monitor their development and develop regulatory requirements/safeguards.

Q3: What may be the potential implications of self-directed trading and gamification from a retail risk and conduct perspective? Should high risk aspects of these activities be regulated or prohibited, for example, certain risky gamification techniques?

As indicted in our response to **Q2**, crypto games are being accessed by minors. In our view, nobody under the age of 18 should be able to gamble or speculate. Our views are aligned with relevant financial services legislation in most jurisdictions.

We note that most major centralised cryptocurrency exchanges comply with KYC requirements to ensure that users are 18 or older. However, several decentralised platforms remain unregulated and do not meet KYC requirements.

We understand that several platforms allow children to buy crypto assets, e.g., NFTs, via crypto wallets, which underage children can create with parental permission. However, we believe that parents may often be unaware that certain crypto games contain opportunities to gamble. Consequently, minors are presented with an opportunity to buy, gamble and sell crypto assets. Crypto gaming may lead to more normalised gambling attitudes among minors, potentially resulting in gambling and mental health issues.

Further, scams and fake platforms expose minors to additional risks. Online scammers intentionally seek out inexperienced crypto investors and gamers to exploit them. Data breaches, identity theft or fraud can be accomplished in the minor's name without his/her knowledge (see also our response to **Q7**). Moreover, minors may also be more likely to lose their private keys.

In addition to concerns around cryptocurrency, blockchain technology may also pose unintended consequences for minors. For instance, blockchain could be harmful to children because information recorded is permanent and immutable, and this immutability could conflict with current regulations such as Article 17 ('right to be forgotten') of the General Data Protection Regulation (GDPR).

To protect young people, education, awareness and policy changes are required. Regulators need to better inform consumers through transparency and prevention programs. Gambling-related problems must be prevented through improved parental controls, age verification in the digital age and games such as crypto casinos being regulated such that they are available only to individuals of legal age.

We understand that the issues raised above cut across many regulatory areas including securities regulation, consumer regulation, gaming regulation, criminal law and privacy regulation. However, the potential societal and market impacts are such that improved securities regulation of gamification investing needs consideration.

Recommendation 4:

Consider regulating gamification investing such as crypto games such that they are available only to individuals of legal age.

With respect to the regulatory treatment of crypto games, we note that gaming tokens often have a dual function as they allow the owner/investor to 'use' the token for gaming purposes while earning financial rewards. The regulatory treatment of a crypto asset depends on the way in which it is classified. A key question is whether gaming tokens are considered as financial products, in which case they should be captured by financial services regulation. If gaming tokens are utility tokens, which could be considered consumer products, they should be overseen and regulated by relevant consumer protection authorities. If they can be classified as both financial products and utility tokens, we strongly suggest greater cooperation, coordination and information sharing between securities regulators and consumer protection authorities.

Recommendation 5:

Clarify the regulatory treatment of crypto gaming tokens.

Q4: How should regulators consider whether to monitor crypto-asset trading by retail investors? Are there ways that the apparent data gaps with regard to retail investor crypto-asset trading could be filled or other protections for retail investors or ways in which regulators could begin to monitor crypto-asset trading? Are different approaches likely to be more or less effective in jurisdictions with different regulatory, statistical and other governmental and private sector approaches to data gathering?

In light of the potential increasing interconnectedness between traditional financial markets and the crypto asset market, we urge regulators to monitor retail investors' trading of and investing in crypto asset.

If crypto asset investment activities are left unmonitored, larger data gaps will emerge, which risk undermining the ability of regulators to oversee and regulate crypto assets holistically. The systematic collection and publication of crypto asset data must be enhanced and undertaken in a more rigorous and robust manner. This requires harmonised standards deployed across jurisdictions.[1]

Recommendation 6:

Develop harmonised reporting and disclosure standards for crypto assets applicable across jurisdictions.

[1] In CPA Australia's submission to the Australian Treasury on Crypto asset secondary service providers: Licensing and custody requirements we note that differing regulation, supervision, and compliance across markets creates opportunities for arbitrage and raises risks to the stability of financial markets, and the protection of consumers, investors and businesses.

