

27 March 2023

By email: crypto@treasury.gov.au

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

Dear Director

Token Mapping Consultation Paper

Consumer Action Law Centre (**Consumer Action**) thanks you for the opportunity to respond to Treasury's consultation paper (**Consultation Paper**) on token mapping of cryptocurrency (**crypto**) in Australia. The crypto marketplace currently poses significant risk to consumers and there is a pressing need for adequate protections and safeguards.

Consumer Action applauds the Government for its commitment "to improving the way Australia's regulatory system manages crypto assets – to provide greater protections for consumers and keep up with technological developments" and for recognising the need to review the regulatory framework to address the growing risks to consumers of the crypto ecosystem.

Government intervention in some form in the crypto marketplace is vital, and it needs to have a significant impact upon current industry practices. We note that the consultation paper has detailed consumer harms, particularly where consumers use crypto for speculative investment. We can confirm, through our casework (case studies included below), that consumers have been using crypto primarily for speculative, high-risk investment akin to gambling and have experienced major financial losses for doing so.¹ While dressed as an investment opportunity, crypto is not well understood and is regularly used to deceive unsophisticated consumers and facilitate scams.

The absence of a ban or regulation in the crypto space makes Australia an extremely attractive playground for scammers. As detailed below, we consider the risk posed to warrant the introduction of universal regulation across the sector, regardless of the nature of the crypto assets involved. Leaving aspects of the crypto market open to unlicensed players will leave obvious loopholes for scammers to continue operating in. Our view is that unless banned, any business involved in crypto investing, trading or advice in the retail market must meet strict licensing obligations.

We are concerned that regulating crypto will amount to public recognition and endorsement of its legitimacy by Government. Accordingly, if proceeding with regulation the Government needs to meaningfully reduce the risks involved in the marketplace by applying significant obligations on all businesses operating in the sector, including in relation to detecting and preventing the rapidly increasing problem of scams.

Any regulation should apply universally across crypto where possible as a starting point, to reduce complexity for consumers and ensure safety. It should also include restrictions on advertising and marketing, again, to protect

¹ <https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html>

consumers from scams. Major differences should not exist between the consumer protections afforded to people based upon the differences between crypto assets and tokens explored in the Consultation Paper, as most consumers will be unaware of these differences.

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



Question 1: The role of Government in crypto regulation

Government's role should be to provide consumers with meaningful protections against unsafe products, meet challenges which arise on the introduction of new technologies and ensure markets are reasonably safe for consumers. We expect Government to take proactive steps to make market players act fairly and responsibly.

Do the harms outweigh the benefits of crypto?

Regulation of the crypto sector will unavoidably amount to endorsement by Government for many consumers, sending a message that crypto is safe for the average, unsophisticated investor. It follows that Government must give proper consideration to whether parts of the crypto market causing significant harm in Australia can be made safe, and if they can't, consider bans where risks are unacceptable. Real consideration is needed in relation to currency trading and consumer facing investment opportunities, which is where we see most scams occur..

Recent multibillion dollar collapses of crypto platforms and assets demonstrate the harms complex and reckless conduct in a volatile market can cause, which outweigh the benefits of crypto. These crashes have significantly impacted Australian consumers,² and financial losses resulting from scams on these platforms have also been huge.

To demonstrate the harm we have included case studies below. John's case demonstrated the long term financial harm, investing in crypto, without the ecosystem being regulated, can cause vulnerable consumers. As a result of being scammed by a so called crypto investment last year, John has since been struggling with unaffordable repayments on his loans – and had fallen into a debt spiral in an attempt to meet the repayments on his loans. John is currently working with NDH financial counsellors to understand his rights and options and take back control of his financial situation.

In the UK, TSB, a bank that commits to refunding losses its customers incur due to fraud or scams, has made the decision to ban transfers to crypto platforms altogether because the rates of scam losses were so much higher when crypto transfers were permitted.³ It should not be a given that crypto markets must continue to operate in Australia if they cannot be made reasonably safe.

Government's role is to make marketplaces safe

Whether through a ban of some sort or robust regulation, meaningful Government intervention in the crypto market is essential, particularly in areas that are attracting investors without technical expertise, such as John. Crypto assets are extremely volatile - unpredictable external forces can prompt the value of an asset to skyrocket or become near worthless and misinformation is rife, leaving unsophisticated investors extremely vulnerable to predatory behaviour.

