consumer action law centre

Level 6, 179 Queen Street
Melbourne, VIC 3000

info@consumeraction.org.au
consumeraction.org.au
T 03 9670 5088
F 03 9629 6898

26 May 2022

By email: crypto@treasury.gov.au

Director, Crypto Policy Unit
Financial System Division
The Treasury
Langton Crescent
Parkes ACT 2600

Dear Director

Submission: Crypto asset secondary service providers consultation paper

Thank you for the opportunity to respond to Treasury's consultation paper *Crypto asset secondary service providers: Licensing and custody requirements*. Consumer Action broadly supports the intention of the Government to introduce regulation to oversee the rapidly growing crypto asset environment. The crypto marketplace currently poses significant risk to consumers in numerous ways, and there is a pressing need for a regulatory regime that provides adequate protections and safeguards.

At a high level, the licensing of crypto asset secondary service providers (**CASSPrs**) as the mechanism to regulate the sector appears reasonable. However, it is important that the obligations imposed in the marketplace (and therefore, upon CASSPrs) go far enough to ensure that consumers are provided meaningful safeguards. Regulation of a sector amounts to public recognition and endorsement of its legitimacy. The Government has a responsibility to make the crypto market as safe as reasonably possible before providing this endorsement, and should ensure CASSPrs are genuinely up to a safe standard.

Our submission primarily focuses on the importance that the regulation introduces an adequate framework obliging CASSPrs to take genuine steps to protect customers from scams. Scams operating on crypto platforms are becoming increasingly common, resulting in significant losses and significant harm to individuals.

While there are many other facets to the crypto environment that pose a high risk to consumers (eg the volatility of the assets themselves), our submission only touches upon this in a limited manner. This is not an endorsement of other aspects of the consultation paper, but rather reflects that consumer protection for investment and wealth products is not core to our organisation's services, priorities and expertise.

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.

Terminology and definitions

Question 5 – breadth of CASSPr licencing regime

The definition of CASSPrs should be as broad as possible, to ensure these regulations capture all relevant players. The regulation needs to start from an 'all in' perspective. Australia's financial services laws and regulations have been plagued by the complexity caused by the range of exceptions, loopholes and qualifications to rules and requirements. This was identified by Commissioner Hayne in the Final Report of the Financial Services Royal Commission,[1] and is currently the subject of a major review piece by the Australian Law Reform Commission.[2] Complexity aside, where exclusions are incorrectly made and leave consumers at risk of harm, they generally take years to resolve.

The Government must not fall into the same trap in regulating crypto. While there may be differences in the nature of some crypto assets, the safety of the market would benefit greatly from a uniform licencing requirement. Further, any CASSPrs excluded would effectively be operating in an otherwise wholly unregulated environment. This market in particular is already complex and full of a range of different market players – a fact that will not be changed by the introduction of regulation. Consumers will benefit from the certainty that if they are dealing with a CASSPr of any type, they need to be licenced. This would also bring benefits to responsible players in the industry, as licencing across the board will help make legitimate and safer CASSPrs more easily identifiable.

RECOMMENDATION 1. Do not provide exemptions or loopholes to CASSPR licencing requirements, to ensure the licencing obligations are simple and universal.

Proposed principles, scope and policy objectives of the new regime

Question 6 - stated policy objectives

The policy objectives set out at page 14 of the consultation paper generally appear to be appropriate. However, it is important that the first objective of minimising the risks CASSPrs pose to consumers is not restricted by the sentence referring to minimum conduct standards. While minimum conduct standards are generally the form that regulation takes, it is important that the Government's mandate to protect consumers in a rapidly changing, high risk market is not limited in any way.

Should regulatory intervention need to take a different format – such as if temporarily necessary to respond to a problem identified – the Government should not be limited in how it can respond. Consistent with this, we recommend that as part of this reform, ASIC's product intervention power should be expanded to allow it to respond to major risks involving CASSPrs, even if unrelated to financial services. This is a high risk environment, and the regulator should have all appropriate powers at its disposal to intervene where necessary.

RECOMMENDATION 2. Ensure the Government's crypto policy objectives do not prevent the introduction of legislation or regulation that is reasonably necessary to protect consumers.