Further, important international initiatives to close the crypto data gaps should include, but not be limited to:

- Developing and regularly reviewing/updating the standardised definition of crypto asset service providers / virtual asset service providers used across jurisdictions.[2]
- Identifying and defining data gaps and data needs such as:
    - the number and value of transactions processed via centralised exchanges.
    - the value of crypto assets held by and/or staked on decentralised exchanges.
    - the value of crypto assets held by crypto wallets and other custodial services.
    - data on the level of interconnectedness of crypto asset service providers with the traditional financial system (e.g., characteristics and size of financial services provided by crypto asset service providers, funding received by crypto asset service providers from traditional financial services providers)
- Establishing a global registry of crypto asset service providers using information available in the public domain and request information from private institutions specialising in the crypto economy, such as Chainalysis.
- Requesting and collecting relevant data from public and private institutions (e.g., tax authorities that collect data from centralised exchanges, crypto insurance providers).
- Using innovative procedures and methods to collect and capture data (web-scraping, artificial intelligence and/or data analytics techniques).
- Sharing data and information across authorities (nationally), and across jurisdictions (internationally; including tax information exchange agreements/statements).

Recommendation 7:

Initiate targeted international initiatives involving regulators across jurisdictions to narrow data gaps related to crypto assets.

It is important to note that data collection initiatives for the purpose of data gaps minimisation need to strike the right balance between the usefulness of the data and the burden imposed on the data collector/ reporting agents.

Even as the availability of data improves, some indicators may be harder to monitor than in the traditional financial sector, underscoring the continued importance of gathering intelligence from market participants to supplement these indicators. Further, as crypto assets and decentralised finance (DeFi) continue to evolve rapidly, the data that are needed to adequately monitor them will change.

Q5: How should regulators approach these trends (e.g., both trading for crypto-assets or brokerages using hidden revenue raising mechanisms) and when should they seek to intervene?

No comment.

[2] For instance, the Financial Action Task Force's (FATF) definition of Virtual Asset Service Provider (VASP) is used in Hong Kong and Singapore. The Australian Treasury has proposed a different term, Crypto Asset Secondary Service Providers (CASSPrs), which is aligned with the content of the FATF's definition, although named differently. As different terms used in different jurisdictions may be confusing, this example demonstrates the need to develop a standardised definition of crypto asset service providers used across jurisdictions. See also CPA Australia's submission to the Australian Treasury on crypto asset secondary service providers.

Q6: Should regulators proactively monitor social media and online statements for retail investor protection and if so, when and how? Should social media be subject to additional regulatory obligations regarding securities trading and/or crypto-asset trading? How could such monitoring be implemented, and obligations enforced proportionate to the harm/potential harm? Are there any legal (e.g., data protection) or technical obstacles? What sort of risk assessment should regulators do to determine where to allocate their resources?

Surveys show that a third of young investors rely on social media for investment advice.[3] One major concern is that retail investors will be particularly vulnerable to exploitation both by fraudsters and finfluencers on social media, because of their lack of financial literacy. The anonymity of certain social media platforms also increases the potential for misinformation and manipulation. Aggressive promotion of crypto assets on social media fuels this concern.

We note that market participants have recognised the growing importance of retail investors and are developing new strategies for engagement, including the use of social media. In our view, retail investors will continue to rely on non-traditional sources of investment information, particularly social media posts, to inform their investing decisions. Therefore, regulators must continue to pay attention to the use of social media platforms, not only to enhance investor protections but also to secure market integrity and stability.

As suggested in our response to **Q4**, regulators could deploy innovative techniques such as web-scraping, artificial intelligence and data analytics tools to identify and collect relevant data from social media platforms. This data could be used to identify finfluencers who illegitimately provide financial advice.

Further, we believe that finfluencers should be included in the scope of financial services legislations (i.e., financial services licencing regimes) to ensure that their followers are not misled regarding their advice credentials, and to provide a level playing field vis-à-vis regulated financial advisers. To increase transparency, finfluencers should be required to disclose their sources of income (e.g., sponsorship agreements with cryptocurrency exchange) as well as amounts paid to them in exchange for promoting certain (regulated and unregulated) financial products. Volume-based payments should be discouraged, if not banned outright.