RECOMMENDATION 1. If the Government decides to regulate crypto, it must be comprehensive and in a way that introduces meaningful obligations upon all market players operating in Australia, This should include meaningful obligations related to the prevention and deterrence of scams (discussed below). Crypto related businesses should be expected to earn the implicit endorsement that any regulation would provide. If regulating crypto, the Government should introduce all obligations and safeguards necessary to make crypto markets safe, reasonably navigable and require fairness and accountability of all market players.

RECOMMENDATION 2. Crypto regulation must provide a regulator with sufficient powers to intervene in the market, and resourced to effectively enforce the law.

² <https://www.investopedia.com/what-went-wrong-with-ftx-6828447>; <https://www.theguardian.com/australia-news/2023/jan/30/australian-regulator-had-ftx-under-surveillance-at-time-of-collapse-documents-reveal#:~:text=FTX%20put%20its%20Australian%20companies,ranging%20up%20to%20%24.1m>

³ Details on TSB's fraud refund guarantee available here: <https://www.tsb.co.uk/fraud-prevention-centre/fraud-refund-guarantee/>

Regulate from an all-in perspective

The complexity and length of the Consultation Paper reflects the vast information that anyone must be across to truly understand crypto. The ecosystem is also changing rapidly. The whole sector is already too complex to allow completely unregulated voices or businesses to persist. Accordingly, any plans to regulate the industry should involve a broad, all-in approach to licensing and regulation.

If the Government declines to ban crypto, all businesses seeking to profit in crypto markets in any way in Australia should require a licence. While we support functional definitions, falling outside the definition of financial service should not exempt crypto businesses from regulation. Australian financial services laws are notoriously difficult to understand due to the complex and numerous boundaries and exemptions. There is also a proliferation of business models at the regulatory perimeter that avoid capture as financial products or credit products, despite presenting the same (or worse) risks which, we acknowledge the Government is trying to understand through the token mapping and also this consultation process. It is inaccurate to suggest that outside crypto, our financial services laws apply a simple functional definition that captures all appropriate financial products. Findings from the Australian Law Reform Commission's inquiry into the complexity of financial services legislation demonstrate this.⁴

RECOMMENDATION 3. Define the crypto market as broadly as possible and require all relevant entities in the sector be licensed as a starting point, if regulating. Do not provide licensing exemptions in legislation.

Question 2: Potential consumer safeguards

Development of consumer safeguards needs to be driven by an exhaustive examination of all the risks that are causing harm in crypto markets. Safeguards must rely on well-established consumer protections that have been proven to meaningfully improve the safety of markets and go some way to address the stark power imbalance between industry and consumers in the marketplace, as outlined below.

Financial services and products regulation a minimum equivalent

We recognise that the Consultation Paper provides important detail about the different crypto tokens and how the financial services framework presently applies to them. Despite the differences in crypto, we urge the Government to ensure that regulation, at a minimum, universally contains equivalent protections for consumers that currently exist for financial products. Boundaries of regulation should not revolve solely around the question of whether a product meets the functional definition of a financial product.

There are consistent challenges consumers face across the whole crypto space that mirror those posed by financial services. In particular, this includes the complexity of understanding products and terminology used in the space and the risks that come with investments (including scams). As has been well established in financial services, there are significant limits the effect of disclosure of complex terms and conditions can have, making obligatory responsible product design and clear laws protecting consumers essential.⁵

Assuming the Government declines to ban crypto, we would urge the Government to develop a crypto regulatory framework that (among other things):

- Requires all market players to be licensed (this must include trading platforms)
- Obliges licensees to provide their services with due care and skill
- Contains important sales practice obligations, such as bans on unsolicited selling

⁴ <https://www.alrc.gov.au/inquiry/review-of-the-legislative-framework-for-corporations-and-financial-services-regulation/>

⁵ 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/>

- Applies the design and distribution obligations regime (or equivalent) to all crypto tokens or services, where appropriate
- Provides a power for the regulator to intervene to prevent and deter significant consumer detriment
- Obliges licensees to take meaningful action to detect and prevent scams and reimburse victims for their scams losses (see response to question 3 below)
- Requires licensees to be members of an external dispute resolution scheme.

