Level 6, 179 Queen Street
Melbourne, VIC 3000

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

31 January 2024

By email: scamspolicy@treasury.gov.au

Toby Robinson
Director
Scams Taskforce
Market Conduct and Digital Division
The Treasury

Dear Director

Scams – Mandatory Industry Codes Consultation Paper

Thank you for the opportunity to provide feedback on the Government's proposed scams code framework. This is a joint submission made on behalf of:

- Consumer Action Law Centre
- CHOICE
- The Australian Communications Consumer Action Network

This joint submission has also been endorsed by:

- Super Consumers Australia
- Financial Counselling Australia
- WEstjustice

- Consumer Policy Research Centre
- Financial Rights Legal Centre
- Consumer Credit Legal Service

Consumer Action Law Centre, CHOICE and the Australian Communications Consumer Action Network have been conducting regular roundtables with scams victims and consumer organisations, to develop our responses to the proposal outlined in the Scams – Mandatory Industry Codes Consultation Paper (the Paper). This submission includes the collective view of our organisations.

At the heart of the scams regulatory framework must be liability for reimbursement resting with industry. For the reasons and examples outlined below, the only workable framework that will effectively disrupt scams and protect consumers would be a presumption of reimbursement of scam losses, with industry bearing the onus of proof otherwise. The regulatory framework needs to be governed by the key principles outlined below and explained in further detail in the full joint submission.

If the money lost to scams were to come straight out of the bottom line of the industries who are the gatekeepers of people's money, personal and online information, industry will be incentivised to significantly increase their investment in measures and new technologies to keep the public and their customers safe and secure. This is the only way to achieve the level of investment needed by industry to disrupt scams in Australia.

Consumers need a simplified, single pathway to seek redress after businesses fail to protect them from scams. This complaint avenue should be through the customer's bank or financial institution where the funds were initially kept or lost. The regulatory framework proposed in the Paper is far too complex and will be virtually impossible for consumers to navigate on their own and for industry to deliver.

While the core principles of the Paper are a step in the right direction, they do not meet community expectations of the 'tough new industry codes' or a 'high bar for liability' that the Government has been promising for the past year and a half. The primary goal of the introduction of mandatory laws and codes relating to scams should be modelled around improving consumer outcomes and preventing harm, rather than solely relying on businesses to comply with minimum obligations, which will continue to result in victim blaming and shifting obligations and costs onto consumers who are near-powerless to detect or prevent scams from occurring.

10 Core Recommendations

1. **The frameworks needs to be governed by mandatory and enforceable prescriptive codes** imposing high standards on the banking, telecommunications and digital platform sectors, that are enforced by empowered and resourced regulators:
    - ASIC for banking (and eventually all other financial services providers)
    - ACCC for telecommunications and digital platforms (and all others).

    We need prescriptive standards covering **prevention, detection and disruption,** that are amendable as technology and scammers develop and innovate.
2. **Mandatory reimbursement of consumer losses by their banks. Mandatory reimbursement** is the **best** way to prevent and disrupt scams – through incentivising adequate investment in prevention systems – and ensuring consumers can access redress where industry has failed to protect them. A strong presumption of reimbursement must apply.
3. The obligations on industry and the **presumption of reimbursement must be higher for vulnerable consumers.**
4. **A fair, simple, fast and effective dispute resolution pathway for consumers.** A single internal dispute resolution (IDR) pathway for reimbursement through a consumer's bank(s), with a compressed 5-day decision timeline.
5. Where IDR fails, there needs to be a **single door** for the consumer to access external dispute resolution (EDR) to cover all code-regulated bodies. The **single door EDR** can leverage existing dispute resolution architecture, specifically, the Australian Financial Complaints Authority (AFCA).
6. **Provide a mechanism for banks to recover the cost of scam losses from other bodies** regulated by the Code where action (or inaction) by those entities contributed to the scam occurring. This process should occur after a scam victim has already been reimbursed by their bank. The burden of apportionment should lie with industry not consumers.
7. We need a practical, as **broad as possible** definition of scam to include all circumstances where a consumer has lost money as a result of being scammed. For example, the **definition of a scam** should not impose an unreasonable evidentiary burden or barrier by requiring victims to prove the mental intention of a scammer, in order to seek redress for losses under the framework.
8. The **ePayments Code should be made mandatory** and be subordinate and consistent with overarching scams legislation and industry codes to **ensure no consumer falls through the gaps** between the two regimes.
9. **Fast-track the best model possible**, as soon as possible (before the end of 2024). The **2-year timeframe is too long**.
10. Expand the proposed definition of digital platform to reflect the scope of digital platforms covered by the Digital Platform Services Inquiry, which includes electronic marketplace services.