RECOMMENDATION 3. ASIC's product intervention power should be expanded to allow it to make orders to prevent significant detriment to retail clients involving the conduct of CASSPrs.

Question 7 – additional policy objectives

The Government also needs to play a more proactive role in protecting vulnerable groups (including children) in the community from being caught up in the furore surrounding crypto assets. While this may change in future, the value in crypto assets at present is nearly entirely speculative. Further, it is extremely volatile—entirely

[1] Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry; Final Report; 4 February 2019, p 494.
[2] https://www.alrc.gov.au/inquiry/review-of-the-legislative-framework-for-corporations-and-financial-services-regulation/

unpredictable external forces can cause the value of an asset skyrocket, or become near worthless. Investing in crypto assets is currently most similar to gambling.

The Government should therefore be taking steps to reduce the risk that these products are marketed toward people who are more susceptible to misleading marketing, such as unsophisticated investors (i.e. the general public). While the current saturation of gambling advertisements in all forms of media represents an astounding policy failure of all recent governments, some (extremely) basic limitations on where gambling can be advertised do exist, such as during television programs directed at children. At a minimum, these kinds of advertising restrictions should apply to crypto assets and CASSPrs. There is no reason crypto assets or CASSPrs should be marketing themselves toward anyone under 18. Equivalent restrictions should also be introduced to other media platforms (eg websites with childrens games; online videos likely to appeal to children).

Moreover, we consider that there should be restrictions from mass marketing by these firms, given that crypto is high-risk and unsophisticated investors are at high risk of losing significant funds. Crypto advertising is becoming commonplace across our sports codes – both via relationships with teams, as well as with venues. Just like betting odds in sports becoming almost completely ingrained in sports programming, crypto's current trend will likely result in speculative crypto assets being associated with sports teams, and ingrained in our psyche as an acceptable way to risk money. The government's failure to limit harms caused by the advertising of gambling doesn't mean that the crypto industry should get a pass on what we allow them to do in terms of mass marketing, too.

RECOMMENDATION 4. Introduce restrictions on the advertising of crypto assets and CASSPrs, to ensure that:

- adverstisements do not target unsophisticated investors, particularly children; and
- restrictions are placed on mass marketing by crypto assets and platforms in ways that are likely to reach children (eg via association with, or during the televising of, sports).

Question 8 – scope of licencing regime

We support the proposed scope of the licencing regime (subject to our comments responding to Question 5 above), provided that:

- all CASSPr conduct impacting consumers and relating to crypto assets is captured by either the financial services regime or the CASSPr regime; and
- where a CASSPr is dealing with a crypto asset that is also a financial product, the higher conduct standard applies.

The consultation paper appears to indicate that that the financial services licence regime will impose a higher standard of conduct than the CASSPr regime—so we support the financial services regime applying in this situation. However, if there are aspects of the CASSPr regime that go beyond the financial services regime, they should also additionally apply to all CASSPrs when dealing with a crypto asset that is a financial product.

Proposed obligations on crypto asset secondary service providers

Question 11 – CASSPr obligations

We draw attention to the proposed obligation 9 on page 16 of the consultation paper, concerning scams. It would be nigh on impossible to live in Australia and be unaware (or unbothered) by the alarming increase in the prevalence of scams on technology and communication platforms. Around $2 billion in Australia was lost to scams in 2021.[3] Losses from scams for individuals often involve significant, life changing amounts of money.

[3] Senate Estimates, Economics Legislation Committee, 17 February 2022, p 14 transcript.

Scams are also getting more complex and difficult for individuals to identify. Further, scams generally involve the development and exploitation of consumer trust, meaning that people are misled into trusting a scammer. This is often true for investment scams, which are the most likely to be occurring in relation to crypto assets, and involve CASSPr platforms. This all means that it is becoming increasingly less likely that consumers will be able to identify a scam.

At present, consumers who lose money to scams are left with little legal right of recourse to be reimbursed for any losses suffered. The current legal framework in this regard falls short of what is a fair distribution of risk, considering the fact that these scams necessarily occur on a financial or technology service provider's system.

