Treasury Consultation Paper: Scams – Mandatory Industry Codes

5th February 2024
scamspolicy@treasury.gov.au

Blockchain Australia welcomes the opportunity to respond to the Treasury consultation paper, "Scams – Mandatory Industry Codes".

The digital asset platform industry is a notable exclusion from the prescribed applicable industries. Foreseeing that this may change once legislation stemming from Treasury's Regulating Digital Asset Platforms consultation paper is enacted, our members felt it best to respond, such that our voices be heard during the policy formation of Mandatory Industry Codes related to Scams.

Blockchain Australia and its members are active participants of the National Anti-Scam Centre's (NASC) Advisory Board and Working Groups, respectively.

Committed to fighting scams, Blockchain Australia's members wish to ensure that practical Mandatory Industry Codes are adopted.

Please direct all enquiries to:

Simon Callaghan

Chief Executive Officer

Blockchain Australia

scallaghan@blockchainaustralia.org

Blockchain Australia
#MoreThanAConversation

RESPONSE TO CONSULTATION QUESTIONS

Q2. Is the structure of the Framework workable – can it be implemented in an efficient manner? Are there other options for how a Framework could be structured that would provide a more efficient outcome?

Anti-scam strategies will need to follow a risk-based approach so that the specific risks and limitations present in the relevant industry can be considered when assessing "reasonable" actions and liability.

Q5. Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?

Obligations not compatible with DCE services or blockchain technology:

- "A business must seek to detect, block and prevent scams from initiating contact with consumers" - doesn't apply to DCEs as our services do not facilitate this; seems applicable only to telcos/social media.
- "A business must seek to verify and trace scams where scam intelligence has been received" - although funds can be traced, unable to obtain beneficiary details like banks.
- "A business must provide their consumers or users with tools to verify information in real time" - unable to verify owners of wallets.

Q7. What impacts should the Government consider in deciding a final structure of the Framework?

Need to consider excessive customer friction that will lead scammers and their victims to use unregulated platforms.

Obligations of concern:

- "Where a business receives intelligence that a consumer is or may be a target of a scam, the business must take steps to disclose this to the consumer in a timely manner to minimise the risk of consumer harm or loss" - need clarification on the expectations for this as where investment company involved, possible that disclosure could result in defamatory remark of legitimate entity.

Q16. Are the obligations set at the right level and are there areas that would benefit from greater specificity e.g. required timeframes for taking a specific action or length of time for scam-related record-keeping?

The obligations proposed are less relevant to DCEs.

- Generally, DCE platforms do not provide any means for scammers to initiate contact with customers. DCEs can use measures such as anti-phishing codes or online verification tools to help users confirm if they have received a genuine piece of communication from the DCE.
- DCEs may take different actions in response to the receipt of scam intelligence. For example, a DCE can use blockchain analysis tools to trace funds, assess the risk level of wallet addresses and perhaps subsequently notify other DCEs of any unusual activity but are unable to obtain beneficiary details.

Q18. Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?

- Where scam reporting is required, should consider legislative amendment to AML Act to clearly establish that scam activity does not require an SMR (to prevent double up on reporting).
- Reporting through NASC would be ideal, as NASC engages each of the sectors involved. If this is not an option, reporting through AFCX may also help streamline reporting processes for banks and DCEs.

Q20. What additional resources would be required for establishing and maintaining an anti-scam strategy?

ACCC will likely need to produce a guidance paper that assists entities to assess their risk.

Q22. Are there parts of a business's anti-scam strategy that should be made public, for example, commitments to consumers that provides consumers an understanding of their rights?

Possible requirement to publish anti-scams strategy:

- Critical that we do not publish anti-scam strategies, as this would just put information about how entities are detecting and preventing into the hands of bad actors and allow them to pivot behaviour.

The entity could issue a statement about its compliance with the scam code framework (like the requirement for Modern Slavery Act statements), rather than publish their Anti-scam strategy.

Q26. What resources would be required for establishing and maintaining additional information sharing arrangements with other businesses, the NASC and sector-specific regulators under the Framework?

Obligations of concern:

- "A business must share data and information on the incidence of scams, and action taken in response, with designated industry bodies, law enforcement and regulators, and the NASC" - should require legislative update to Privacy Act to allow disclosure of personal information to third-parties for the purpose of financial crime prevention.

Q31. If the remit for existing EDR schemes is expanded for complaints in relation to this Framework:

a. what criteria should be considered in relation to apportioning responsibility across businesses in different sectors?
b. how should the different EDR schemes operate to ensure consumers are not referred back and forth?
c. what impacts would this have on your business or sector?

- The apportioning of responsibility across businesses in different sectors should take into account the steps taken by each business to detect, prevent and respond to the scam activity, whether the steps taken were reasonable.
- The methodology applied by EDRs for the determination of compensation to be paid for financial and non-financial loss should be agreed between the EDRs and applied consistently. The methodology should also be disclosed to respective member firms. AFCA may need more training to achieve better consistency in handling scam-related complaints.

Q32. Should the Government consider establishing compensation caps for EDR mechanisms across different sectors regulated by the Framework? Should these be equal across all sectors and how should they be set?

EDR compensation caps should apply equally across all sectors to avoid the heaviest consequences being unfairly directed to the businesses at the 'exit' stages of the scam ecosystem.

CLOSING REMARKS

Blockchain Australia appreciates the opportunity to provide feedback on Treasury's Scams – Mandatory Industry Codes consultation paper.

This policy submission was coordinated by Jedda Stocks-Ramsay, in close consultation with other members from Blockchain Australia's Digital Currency Exchange Working Group and Digital Assets Working Group. Blockchain Australia also thanks Michi Chan for her contributions.

These opinions were formed through observations made through various forums, including participation in the National Anti-Scam Centre, and experience in dealing with fraud/scams.

Our other policy submissions are available for viewing at:
https://blockchainaustralia.org/submissions/

ABOUT BLOCKCHAIN AUSTRALIA

Blockchain Australia is the peak industry body representing Australian businesses and business professionals participating in the digital economy through blockchain technology. Blockchain Australia encourages the responsible adoption of blockchain technology by the government and industry sectors across Australia as a means to drive innovation and create jobs in Australia.

Blockchain Australia's membership base consists of 120+ leading cryptocurrency and blockchain-centric businesses and 90+ individuals across multiple verticals, including:

- Accounting and Taxation
- Artificial Intelligence
- Art
- Banking
- Building & Construction
- Cyber Security
- Development
- Digital ID
- Education
- Energy and Resources
- Entertainment
- Gaming
- Health and Wellbeing
- Insurance
- Investment
- Legal
- Professional Services
- Recruitment
- Real Estate
- Risk and Compliance
- Supply Chain
- Venture Capital