

11 December 2023

By email: crypto@treasury.gov.au

Director – Crypto Policy Unit
Financial System Division
The Treasury
Langton Crescent
Parks ACT 2600

Dear Director

Regulating Digital Asset Platforms

Thank you for inviting us to respond to Treasury's proposal paper *Regulating Digital Asset Platforms (Paper)*. Consumer Action welcomes the Government's intention to regulate the digital asset (**crypto**) market and acknowledges the significant step forward this entails.

Through our frontline services, we see widespread harm in the crypto market, and the urgent need for intervention. Regulating digital asset platforms (**DA Platforms**) as a financial service makes sense. However, we have concerns about whether the proposed obligations go far enough to protect consumers from bad actors and scammers. Regulating DA Platforms confers a high degree of legitimacy on the entire industry and we consider the Government has an obligation to ensure that when doing so, it also includes measures to adequately protect consumers from harm. Cryptocurrency carries significant and inherent risks. Over a million Australians currently hold cryptocurrency worth an estimated \$21.6 billion.¹ Info Box 12 in the Paper recognises that the cryptocurrency markets are rife with bad actors attempting to manipulate the market and dupe people into bad investments. The crypto markets are inherently volatile and opaque, and extremely difficult for the average consumer to understand. It is also internationally reported to be used to finance organised crime, human trafficking, and trade in illegal arms and narcotics.²

We query whether the Government's aim of protecting consumers and achieving legal consistency within the international community can be achieved by simply extending financial services laws to DA Platforms or regulating merely to prevent their collapse. Regulation in this area should be as broad as possible to ensure that bad actors are actively prevented from exploiting any loopholes or exemptions.

An important aspect of regulation must be strengthening obligations to prevent scam losses and including measures to address the high-risk nature of financial investment in crypto. We consider that broader regulation to capture more of the crypto sector is likely required.

The Treasury's consultation paper on the draft industry scams codes acknowledges that the current AFSL regime is insufficient to combat scams and proposes specific, stricter obligations for the banking sector. While the Government and banking industry are implementing important measures to protect consumers from scam losses,

¹ Research published by Roy Morgan 12 April 2022 [Over 1 million Australians now own Cryptocurrencies such as Bitcoin, Ethereum, Ripple, Cardano, Dogecoin and Shiba Inu - Roy Morgan Research](#)

² For example, the legal proceedings against Binance in the USA [Crypto giant "Binance admits to money laundering and agrees to pay \\$4.3bn" \(The Guardian\)](#)

progress has been slow, and vigilance is needed as scammers continually develop new ways of stealing money. Stronger safeguards are well overdue.

Reflecting the inherently high-risk nature of crypto and DA Platforms, and broad use and accessibility including to consumers with barriers to understanding the risks involved, the Government should look to make additional interventions. If the Government is not satisfied that consumer harms can be appropriately limited, we consider that DA Platforms should be prohibited from dealing with Australian retail investors.

In considering the how broad the regulatory framework should be we have applied three guiding principles in developing our response to the proposals. We strongly recommend that Treasury consider adopting the same set of principles:

- DA platforms and platforms are effectively safe for individuals and impossible for scammers to exploit
- Regulation is capable of being effectively enforced so that bad actors and market manipulators are held to account
- Consumers have effective affordance, fair and timely access to justice and redress

If any of the guiding principles cannot be implemented then greater intervention or outright prohibition may be required.

A summary of recommendations is available at **Appendix A**.

About Consumer Action

Consumer Action is an independent, not-for profit consumer organisation with deep expertise in consumer and consumer credit laws, policy and direct knowledge of people's experience of modern markets. We work for a just marketplace, where people have power and business plays fair. We make life easier for people experiencing vulnerability and disadvantage in Australia, through financial counselling, legal advice, legal representation, policy work and campaigns. Based in Melbourne, our direct services assist Victorians and our advocacy supports a just marketplace for all Australians.

Digital asset platforms are a haven for scammers

The Paper only makes passing reference to the use of DA Platforms for fraud and scams. Australians are losing billions of dollars to scams every year,³ and scams involving cryptocurrency are growing faster than other types of scams.⁴ Furthermore, banks also tell us that even if the scam itself does not involve crypto, DA Platforms are the fastest, easiest way for scammers to get stolen funds out of the country and beyond reach of authorities.