We are concerned that the standard of conduct that obligation 9 in the consultation paper proposes to apply to CASSPrs in relation to scams falls well short of what consumers should be able to expect from these service providers. The language used ("respond in a timely manner") is vague and uncertain. An absence of clear obligatons in this regard risks leaving consumers unreasonably exposed to losses due to scams, and CASSPr operators with insufficient incentive to invest in making their platforms safe from scams. Obligation 9 should be improved by obliging CASSPRs to:

- proactively detect and prevent scams from occurring on their platforms; and
- reimburse consumers for losses they suffer due to scams, where the consumer has not been grossly negligent.

These obligations are consistent with obligations imposed under the UK Contingent Reimbursement Model Code, described further below, which is soon to be made mandatory for certain entities involved in that country's payment systems. This is an opportunity to embed genuine financial safety in the consumer protection framework that applies to the crypto marketplace from the outset.

Detection and prevention of scams

Crypto markets are a prime location for scammers to operate in. There is a high level of complexity to the assets, there are many different players, values of assets are susceptible to market manipulation, and the technology itself helps foster interactions between strangers with anonymity. It is therefore no surprise that there are reports that scams are highly prevalent in the crypto marketplace. At Consumer Action we have spoken with a number of clients who have lost significant sums through complex and difficult to identify scams making use of crypto platforms.

Case Study – Eugene's story

Eugene (name changed) is in his 60s and lives with significant physical and mental disabilities, and his sole income is the disability support pension. Over a period of ten weeks in mid 2021, Eugene lost over $150,000 – virtually his whole life savings - to scams involving three separate and well-known cryptocurrency exchanges, two of which are based in Australia.

The scammers posed as legitimate businesses and developed a relationship of trust with him, exploiting the way his disabilities impact his cognitive functioning and memory. As part of this scam, the scammers gained remote access to Eugene's computer, and created trading accounts on these crypto platforms. While these accounts were in Eugene's name, the scammers had access and control over them.

At one point, Eugene made a number of requests to at least one of the crypto platforms that should have made it plainly obvious to a competent service provider that his transactions were being influenced and misdirected by a third party. Despite these messages, the platform did not warn Eugene that he was being scammed, which resulted in Eugene suffering further losses.

These scams often use major platforms that are regarded as legitimate in the industry, adding to the difficulty to identify a scam. Binance is one company that has repeatedly come up in calls to our legal advice line about scams. Binance describe itself as the largest crypto exchange on their website,[4] and advertise the security of their platform on their website.[5] However, at law Binance have very few (if any) obligations to make their platform safe.

These platforms are worth billions, trade in complex technology as a speciality and derive financial benefit even from scam traffic on their platform, yet all the risk for scams sits solely on the shoulders of the individual. Further, many of the scams consumers have reported to our advice services could have been prevented if the crypto platform had even relatively basic safeguards and processes. Many of the scams rely on the ability to create accounts on crypto platforms with little to no chance of being caught, likely due to limited identification requirements and a near completely hands off approach to transactions (even when funds leave the platform). Other scams we have seen rely on being able to use a platform to redirect people to transfer funds from the platform to third party sites that will then vanish soon after. These are not characateristics of a safe marketplace.

Scams are a significant risk to the public benefit that regulating the crypto marketplace would achieve—if real efforts are not put into stopping them, the market will remain unsafe. Introducing regulation with soft or vague obligations on the licensed entities in the space will not provide sufficient incentive to CASSPrs to stop scams. The absence of clear obligations on banks in relation to preventing (and being liable for) authorised push payment (**APP**) scams demonstrates this—APP scams are occurring at a rapidly increasing frequency. The regulation of CASSPrs must contain certain obligations to proactively detect and prevent scams, rather than merely requiring a timely response to scams.

If CASSPrs are the regulated entity, this must be where these obligations sit. Consumers will always do their best to avoid being scammed—they need no greater incentive to act in their own best interests. Falling victim to a scam does not only bring the financial consequences for individuals, but it also has a significant psychological impact. Victims are left feeling taken advantage of, and the experience leave people feeling distrustful of others and technology. Public education efforts on the risk of scams and the prevalence of them may help, but it will no doubt be insufficient alone to effectively combat this—particularly considering the undue influence many scammers wield over their victims. The failure of disclosure as a means of consumer education and empowerment in the financial services space is a relatable example that demonstrates the limits of a 'buyer beware' approach.[6]

CASSPrs are far more likely to have the expertise and information available to them necessary to identify scams. Their platforms will see many more transactions pass through it than any one individual will ever be involved with, and they should have information regarding other individuals or entities using the platform. They are the facilitaor of the connection, and need to be required to make this connection safe. For this reason, the privilege of being licensed should be subject to a positive obligation to detect and prevent scams from operating or occurring on their platforms.