Social media channels providing a platform to finfluencers and retail investors should also be subject to stronger regulatory oversight. Ideally, where an entity providing financial advice is required to be licensed (or regulated in such a way) in a particular jurisdiction, they should be licensed and details of that licence, together with the jurisdiction, should be required to be disclosed.

Recommendation 8:

Consider including finfluencers in the scope of financial services legislation and provide stronger regulatory oversight of social media channels providing platforms to finfluencers.

Regulators should require social media platforms to provide financial education tools to retail investors.

As many retail investors using social media platforms may not be financially literate, we recommend that platforms must issue warnings and provide investors with access to educational material. Certain social media posts identified by artificially intelligent bots should automatically trigger such warnings and provide educational material in an easy-to-understand manner.

Just-in-time education could encourage investors to reconsider risky or unusual investment decisions with a pop-up asking something like "are you sufficiently informed about the financial product?" An investor who indicated uncertainty could then be directed to a source of additional financial education. To make them more appealing to retail investors, such pop-ups could use features including bright colours, confetti, easy-to-use designs to reward retail investors for accessing educational material or demonstrating their understanding of financial concepts.

Recommendation 9:

[3] Emily Graffeo (2021): A third of young traders go to social media for investment advice — and 12 per cent say they invest because it 'feels like a game', Markets Insider, available at: https://markets.businessinsider.com/news/stocks/retail-investing-trends-robinhood-gamification-survey-social-media-trading-2021-8 (accessed on 31 May 2022).

Issue (automated) warnings and educational material to protect retail investors and enhance their financial literacy.

Moreover, in an increasingly digital online environment, regulators should consider building a social media presence to demonstrate their oversight powers and signal to social media users that they are paying attention.

This does not necessarily mean that regulators should interfere online and/or interact directly with social media users. However, their social media presence could help them to monitor ongoing developments, to play a role in educating investors about how to determine the reliability of posts, and even to flag posts that are particularly suspect.

In a borderless online world, social media presence of regulators could help them facilitate greater collaboration with regulators in other jurisdictions, and to collectively confront the challenges presented by social media platforms.

Recommendation 10:

Encourage regulators to build an online presence on social media platforms.

Another challenge is around data governance. Social media platforms seem to collect as much personal data on their users as possible. When big data are parsed with advanced technologies like artificial intelligence, they can predict user actions in ways that users may not grasp. Social media platforms may even exploit behavioural biases to manipulate retail investors' preferences. Whilst several government inquiries have been conducted at global scale, data protection authorities must continue monitoring and addressing such emerging risks and challenges.

Q7: Are the main fraud types covered correctly (e.g., crypto-asset scams, boiler room scams, clone investment firms, and misleading information and promotional material)? What are the fraud patterns that cause/have potential to cause most retail investor harm? Are there other types of frauds or scams that regulators should consider?

In our view, the IOSCO has covered the most relevant and severe fraud types. One fraud type we suggest should be considered is identity theft. Fraudsters have exploited weaknesses in the security of crypto exchanges by creating new accounts using fake identities and using stolen identities to take over existing accounts and empty digital crypto wallets. Regulators must encourage crypto asset service providers to embrace more robust identity verification methods to check the identity of their users and safeguard their assets.

Recommendation 11:

Consider identity theft as a fraud type and encourage crypto asset service providers to implement more robust identity verification methods.

Q8: How has COVID-19 impacted retail conduct and frauds? How should regulators best respond to fraud and misconduct in the current environment, also in consideration of the impact of COVID19 on retail market conduct?

See our responses to previous questions.

Q9: Does the Consultation Report capture well the existing cross-border challenges? Are there any missing concerns or issues that are not highlighted? Are there any other novel ways of addressing cross-border challenges affecting retail investors? As an international body, what could be IOSCO's role in addressing the cross-border challenges highlighted in this consultation report?

See our responses to previous questions.