We are concerned that extending current Australian Financial Services License (AFSL) obligations to DA Platforms would approve a pathway for scams losses out of the country and fail to address how scammers are exploiting regulatory loopholes in Australia. Current legislative obligations do not adequately protect consumers from scammers, hence the need for major reform. Recent developments such as the Australian Banking Association's Scam-Safe Accord and the Government's proposed industry scams code are welcome steps towards a safer market, but the obligations will not be imposed on DA Platforms. The immediate outcome would be that DA Platforms are required to meet a much lower standard than the banking sector in preventing, disrupting and responding to scams. Given the significant proportion of scam losses occurring via crypto this amounts to very thin protections for consumers. While the Government has indicated that the scams code may eventually apply to digital currency exchanges, this would leave consumers exposed for a period of considerable time.

Financial institutions have been failing to invest and implement the technology needed on a large scale to protect Australian consumers from life-changing scams losses and this is not meeting community expectations. The recent ABA announcement indicated that the major banks and customer owned banks are collaborating through technology, including blocking certain crypto transfers, but the real test will be in how these measures ultimately protect consumers against scammers who are sophisticated and know how to exploit the loopholes. Consistent with the absence of meaningful legal obligations, the Australian Financial Complaints Authority has consistently issued determinations in favour of the banks, meaning there is currently little to no impetus on banks to do better by their customers. We do acknowledge however that there is a present opportunity to strengthen the regulatory framework through the development of new scams codes.

Many of the scams perpetrated against our clients are effectively facilitated by well-known crypto platforms. We consider that current anti-money laundering and counter terrorism financing requirements imposed on digital currency exchanges are not sufficient to prevent scams. Consumers have no visibility on whether a DA Platform is complying with AML/CTF obligations and no requirement to remediate customers arises due to non-compliance.

Case Study - Sam

Sam works as a rideshare driver and his partner is casually employed. They have school aged children.

Sam saw an advertisement on Facebook for a cryptocurrency trading website. He made contact with individuals representing the website, who helped him to open an account and start making trades.

To fund the trades, Sam borrowed money from family and friends, which he transferred to Coinbase. From Coinbase the funds were sent to the website immediately, totalling approximately \$22,000 over two months. Sam says that Coinbase raised no concerns about the transfers.

The website disappeared and Sam was unable to contact the people he had been previously dealing with. He contacted the National Debt Helpline in financial distress, unable to meet his mortgage repayments, and with friends and family expecting to be repaid.

³ ACCC Targeting Scams 2022

⁴ [National Anti-Scam Centre in Action Quarterly Report \(Q1 FY23-24\)](#) page 19.

Case Study - Danielle

Danielle is in her late 50s and lives in Queensland. She had no prior experience with cryptocurrency or complex financial products. In late 2022, Danielle wanted to learn about online trading and found a website that offered a course. The website provided her with software to download and run on her computer and told her to transfer money to a Binance wallet. She withdrew funds from her superannuation to her ordinary bank account, and then began transferring large amounts to Binance.

Her bank's fraud team called and asked some questions about the transfers. Danielle says that she told her bank she was going to trade cryptocurrency online and had never done so before but didn't understand the red flags that were being raised. The bank didn't explain why they were asking questions or indicate they thought she was being scammed.

Danielle says that the online scammers made it look like she was sending funds to her own wallet with one digit difference, so she didn't realise she was transferring huge amounts of money to a wallet she did not control.

Danielle lodged a complaint with AFCA about her bank but has only been offered \$10,000 in compensation for the \$150,000 she lost.

Danielle and Sam's stories demonstrates that online scammers are easily able to obtain and use crypto wallets to transfer stolen funds away from any chance of recovery, with little to no response from DA Platforms.

Danielle's case study demonstrates the harm that not banning bad actors causes. Every week our financial counsellors and lawyers receive calls about scams involving crypto. Regulating DA Platforms under the AFSL regime without introducing specific obligations to address scams would be a failure by Government to address a growing (and already significant) cause of consumer harm.

Licensing DA Platforms without strengthening consumer protections in the AFSL regime may leave consumers suffering scam losses worse off.

Government legitimisation and approval of DA Platforms may reduce the current and proposed responsibilities of banks to protect consumers. Consumers are already unlikely to secure any compensation from their bank. If their funds are transferred from a bank to a licensed DA Platform and subsequently lost to a scam, they would not benefit from the protections in the industry code or the Scams-Safe Accord.