RECOMMENDATION 4. Any attempt to regulate crypto should ensure that all consumer facing businesses working with crypto are subject to the same obligations that exist in financial services, at a minimum, with additional obligations to address scams.

Some areas of crypto should be more heavily regulated

The Government should also not shy away from introducing additional protections where necessary, recognising that many crypto assets are less understood, more speculative and more complex than many financial products. The increasing tendency for scammers to use crypto and crypto platforms as the preferred vehicle for their model is one example of why this is appropriate (discussed further in response to question 3).

Outside of scams, other risk factors that may justify additional intervention include:

- the risks that come with a entirely digital marketplace, including fraudulent websites and international players
- risks that arise from the anonymity that crypto is designed to permit
- the volatility of the market and its potential for manipulation, particularly by large investors
- the constantly changing understanding of different forms of crypto technology and assets.

RECOMMENDATION 5. Any area of the crypto ecosystem identified as posing a higher risk to consumers should be subject to additional safeguards tailored to address the risks.

Consider temporary interventions as a stop gap

The Consultation Paper and other indications suggest that major decisions on a Government approach toward regulation of crypto are still a long way away. This is understandable considering the complexity involved, but is also concerning. The Government should consider introducing temporary measures to address obvious existing financial safety concerns outlined. For example, the fact that a trading platform as large as Binance avoids capture by regulation should be of major concern to the Government. Scams involving the Binance platform are a frequent problem raised by callers to our services- see Anil's story below. As a result of the Binance scam Anil is now facing the risk of bankruptcy. Binance is a massive multinational company making significant money out of its operations in Australia. It should not be able to continue to operate unchecked.

RECOMMENDATION 6. Introduce stop gap bans or oversight of major companies in the crypto space that are known to be involved in, or whose platforms are used for, scams.

Question 3: Addressing scams

Australians lost around \$2 billion to scams in 2021 overall⁶ - a figure that is estimated to have doubled to \$4 billion in 2022.⁷ Scams involving crypto have increased at an even faster rate than these figures, with the ACCC's

⁶ ACCC, Targeting Scams: Report of the ACCC on scams activity 2021, available at: <https://www.accc.gov.au/publications/targeting-scams-report-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2021>

⁷ <https://www.accc.gov.au/media-release/scams-awareness-week-2022-empowers-australians-to-spot-a-scam-o#:~:text=This%20year%20combined%20losses%20might,the%20same%20period%20last%20year.>

Targeting Scams report on figures for 2021 indicating a 216% increase in cryptocurrency losses. The ACCC has also indicated that crypto has become the preferred payment (or theft) method for investment scammers.⁸

Our casework indicates that scammers exploit the complexity, volatility and lack of clear guidance around crypto when engaging in scams. Often victims are engaged through targeted online marketing and many scammers foster 'business' relationships that involve the development of significant trust as part of the scam. Crypto is also used opportunistically in romance scams, particularly when the scammer claims to be from a country where financial freedom or stability is not guaranteed – sending funds via crypto platforms is claimed to be safer than sending money by more formal means. Our clients have reported significant harm, both financially and psychologically, due to falling victim to these kinds of scams.

Case Study – Anil's story

Anil (name changed) is married with two children. He told a financial counsellor that late last year he was close to saving a deposit for a family home but had been struggling with increases in property prices and the cost of living, and was seeking further income. He told us it was around this time he was contacted via Whatsapp and offered an opportunity to make extra income via investing in an app design website platform.

He said that he was credited \$80USD to start, and transferred \$20USD to the platform himself, which he did by transferring money from his NAB account onto crypto platform Binance and exchanging it into USD, as directed on Whatsapp. Anil said he then transferred the USD to another Binance wallet which led to his account on the other website being credited. Anil told us that in the first couple of days he engaged with the website like a second job and made some money on the platform and was able to withdraw some of it a few times, which led to him investing significantly more money (via Binance) – eventually \$140,000, his whole house deposit savings.

Anil said soon after these deposits he could no longer get any money out, and was told that he needed to deposit more to access it within a day or two, which created a sense of urgency for him. He said in desperation he eventually obtained two loans totalling \$90,000, and his wife got another \$45,000, which was all 'invested' as well, but not recoverable. Anil told us that at this point he sought assistance from family and friends, whose questions led him to grow suspicious and question whether it was scam, and started making his own investigations that raised significant concerns.