While introducing this proactive requirement would set a somewhat higher bar than that which currently applies to financial services in regard to scam prevention,[7] it would not be an altogether new concept. The obligation to perform services efficiently, honestly and fairly already requires financial service licence holders to deliver services with an adequate level of cybersecurity. In the recent case of *Australian Securities and Investments Commission v RI Advice Group Pty Ltd*, the Federal Court found that a financial services licencee had failed to deliver financial services efficiently and fairly because it did not have an adequate cybersecurity and cyber resilience framework in

---

[4] https://www.binance.com/en-AU/about

[5] https://www.binance.com/en-AU/

[6] Australian Securities and Investments Commission and Dutch Authority for Financial Markets, *Disclosure: Why it shouldn't be the default*, 14 October 2019, https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default/

[7] Though we strongly encourage Treasury to consider introducing an obligation for financial institutions to detect and prevent scams on their platforms as well, where relevant. For more information, see: https://consumeraction.org.au/banks-should-take-more-responsibility-for-scams/

place.[8] In that case, a number of cybersecurity incidents had been suffered by the licencee over a number of years. ASIC conducted an investigation which found that the licencee did not have sufficient controls and risk management measures in place to meet the public expectations of how a licencee would efficiently and fairly manage cybersecurity.[9]

The obligations of financial service licencees have also been found by the courts to at times require licencees to proactively intervene to prevent specific transactions where warning signs or red flags are known to them, even if the transaction is initiated by a customer. There has been a recognised duty at common law for bankers to exact a reasonable standard of care to combat fraud and protect bank customers and innocent third parties.[10] The UK High Court's Court of Appeal recently determined that this obligation extends to situations where a transaction is initiated by the customer, should the bank have reasonable grounds to believe that it may result in the funds being misappropriated.[11] There has also been recognition in Australian courts that the duty to follow a customer's direction or mandate to make a transaction may be overridden if the bank is on notice about a potential red flag.[12]

These cases demonstrate that while an explicit obligation to take positive steps to make a platform safe from scams would represent an enhancement in existing protections owed by similar licencees to their customers, it would not be a wholly new concept or without relation to existing conduct obligations. It would also be clearer and easier for consumers, CASSPrs and regulators to understand the extent of existing obligations in this regard.

Reimbursement for scam losses

To help make the obligation to detect and prevent scams meaningful, where CASSPrs fail to prevent a scam that takes place on their platforms and their customer suffers a loss as a result, they should be required to reimburse the victims of the scams. Making CASSPrs financially liable for losses will provide sufficient incentive for scam prevention to be treated as a priority.

This approach is already being adopted in mainstream financial markets in the UK, where the payment systems regulator introduced a voluntary Contingent Reimbursement Model (**CRM**) Code for banks in May 2019. Under the CRM Code, signatory banks commit to reimbursing their customers who fall victim to APP scams involving transfers through their banking platform, provided the customer is not grossly negligent.[13] Despite being voluntary, nine banks are signatories to the CRM Code. Further analysis by regulators and legislators on the impact of this in the UK has now led to the recent decision that this reimbursement obligation will be made mandatory for banks in the near future.[14]

The case for delivering the same level of consumer protections in the crypto asset marketplace in Australia is just as strong, if not stronger. The power imbalance between customers and CASSPrs exists in largely the same way as in banking, as does the far greater ability of CASSPrs to identify scams. Considering the technical complexity of some crypto assets and markets, and the vast array of misinformation in the space, it arguably presents an even greater case for requiring more efforts of CASSPrs to prevent scams.

An obligation to reimburse victims of scams would be consistent with the stated behavioural goals for CASSPrs described in the consultation paper as the intent of these obligations (flexible, honest,fair, integrity, competent). The regulation need not prescribe how CASSPrs protect consumers from scams, it would simply require that they

---

[8] [2022] FCA 496.