A small number of Australian banks have blocked transfers to certain DA Platforms. If these platforms are granted an AFSL there will likely be pressure to allow these transactions to proceed without the level of friction and scrutiny necessary due to the high risk of scams.

RECOMMENDATION 1: Place an obligation on banks and DA Platforms to take steps to detect and prevent losses to scams. This should include:

- Mandating confirmation of payee for traditional accounts and digital wallets
- Stronger identity verification measures for individuals and business using or receiving payments via DA Platforms
- Immediate freezing of receiving accounts when a transaction is reported by customers, regulators or through the Australian Financial Crimes Exchange, or otherwise identified by the financial institution to be a scam loss
- Accessible and timely fraud reporting pathways for consumers

RECOMMENDATION 2: Place an obligation on banks and DA Platforms to reimburse consumers for scam losses, with any exceptions only in extremely unusual circumstances.

RECOMMENDATION 3: Require banks and DA Platforms to block transfers to unlicensed DA platforms. Where they fail to do so, there should be an obligation on the licensee to remediate any losses to the consumer.

RECOMMENDATION 4: Government should provide guidance to banks that regulation of cryptocurrency does not amount to any endorsement of its safety, and that banks should continue to take and expand upon a risk-based approach to blocking high risk transfers onto DA platforms, even where licensed.

Other general recommendations

Advertising restrictions

Our reading of the Paper suggests that licensing requirements would only apply to advice or promotion around using a DA Platform. It would not apply to promotion of digital tokens themselves unless they are otherwise considered to be a financial product or if specific reference to dealing with them via a DA Platform is made.

Consumer Action is concerned that opting not to regulate these activities would undermine the proposed framework's objective of protecting consumers. Digital assets are an inherently high-risk, complex product that consumers use as a financial investment. Misleading information is rife in this space and consumers are frequently misled by the promise of significant and safe returns on their spend. Accordingly, promotion should require similar risk warnings as high-risk financial products including contracts for difference.⁵ The proposed principles would allow non-DA Platform entities to continue advertising without any regulatory oversight.

Bringing advertising of digital assets within the AFSL regime would enable consumers to identify bad actors, provide recourse to internal and external dispute resolution, and enliven misleading and deceptive conduct and anti-hawking provisions in the *Corporations Act*. The Government should extend the proposed regulation to cover advertising of digital assets. A low intervention approach could be that advertising about any asset able to be purchased through a DA Platform requires a license and compliance with financial product promotion restrictions.

If the Government believes that regulation would not be effective in this regard, we submit that advertising digital assets in traditional media and online platforms should be prohibited.

RECOMMENDATION 5: Extend the licensing requirement to cover advertisements of digital tokens, and if unable to do so satisfactorily prohibit advertising altogether.

Additional safeguards and funding for ASIC

ASIC's regulatory portfolio has increased dramatically in the past ten years and is significant compared to equivalent regulators internationally. However, we note that ASIC has a comparatively small headcount amongst Australian regulators, and in 2021-22 was only approximately 200 greater than in 2011-2012.⁶ Funding has not kept pace with increased responsibilities. Any proposal to bring DA Platforms within its regulatory remit will need to be accompanied by appropriate funding and resourcing.

Consultation Questions

Set 2: Does the proposed exemption appropriately balance the potential consumer harms, while allowing for innovation? Are the proposed thresholds appropriate? How should the threshold be monitored and implemented in the context of digital assets with high volatility or where illiquid markets may make it difficult to price tokens?

⁵ As broadly discussed in ASIC Regulatory Guide 234 *Advertising financial products and services (including credit): Good practice guidance*

⁶ ASIC Submission to the Senate Economics Reference Committee Inquiry, pg 68.

The proposed licensing requirement is already a conservative approach to a high-risk area and we urge the Government to be cautious in considering any exemption.. If satisfied that this appropriately balances consumer protection with the need to encourage innovation, the Government should ensure the carve out for platforms holding less than \$1,500 per consumer or \$5mn total can be effectively enforced and is not at risk of manipulation.

We suggest DA Platforms claiming this exemption should be independently audited on an annual basis to confirm both that they meet this threshold and have adequate systems to prevent exceeding it. For instance, platforms need to be able to detect consumers holding multiple accounts beneficially. Accounts with platforms claiming this exemption also should not be able to be opened in the names of corporations or trusts, which may obscure the beneficial owner.