Anil told us he reported the scam to NAB, which took many weeks to investigate the scam but eventually told him nothing was recoverable and they were not able to help. He also said NAB didn't contact him at all about these transactions, despite emptying his whole account and taking out a significant loan with them.

⁸ <https://www.accc.gov.au/media-release/australians-are-losing-more-money-to-investment-scams>

Case Study – John’s story

John (name changed) contacted the NDH in October 2022 for assistance with unmanageable debt. John told us he had invested \$250 in cryptocurrency after receiving a cold call about an investment ‘opportunity’ with ‘SwipeCapital’. John recalls that after his ‘investment’ started to drop after a week or two, a scammer posing as a representative of SwipeCapital, using AnyDesk, helped him apply for a personal loan of \$20,000 from a fringe lender. In fact, the lender approved John for a loan of \$40,000, all the proceeds of which he promptly invested in crypto.

John told us his initial attempt to transfer the loan amount from his bank account with Bendigo Bank into the exchange platform CoinSpot was flagged by Bendigo Bank and rejected. The scammers then encouraged John to use the alternate exchange platform CoinJar and the transfers were authorised by the bank. John says he watched the scammers make riskier trades with his money over several weeks. He recalls the scammers' claims that another trade and more money was needed to avoid him suffering significant losses. Ultimately, John obtained another \$10,000 loan, and transferred this to the scammers, who soon disappeared. John explained that he has since been struggling with unaffordable repayments on his loans – and had fallen into a debt spiral in an attempt to meet the repayments on his loans. John is currently working with NDH financial counsellors to understand his rights and options and take back control of his financial situation.

Uniform licensing necessary to stop misinformation

The absence of a ban or regulation in the crypto space makes Australia an extremely attractive playground for scammers. As detailed above, we consider the risk posed to warrant the introduction of universal regulation across the sector, regardless of the nature of the crypto assets involved. Leaving aspects of the crypto market open to unlicensed players will leave obvious loopholes for scammers to continue operating in. Our view is that unless banned, any business involved in crypto investing, trading or advice in the retail market must meet strict licensing obligations.

A broad approach to licensing would make it easier for a regulator to crack down on misinformation in the crypto space and would make it easier for consumers to determine the legitimacy of an entity they were dealing with, and identify unlicensed or unlawful players. Based on our casework, this should at the very least apply to anyone involved in crypto trading and investment – whether it be facilitating trades (like a platform) or providing advice.

Case Study – Sarah’s story

Sarah (name changed) is a single mother who was referred to the NDH by Victoria Police in August 2022. Sarah explained she signed up to an investment platform (AllCryptMarket) after seeing an ad on Facebook which promised education on trading platforms and engaging in the stock market. As a deposit to the platform, Sarah paid a little over \$350 in bitcoin, via the exchange company CoinSpot. Sarah recounted she was assigned an account manager, who built her confidence to continue to transfer greater amounts into her wallet on the AllCryptMarket platform.

Over two months, Sarah ended up investing around \$200,000 of Bitcoin into AllCryptMarket via CoinSpot. During this time, transactions between her bank and CoinSpot were frozen twice for a 24hour period, though Sarah told us the bank didn’t contact her to explain the freeze or to query the transactions. Sarah told us that when she grew wary and requested a withdrawal of her investment, she was only able to secure \$1000 of the money she had invested. She said the scammers then told her the remainder of her money had gone into an ‘escrow’ account, but it was recoverable with a payment of \$100,000.

Sarah said this was when she ended up reporting the matter to Victoria Police. Sarah recounts she spoke to CoinSpot who explained AllCryptMarket was a scam. CoinSpot also outlined they had no obligation to verify third-party entities engaging with their platform, such as AllCryptMarket. Despite having written to AllCryptMarket with a letter of demand and reporting their activities to the police, AllCryptMarket has continued to trade under the moniker ACM. Sarah has described the impact this scam has had on her life – she explained the shame she felt, how she struggles to eat and sleep as she feels helpless. Sarah has lodged complaints with AFCA about both her bank and CoinSpot.