Q10: What may be the concerns or issues that regulators should ask for disclosure of (at both firm and product level), keeping in mind the balance between quantity of disclosure and the ability of retail investors to absorb such disclosure? Should markets continue to seek to put in place special arrangements that could encourage companies during stressed market events to provide disclosures and updates that help retail investors better evaluate current and expected impacts of such events? If so, what may be the practical options to achieve this, including who should provide this information? Are there specific technological measures or non-technological measures (e.g., changing the timing, presentation of the information) you would suggest to enhance the ability of retail investors to process the disclosure?

An ongoing challenge with disclosure-based regulation is that, even if regulations mandate disclosures many retail investors are unlikely to read them.

As we suggest in our response to **Q6**, social media platforms could provide questions or tools that require retail investors to demonstrate their familiarity with the disclosures and general understanding of certain types of financial products. However, we would consider that a useful model for disclosure should be at the very minimum – disclosure which can be equated to that which is presently required for financial products.

This does not necessarily need to be paper-based – we believe blockchain to be an ideal technology to house up-to date disclosure. However, the entity providing the asset should be the entity responsible for ensuring its accuracy at any given point in time. Disclosure should ensure that information such as fee and cost disclosure, product features and dispute resolution processes are available in a format that can be relied on to be current.

Additional disclosure measures could be considered in relation to duties on offerors or intermediaries to prevent consumers from investing in products not suitable to them. Several online stockbrokers, for example, screen their clients with an exam-style questionnaires, prior to allowing them to trade options. Such measures could be imposed on intermediaries prior to trade in riskier assets.

Q11: Where product intervention powers exist, what factors should regulators consider determining when it should be used and at what stage to ensure suitability and to mitigate investor harm? For example, should regulators monitor leverage levels in retail trading and/or seek the power to limit leverage? If so, is it possible to describe the kind of situation in which such powers could justifiably be used?

Product intervention powers should be developed for situations where products are mis-sold or defective.

In many jurisdictions, target market determinations are used to ensure that the details of for whom a product would be useful, are included in financial products. Product intervention powers can therefore be used in instances where products are sold outside designated target markets in ways that pose systemic risks to consumers.

The problem with several crypto assets lies with the nature of the assets themselves. In cases where financial products are mis-sold or are defective in some way, product intervention powers exist enabling regulators to recall products and order settlements. Assets on append-only databases such as blockchains are unable to have transactions reversed without costly and highly disruptive interventions, such as "forking" the code. One example of where this was utilised was in May 2016, where the Ethereum blockchain was forked to effectively reverse the hacking of a smart contract.

One solution may be to allow for regulators to order such forks to occur to provide restitution to consumers. Such a power must be properly evaluated to ensure that any damage to unaffected users of the same blockchain do not occur.

Present restrictions on leverage are in place in certain retail financial products, such as Contracts for Difference (CFDs) or margin lending products. We believe that consideration should be given to examining whether a rule of thumb can be developed to cover leverage across products – financial or otherwise.

Recommendation 12:

Consider introducing product intervention powers for the crypto asset market.

Q12: Are the developments in retail investor behavior sufficiently significant and persistent to justify reviews by regulators of their current approaches to retail investor protection? If so, is that true globally or only in some markets? If some, what are the characteristics of the markets for which that is most true?

Retail investor engagement in the capital markets should be an issue of ongoing concern for regulators across jurisdictions.

As pandemic-related restrictions are lifted globally and people return to workplaces and social interactions, the appeal of social media informed stock trading may fade, as will the liquidity provided by governments through pandemic stimulus payments. At the same time, however, the financial markets have experienced, amongst others, an increase in short-selling by retail investors informed by information obtained from social media platforms (Game Stop "frenzy"), increasing interconnectedness between traditional financial markets and novel markets such as the crypto asset environment. Time will tell whether changes in retail investor behaviour are sufficiently significant and persistent, however we see no indication of it slowing.

Q13: Are the above regulatory tools appropriate, proportionate, and effective? Are there other regulatory tools regulators might consider? What new technologies may help regulators as they continue to address misconduct and fraud (including online/via social media)?

See our responses to **Q4** and **Q6**.

Q14: Since the date of the IOSCO survey exercise in August 2021, have there been any other measurable changes in retail investor trends that should be taken into consideration?

Crypto gaming, as mentioned in our responses to **Q2** and **Q3**.