Digital Platforms

We have provided an additional sections detailing sector specific obligations and recommendations that should apply to digital platforms (**Appendix A)**. The key results from a number of CHOICE surveys on scams is available at **Appendix B and C**.

Please contact Senior Policy Officer **David Hofierka** at **Consumer Action Law Centre** on 03 9670 5088 or at david.h@consumeraction.org.au if you have any questions about this submission.

CONSUMER ACTION LAW CENTRE

Stephanie Tonkin | CEO

CHOICE

Rosie Thomas | Director, Campaigns and Communications

THE AUSTRALIAN COMMUNICATIONS CONSUMER ACTION NETWORK

Andrew Williams | CEO

Table of Contents

About Consumer Action

Consumer Action Law Centre (CALC) 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.

About CHOICE

CHOICE is the leading consumer advocacy group in Australia. CHOICE is independent, not-for-profit and member-funded. Our mission is simple: we work for fair, just and safe markets that meet the needs of Australian consumers. We do that through our independent testing, advocacy and journalism.

About the Australian Communications Consumer Action Network

The Australian Communications Consumer Action Network (ACCAN) is Australia's peak communication consumer organisation. The operation of ACCAN is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.

Executive Summary

Australian consumers are losing $8.5 million dollars per day[1] to scammers, through no fault of their own. To date, consumers have been paying for the losses because it has been left with industry to improve their systems and respond to their customers who have been scammed—the outcome has been inaction, victim-blaming and Australia becoming a soft target for scammers.

We welcome the Government committing to taking strong action to prevent scams and improve responses for victims. Yet the proposed regulatory framework outlined in the Scams – Mandatory Industry Codes Consultation Paper, will need substantial revision because it will not work effectively for consumers:

- It does not set clear guidance on when consumers will be reimbursed for their losses;
- It fails to set out clear, enforceable consumer rights;
- It does not contemplate a clear or workable process for how consumers can assert any rights or seek reimbursement;
- The lead in time for a code to become mandatory is far too long; and
- The definition of a 'scam' and 'digital communications platform' needs work.

The Consultation Paper rightly seeks to allocate responsibilities in relation to scams prevention and response across the banking, telecommunications (telco) and digital platforms sectors to incentivise all businesses with the power to prevent scams to take effective action. However, in seeking to allocate responsibility, the framework creates highly convoluted and unworkable processes for scams victims to seek redress – such as a victim having to go to internal dispute resolution not only with their bank, but also a telco company that they may not be a customer of and a digital platform – generally with limited information about what has transpired.

In mapping a scams victim's journey, it has become clear to us, and many others we have consulted with, that if you want to apportion liability (which we support subject to certain principles) then apportionment will only be workable if it sits alongside a mandatory reimbursement obligation on banks, subject to limited exceptions.

Primary objective of the proposed framework

Absent from the debate on scams in this country is the reality that, to be successful, scammers must breach the systems of banks, telecommunications and digital platforms that are supposed to protect customers' money and information. We consider the primary objective of the framework ('to set clear roles and responsibilities for the Government, regulators, and the private sector in combatting scams') to be similarly misguided. The striking and obvious exclusion is the absence of protecting consumers or any reference to improving the outcomes and experience of consumers who fall victim to scams.