Require licensees to prevent scams and require reimbursement

For all licensees to which it is relevant, licensing should impose an obligation on the licence holder to detect and prevent scams from operating on their platforms, and where they fail to do so, they should be required to reimburse victims for losses, subject to limited exceptions (such as if the consumer acted with gross negligence). There is currently little legal recourse available for consumers who fall victim to a scam on a financial or crypto service provider’s platform. We strongly recommend that the Government introduce this obligation for all crypto entities that operate a platform where money is held or changes hands, and consider it for the broader financial sector.⁹ Currently, the absence of any meaningful obligations means that scammers are using these platforms as their platform of choice, due to the lax oversight platforms have of users and the transactions taking place on their platforms. Despite crypto exchanges being some of the biggest businesses and winners to come out of the crypto boom, our experience is that these entities appear to treat safety and scam prevention on their platforms as a problem for their customers, not themselves.

The primary policy justification for introducing this obligation is to incentivise crypto businesses to invest in making their platforms safer and to prevent scammers for using platforms to avoid accountability and regulation.

The growth in scams losses for Australians underlines that the current approach of placing virtually all the financial liability for scam losses on the victims has made Australia an attractive target for scammers. Meaningful intervention is necessary and appropriate. Placing the financial liability upon the market players would be a powerful motivator but would also enable crypto businesses to invest in scam prevention the way they consider most appropriate. It would also allow these more powerful and informed market players (rather than consumers) to determine appropriate risk appetite.

⁹ See our comments in our submission to Treasury’s consultation on a strategic plan for the payments system for more information: <https://consumeraction.org.au/a-strategic-plan-for-the-payments-system/>

RECOMMENDATION 7. Introduce an obligation for all entities that are involved in crypto transactions or investment to detect and prevent scams from occurring on their platforms. Where entities fail to do so, they should be required to reimburse their customers for scam losses, unless the consumer acted with gross negligence.

Banks need to mirror and support scam prevention

At present, there are inconsistent approaches applied by different banks in relation to transactions out of accounts by customers that appear to be related to crypto. When speaking with clients who have fallen victim to scams involving crypto in some way, we hear about extremely varied levels of interventions and assessments applied to these transactions. In some cases, banks will query large transactions. This seems to happen more often when it is the first transaction to a new platform or the first involving crypto, but in other cases, first time transactions that are completely out of character in size for the customer to crypto platforms will not trigger any investigation by the bank whatsoever. We have even seen cases where a banks blocks a transaction and the consumer is directed by a scammer to use another bank, which won't make any inquiry at all.

Case Study – James' story

James (name changed) contacted the NDH in August 2022. After seeing ads on Youtube and Facebook, James told us he signed up to a fraudulent crypto platform, Crypto Market (then called Crypt Market). On signing up, James recounted he paid \$250 and was contacted by a 'broker' who talked him through the investment process. James told us the broker assisted him through AnyDesk in applying for an initial loan of roughly \$30,000 to fund his investment. James recounted he was prevented by his bank from transferring this money across to the exchange platform, FTX, as it was flagged as a possible scam. James said the scammers then assisted him in setting up an account with Commonwealth Bank as the scammers knew Commonwealth Bank would permit the transfer through to FTX, where the crypto would be moved into his Bitcoin wallet.

James ended up making nine transactions to FTX of over \$90,000, in about seven weeks James told us he was never contacted by Commonwealth Bank about his activity. James told us he ended up with four different loans he arranged with help of the scammer, amounting to over \$80,000, with fortnightly repayments of more than 50% of his income. James has since declared bankruptcy and has lodged a number of complaints to AFCA. Commonwealth Bank offered \$5,000 of pain and suffering compensation.

While strict legal obligations on banks require minimal inquiry, we consider the inconsistent approaches currently taken by the banking industry to scam prevention to be insufficient. Australian Financial Complaints Authority (AFCA) decisions however indicate that most banks are meeting the low legal standard – our analysis of published decisions from mid 2021- early 2022 found that around only 6% of cases that reach final determinations in complaints against banks for scam losses resulted in the consumer receiving a refund for their loss.¹⁰

As scams continue to increase, a significant change in ordinary practice within the crypto and scams ecosystem is required to prevent financial losses from climbing higher each year. Considering the prevalence of scams involving crypto, banks should be expected to meaningfully engage with (at least first time) account holders making significant transfers onto a crypto platform. This is justified at present because of the lack of regulation and consumer safeguards in the space.