The value per account in assessing eligibility for this exemption should be taken as the higher of the actual purchase price paid by the consumer or the estimated value of the wallet. Where a digital asset is too illiquid or volatile for its value to be reasonably estimated, it should be taken as the actual price paid. This is essential to prevent further transfers where a consumer's digital assets have significantly devalued.

In addition to the proposed financial holding limit, we also suggest the Government considers a transaction limit on accounts with DA Platforms claiming this exemption. It would be a poor outcome if a scammer could use the exemption to transfer large amounts of consumer funds offshore and evade being detected as they would on a licensed DA Platform. The Government should consider imposing a monthly cap of \$1,500 in digital assets transfers to other platforms or wallets. The value should be calculated in the same method as above.

We consider that some obligations placed on licensed DA Platforms logically should be extended to any exempt DA Platforms. For instance, they should be required to block transfers to unlicensed DA Platforms. This is essential to prevent the exemption becoming a major loophole exploited by scammers.

To qualify for the licensing exemption, DA Platforms should be required to apply to ASIC. In approving an application ASIC should require satisfactory evidence that a DA Platform has adequate systems to prevent exceeding the exemption parameters.

RECOMMENDATION 6: Require that exempt DA Platforms:

- Apply to ASIC for an exemption
- Are audited to confirm that they comply with the exemption requirements
- Prohibit accounts held by incorporated organisations and trusts
- Impose transaction limits on all accounts
- Block transfers to unlicensed DA Platforms

Set 5: Should a form of the financial advice framework be expanded to digital assets that are not financial products? Is this appropriate? If so, please outline a suggested framework.

Our reading of Info Box 7 suggests that advice around purchasing or disposing of a digital asset would not be considered financial product advice unless it referred explicitly to using a DA Platform. This would undermine the proposed intention of protecting consumers and we refer to our comments above under 'Advertising restrictions'.

Set 16: Is this transitory period appropriate? What should be considered in determining an appropriate transitory period?

A 12-month transitory period from the passing of any legislation means that consumer safeguards remain a long way off. While we understand the need to give businesses time to adapt their processes, there is a high level of harm impacting Australian consumers every day. We urge the Government to intervene via regulation or a

prohibition as a matter of urgency and to consider requiring some key measures immediately if the proposed principles are passed into law, including:

- Require all DA Platforms applying for an AFSL to hold membership of AFCA immediately
- Require banks and DA Platforms for block transfers to DA Platforms that have not applied for an AFSL



APPENDIX A - SUMMARY OF RECOMMENDATIONS

RECOMMENDATION 1: Place an obligation on banks and DA Platforms to take steps to detect and prevent losses to scams. This should include:

- Mandating confirmation of payee for traditional accounts and digital wallets
- Stronger identity verification measures for individuals and business using or receiving payments via DA Platforms
- Immediate freezing of receiving accounts when a transaction is reported by customers, regulators or through the Australian Financial Crimes Exchange, or otherwise identified by the financial institution to be a scam loss
- Accessible and timely fraud reporting pathways for consumers

RECOMMENDATION 2: Place an obligation on banks and DA Platforms to reimburse consumers for scam losses, with any exceptions only in extremely unusual circumstances.

RECOMMENDATION 3: Require banks and DA Platforms to block transfers to unlicensed DA platforms. Where they fail to do so, there should be an obligation on the licensee to remediate any losses to the consumer.

RECOMMENDATION 4: Government should provide guidance to banks that regulation of cryptocurrency does not amount to any endorsement of its safety, and that banks should continue to take and expand upon a risk-based approach to blocking high risk transfers onto DA platforms, even where licensed.

RECOMMENDATION 5: Extend the licensing requirement to cover advertisements of digital tokens, and if unable to do so satisfactorily prohibit advertising altogether.

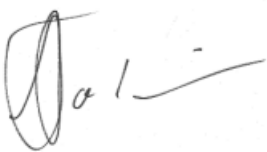
RECOMMENDATION 6: Require that exempt DA Platforms:

- Apply to ASIC for an exemption
- Are audited to confirm that they comply with the exemption requirements
- Prohibit accounts held by incorporated organisations and trusts
- Impose transaction limits on all accounts

Please contact Policy Officer **Rose Bruce-Smith** at **Consumer Action Law Centre** on 03 9670 5088 or at rose@consumeraction.org.au if you have any questions about this submission.

Yours Sincerely,

CONSUMER ACTION LAW CENTRE



Stephanie Tonkin | CEO