This reflects and summarises a concern we have with the whole Paper – that it has not been developed with the goal of ensuring the prevention of scams and improving the experience of the individuals who are targeted by, or victims of, scams. Instead, the approach in the Paper establishes a safe harbour of sorts for industry, so the minimum standards (and limits of) business obligations are clear, whether or not the measures are effective in preventing scams or reducing scam losses. Currently, victims of scams are the ones who wear the burden of scam losses in almost all cases and it is difficult to say whether the proposed framework will significantly improve outcomes or experiences for victims.

[1] In Australia, victims reported a loss of $3.1 billion AUD (or approximately 2 billion USD) to scams in 2022 – Australian Competition and Consumer Commission, April 2023, '*Targeting scams Report of the ACCC on scams activity 2022*', Available at: https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf

In particular, we are concerned that the Paper fails to clearly address the allocation of liability for scam losses. The broader framework does not do this, despite it being the primary harm and outcome of scams for consumers. The Paper talks about general obligations of industry, and consumer rights to redress where these are not met, but it fails to explain what such redress would be and only vaguely alludes to redress being via internal/external dispute resolution processes. This approach also risks industry taking a tick box approach to compliance, and ultimately shifting blame and fault to the scam victim, rather than approaching the problem wholly with the goal of reducing losses to scams altogether.

Overarching principles based obligations

We support the overarching principle-based obligations proposed in the Paper, which we consider to be the strongest and most developed part of the proposed framework. That said, we are strongly of the view that a model that reimburses customers for scam losses, except in very limited circumstances, would be the only effective way to reverse the flow of scams from reaching consumers from the start. The overarching principle-based obligations to be set out in the *Competition and Consumer Act 2010* (CCA Act) must also be mirrored in the *Australian Securities and Investments Commission Act 2001* (ASIC Act) for consistency and to ensure focused regulation of the financial services sector, and in preparation for other financial services like superannuation and cryptocurrency becoming regulated under the scams framework.

Mandatory reimbursement is the only way to drive industry investment

Making banks liable for scam losses is the approach most likely to meaningfully disrupt scams, reduce scam losses and make Australia less attractive to scammers. A presumption of bank liability for scam losses is a far simpler, long-term and more effective model that would provide well-resourced businesses and sectors with the financial incentive to strengthen their own systems to detect, disrupt and prevent scams. Together with the reimbursement model, some level of apportionment can take place between the bank and other industries, subject to principles outlined below. Financial incentives for other industries that are further upstream in the scam business model (eg telcos, digital platforms) can be imposed, separate to dispute resolution between consumer and bank.

In contrast, the model proposed, that establishes checklists, limited transparency and the limits of industry obligations, will set a 'bare minimum, compliance approach'. This approach will leave loopholes for scammers to exploit – it is their business model to work around established systems – ultimately costing industry, Government and consumers much more in the long run.

Single complaints pathway for consumers

The consequence of the proposed 'ecosystem' approach to dispute resolution in the Paper is a system that's complicated and segregated, undermining the possibility of it working, especially for vulnerable consumers. Scams dispute resolution must create a single pathway to seek redress through both IDR and EDR for consumers after they have been scammed. A scams victim cannot be bounced around from bank to telco to digital platform at IDR, and then seek redress at multiple EDR services. This would cause great stress and fatigue for victims and place unrealistic burdens on EDR schemes. Further, many scam victims never have the full picture or access to the information on how the scam occurred.

Setting a list of requirements for banks, telcos and platforms to meet, otherwise they will be liable to customers, won't work due to information asymmetry and the complexity and sheer volume of scams. Under the proposal, it would be extremely difficult for victims of scams to identify whether a business has complied with their obligations under the codes and would result in scams victims never being sure if they have had a fair hearing.