¹⁰ See "More than \$2billion lost as redress system fails scammed Aussies" <https://consumeraction.org.au/more-than-2billion-lost-as-redress-system-fails-scammed-aussies/>

In the future (if crypto were regulated, particularly as we suggest here) this standard could be retained and be treated as an opportunity for banks to inform customers of the existence of a licensing regime that applies across the sector, and help check that all the entities a consumer is engaging with are licensed.

Our submission to Treasury's consultation on a strategic plan for the payments system earlier this year¹¹ contains further information on our views on the need for higher standards to be applied to banks in scam prevention, and the case for similarly requiring reimbursement of customers for scam losses where the losses are via bank transfers.

RECOMMENDATION 8. Introduce a mandatory obligation requiring banks to detect and prevent scams resulting from transfers from their platforms. When banks fail to do so and the money is lost via the bank transfer, they should be required to reimburse their customers for scam losses, unless the consumer acted with gross negligence.

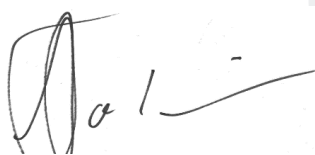
Establishing an obligation upon financial service providers to reimburse customers for scam losses is not without precedent. Reimbursement in the case of scam losses would align existing protective mechanisms against 'unauthorised' banking transfers (under the e-Payments Code). These reimbursement obligations would also be similar to those introduced in the United Kingdom in 2019, under their Contingent Reimbursement Model Code for Authorised Push Payment Scams (**CRM code**).¹² The CRM Code includes a fundamental principle that when a customer has been the victim of a relevant scam, the bank should reimburse the customer. There is currently a proposal in the UK to make the CRM Code mandatory for all banks and payment systems providers, and to limit existing exceptions to only exist where a customer has been 'grossly negligent'.¹³

Further information

Please contact Policy Officer **Tom Abourizk** at **Consumer Action Law Centre** on 03 9670 5088 or at tom.a@consumeraction.org.au if you have any questions about this submission.

Yours Sincerely,

CONSUMER ACTION LAW CENTRE



Stephanie Tonkin | CEO

¹¹ [A Strategic Plan for the Payments System - Consumer Action Law Centre](#)

¹²

¹³

APPENDIX A - SUMMARY OF RECOMMENDATIONS

RECOMMENDATION 1. If the Government decides to regulate crypto, it must be comprehensive and in a way that introduces meaningful obligations upon all market players operating in Australia. This should include meaningful obligations related to the prevention and deterrence of scams (discussed below). Crypto related businesses should be expected to earn the implicit endorsement that any regulation would provide. If regulating crypto, the Government should introduce all obligations and safeguards necessary to make crypto markets safe, reasonably navigable and require fairness and accountability of all market players.

RECOMMENDATION 2. Crypto regulation must provide a regulator with sufficient powers to intervene in the market, and resources to effectively enforce the law.

RECOMMENDATION 3. Define the crypto market as broadly as possible and require all relevant entities in the sector be licensed as a starting point, if regulating. Do not provide licensing exemptions in legislation.

RECOMMENDATION 4. Any attempt to regulate crypto should ensure that all consumer facing businesses working with crypto are subject to the same obligations that exist in financial services, at a minimum, with additional obligations to address scams.

RECOMMENDATION 5. Any area of the crypto ecosystem identified as posing a higher risk to consumers should be subject to additional safeguards tailored to address the risks.

RECOMMENDATION 6. Introduce stop gap bans or oversight of major companies in the crypto space that are known to be involved in, or whose platforms are used for, scams.

RECOMMENDATION 7. Introduce an obligation for all entities that are involved in crypto transactions or investment to detect and prevent scams from occurring on their platforms. Where entities fail to do so, they should be required to reimburse their customers for scam losses, unless the consumer acted with gross negligence.

RECOMMENDATION 8. Introduce a mandatory obligation requiring banks to detect and prevent scams resulting from transfers from their platforms. When banks fail to do so and the money is lost via the bank transfer, they should be required to reimburse their customers for scam losses, unless the consumer acted with gross negligence.

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.