[9] Ibid, at [47]-[49]. Further, Rofe J found that the standard expected to meet by the public should be assessed with regard to an expert's understanding of the security (it was not limited by limited public understanding of complex technology or standards).

[10] *Barclays Bank plc v Quincecre Ltd* [1992] 4 All ER 363, at 376.

[11] *Phillipp v Barclays Bank UK plc* [2022] EWCA Civ 318.

[12] See *Territory Sheet Metal v ANZ* [2009] NTSC 31 at [1197 - 1217].

[13] https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/03/CRM-Code-LSB-April-2021.pdf, see Principles R1 and R2.

[14] https://www.gov.uk/government/publications/government-approach-to-authorised-push-payment-scam-reimbursement/government-approach-to-authorised-push-payment-scam-reimbursement

do so, or be on the hook for their failure. Regulation of this nature would prompt CASSPrs to more proactively identify high risk transactions and stop them, which is what is needed in this space.

RECOMMENDATION 5. Licenced CASSPrs should be subject to an obligation that requires them to:

- Prevent and detect scams from occurring using their platform; and
- Reimburse people who are victims of scams, where those losses occur through their platform.

Alternative options

Questions 17 and 25 – self-regulation

We strongly oppose leaving the crypto industry to develop self-regulation, as proposed by alternative option 2. Self regulation is an insufficient alternative to meaningful laws, and would be an irresponsible policy approach for the Government to take. Regulation exists because there is a need for meaningful protections that are enforced by a body with real powers. Self-regulation can be a useful mechanism for providing additional protection, but it cannot form the basis for oversight of an indstury altogether.

The shortcomings of self-regulation alone are obviously clear from the current operation of the buy now, pay later (**BNPL**) sector. The BNPL Code of practice developed and overseen by the Australian Finance Industry Association contains very few meaningful protections and therefore does little to protect or provide value to consumers. Additionally, the Code's compliance committee received only five complaints to it in its first year of operation,[15] despite the BNPL industry experiencing rapid growth. It is not a legitimate regulatory body. Further, even if the committee did receive many complaints, it has extremely limited powers compared to available under comparable legislation, if it did identify breaches justifying sanctions. Furthermore, the code is voluntary, meaning it has no application whatsoever to many players in the market. The end result is that all independent research suggests BNPL products are causing consumer harm, yet we don't really know the true impact because no regulator has a proper mandate to monitor this.

Politicians and government representatives have also come out and publicly endorsed the BNPL code, effectively amounting to the a similar level of endorsement of the legitimacy of the industry as would be demonstrated by developing regulation. Unfortunately, despite this endorsement, the Code does little for consumers, even if the BNPL provider is a voluntary signatory. Leaving the crypto market to regulate itself would be a similar disaster and would leave a massive loophole in a marketplace recognised by even its greatest supporters to be full of misinformation and risk.

Further information

Please contact Policy Officer **Tom Abourizk** at **Consumer Action Law Centre** on [redacted] or at [redacted] if you have any questions about this submission.

Yours Sincerely,

CONSUMER ACTION LAW CENTRE
Gerard Brody | CEO

[15] https://afia.asn.au/files/galleries/Buy_Now_Pay_Later_The_First_Year_of_Self_Regulation_March_2022.pdf

APPENDIX A - SUMMARY OF RECOMMENDATIONS

RECOMMENDATION 1. Do not provide exemptions or loopholes to CASSPR licencing requirements, to ensure the licencing obligations are simple and universal.

RECOMMENDATION 2. Ensure the Government's crypto policy objectives do not prevent the introduction of legislation or regulation that is reasonably necessary to protect consumers.

RECOMMENDATION 3. ASIC's product intervention power should be expanded to allow it to make orders to prevent significant detriment to retail clients involving the conduct of CASSPrs.

RECOMMENDATION 4. Introduce restrictions on the advertising of crypto assets and CASSPrs, to ensure that:

- adverstisements do not target unsophisticated investors, particularly children; and
- restrictions are placed on mass marketing by crypto assets and platforms in ways that are likely to reach children (eg via association with, or during the televising of, sports).

RECOMMENDATION 5. Licenced CASSPrs should be subject to an obligation that requires them to:

- Prevent and detect scams from occurring using their platform; and
- Reimburse people who are victims of scams, where those losses occur through their platform.