The bank is the consumer's touchpoint and the place from where the money has been lost. In reality, this is where scams victims already go for redress – the Paper complicates this by introducing telco and digital platform IDR. It makes sense for all or the vast majority of scams IDR matters to be dealt with at banks. With a strong presumption

for banks to reimburse scam victims, all banks should be required to respond to customers with a resolution within a fixed compressed timeline of no longer than 5 days after it has been alerted to a scam by a customer (or a representative).

We concede that banks should be able to, once they reimburse a customer, recover a proportion of their losses from other industries without the consumer's involvement – but we remain firmly of the view that an apportionment mechanism must not prevent the fast-tracking of reimbursement of consumer losses or mandatory codes for the banks, telcos and digital platforms.

The need to fast-track the new mandatory scams codes

The paper is largely silent on a timeline, but we understand any substantial obligations will unlikely be imposed upon *any* industry until at least 2025. Put simply, this is far too slow, and consumers desperately need a mandatory framework to be in place and up and running before the end of 2024.

Individuals are suffering life changing losses every day. While collaboration between government and industry is very desirable, the framework needs to impose immediate deadlines upon the banking, telco and digital platform sectors, so scam prevention is treated with genuine urgency.

We strongly recommend that Treasury advise Government to fast-track the proposed timeframe for implementing mandatory obligations on industry. While we need to get the best possible, mandatory framework to stop scams in Australia, this also needs to happen fast.

We need strong mandatory and prescriptive obligations across all sectors

The proposed Codes require a 'scams process', but not the detail of what that process is. We need clear obligations on industry to develop scam detection, prevention and disruption measures.

The below is a sample of the experiences and what some of the people who have recently been scammed told us:

"I felt so embarrassed and ashamed that it had happened, I didn't tell anyone but my husband," Jo said. "I've spent many months and hours trying to get to the bottom of this, I've submitted so many complaints, I've written hundreds of emails, I've made so many calls, my bank always says "it's nothing to do with us, you transferred the money to a different bank, we can't help you", and the other bank says 'you're not our customer, we can't help you…" "You are just sent around in circles, it's like they do their best not to help you. "To me, if feels like they are aiding the scammers, the banks like to make you feel like it's your fault, and that's really hard when you are already feeling so dumb… "It's actually more traumatic -dealing with the banks and getting nowhere- than the actual scam itself."

"I was the victim of an invoice email scam and lost $20,000. In trying to recover my funds I contacted both the transferring bank and the receiving bank and their responses were effectively "we can't (won't) help you"

"We were caught in the infamous Hi Mum scam where we transferred $1850 into the scammers bank account. We quickly realised it was a scam and contacted our bank to stop the transaction. It took 8 weeks for the banks involved to follow up our complaint and it was only after contacting the Australian Financial Complaints Commission that we received a refund of our money."

"We hope by sharing our story of the financial, but also the emotional impact scams have on people, we can bring about legal change and force more responsibility on banks to protect the everyday consumer."

1. Mandatory and enforceable prescriptive codes

The framework needs to be governed by mandatory and enforceable prescriptive codes imposing high standards on the banking, telecommunications and digital platform sectors, that are enforced by empowered regulators

The banking, telecommunications and digital platform sectors are the three key industries that should have obligations imposed upon them in relation to scams. It is essential that meaningful obligations on these industries are made mandatory and enforceable as soon as possible. The current level of security across all three of these industries has proven insufficient to protect their customers from scammers, and this should not be tolerated.

In light of far-reaching consumer harms caused by scams, the Government should move to mandate rules as quickly as practicable for each of these industries – especially while consumers continue to bear the cost of scams.

Due to the pervasiveness and economy-wide impact of scams in Australia, we are supportive of a consolidated multi-regulator approach that builds upon and takes advantage of the existing regulatory framework.

The Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC), as the economy-wide regulators for financial services and consumer matters respectively, should take up central roles in the regulation and enforcement of mandatory scam codes via the following structure:

a. ASIC for banking[2] (and eventually all other financial services providers and digital assets (crypto), regardless of whether crypto is regulated as a financial product)

b. ACCC for telecommunications and digital platforms (and all others)

There is substantial benefit in establishing the ASIC and ACCC as the economy-wide scams regulators. These benefits include:

- Ensuring efficiencies in regulating and evaluating mandatory scam codes across multiple sectors of the economy. This will also have the effect of precluding parties engaged in scam activity from taking advantage of industry boundaries by structuring their operations to avoid enforcement action.
- Leveraging ASIC's decades of experience and unique expertise in the licensing, regulation and enforcement of banking and financial services, which are largely the frontlines in the fight against scams and also the last line of defence in protecting Australian's money.
- Building on ASIC's primary role and increasing expertise in emerging market that are growing frontiers for scams, including superannuation markets and crypto markets.
- Establishing the ACCC as the economy-wide scams regulator all other non-financial related markets, leverages its recognition as Australia's top consumer regulator, including its strong enforcement of the Australian Consumer Law (ACL) with the telecommunications sector, and its unique position to assess and respond to emerging regulatory issues affecting consumers in the digital platform sector.
- Establishing the ACCC as the single source of enforcement for non-financial related markets ensures that it has a uniform cross-industry purview wherever scam regulation may be required.
- Avoiding confusion regarding the Australian Communications and Media Authority's (ACMA) remit and the duplication of responsibilities which may arise should the ACMA be established as an economy-wide scams code regulator.
- Retaining and leveraging the expertise and knowledge of the ACMA when concerning telecommunications by embedding consultation processes.
- Leveraging cross-sector learnings to improve outcomes across industries.

[2] All banks including community owned banks, building societies, credit unions and commercial banks

- Leveraging the best existing enforcement structures and penalty regimes for cross-industry enforcement.

To give sufficient regulatory powers and oversight to scams regulators, and for consistency, we strongly recommend that the high level obligations proposed for the *Competition and Consumer Act 2010* be replicated in the *Australian Securities and Investments Commission Act 2001*, to ensure that ASIC can take enforcement action against banks and any future financial service providers that are designated by the Minister.

Mandatory codes

We are concerned that the Paper suggests that some industries such as digital platforms or telecommunications could be left to develop their own codes or be regulated under existing regulatory frameworks. Such frameworks have historically suffered from poor enforcement and penalty mechanisms and have failed to encourage compliance or deter bad practice. Until now, responding to scams has been left to industry to manage and as a result consumers are losing billions of dollars each year and suffering great harm.

From our experience, existing regulatory frameworks that are voluntary or co-regulatory in nature, such as the voluntary telecommunications industry codes that regulate consumer protections, have put industry's interests ahead of the needs of customers and have failed to protect consumers. For example, the Telecommunications Consumer Protections Code (TCP Code) contains a 'two-step' or warning process for compliance. The ACMA can only seek penalties for a breach of limited civil penalty provisions of the TCP Code,[3] such as a further breach the code after a 'direction to comply' is given by the ACMA[4], slowing regulatory responses to consumer harm. Furthermore, a breach of the code after the ACMA has issued a 'formal warning' is not enough to attract penalties.[5] Voluntary industry led regulatory frameworks such as these should not be modelled for scams if the government is serious about creating strong laws to protect people from harm.

The limited, existing, anti-scam codes and regulation that have been developed for the telecommunications sector has led to some benefits for consumers. Participating carriage service providers have blocked over 336.7 million scam texts since July 2022.[6] Additionally, we welcome the proposed development of the Sender ID registry in combatting harmful text scams. The incoming SMS ID registry will provide consumers with greater confidence when they receive important information via SMS and underpin the functioning of the SMS system. Establishment of the SMS ID registry needs to be expedited and made mandatory this year. Billions of scam phone calls and messages are still reaching Australians daily, which demonstrates that the millions of calls and messages that have been blocked are just a small proportion of the total, and compliance with and enforcement of voluntary scam codes is grossly inadequate[7].

Enforcement and penalties

The development of all mandatory scam codes should be accompanied by swift enforcement powers, supported by a strong penalty regime. This should include increases in the penalties proportional to the size of businesses, in addition to being based on the potential level of harm to consumers for breaches of the law. A strong penalty regime will help to encourage high industry standards, better reflect penalties in other service sectors and adequately disincentivise non-compliance.

The part-voluntary nature and levels of enforcement of existing anti-scam rules, which has to date been limited to the telecommunications sector, is not adequate or proportionate to the level of consumer harm being experienced by consumers.[8] Since June 2022, two telecommunications providers have paid infringement notices as a result of

[3] Telecommunications Act 1997 (Cth). 572M and Telecommunications (Infringement Notices) Guidelines 2022, 9
[4] Telecommunications Act 1997 (Cth). 121
[5] Telecommunications Act 1997 (Cth). 122(2)
[6] ACMA. 2023. 336 million scam texts blocked by telcos. Available at: https://www.acma.gov.au/articles/2023-11/336-million-scam-texts-blocked-telcos.
[7] The Age. 19 December 2023. 'Bombarded with scam calls and messages? There's a way to stop them?' Available at: https://www.theage.com.au/national/bombarded-with-scam-calls-and-messages-there-s-a-way-to-stop-them-20231219-p5eshi.html
[8] Telnyx Australia Pty Ltd paid a $106,560 infringement notice for breaching anti-scam legislation. This is the first monetary penalty paid by a telecommunications provider since the introduction of the anti-scam rules.

contravening anti-scam legislation.[9] Additionally, there have only been four other directions to comply, and a formal warning issued to other telecommunications providers who had previously violated anti-scam regulation.

To be effective against combatting scams, the ACCC and ASIC would need access to the broadest penalties (or even broader, for cases relating to multi-national companies with deep pockets) that they currently have under their existing enforcement regimes. This power could be further strengthened by incorporating the best practice enforcement mechanisms that have been adopted in other key areas of the Australian economy, such as in the energy sector, where penalties have been raised, segmented, and indexed to inflation to increase deterrence of contraventions.[10] Both under the ASIC Act and in the energy sector, fines and civil penalties are linked to a business' revenue which helps to incentivise providers to put more effort into ensuring compliance with legislation.[11]

Ensuring that penalties are sufficient to provide a deterrence to non-compliance is crucial to the establishment of an effective regulatory regime for scams which adequately disincentivises malpractice and consumer harm.

Prescriptive standards and obligations

Substantial and mandatory sector specific obligations are essential for the framework to have an impact upon the prevalence and cost of scams. While there are some very strong high-level principles proposed in the Paper, each sector has completely different problems and shortcomings in how they respond at present to scams, and obligations in law or codes need to address this.

One of our main concerns with the proposed obligations outlined in the Paper is the generality of them, which will make it difficult to establish the requisite standard expected of businesses and identify where the standard of conduct has not been met. A business has latitude to deem a scam prevention system or policy "reasonable", which would satisfy the proposed law, but fall far short of community expectations. This is the position we find ourselves in today, where in the vast majority of cases, businesses tell their own customers who fall victim to scams that they are meeting obligations and doing enough, despite the scam breaching the business' systems. To address this, in addition to the mandatory reimbursement component of the law, we recommend non-exhaustive guidance be included in the sector specific codes to provide specific examples of actions industry members are expected to take to comply with these obligations.

The possible sector specific obligations contemplated in the Paper offer some examples of appropriate guidance, but overall, it falls well short of the level of detail that should be included. We expect that many more obligations could be proposed by entities with more expertise than us, such as regulators of relevant industries. This is an area where we think that the Government also needs to push all industries to go much further than they have to date and ultimately ask whether what is proposed is enough.

In this submission, we provide examples of additional specific obligations that should be included in the sector specific codes, most notably for banking and digital platforms.

Banking sector specific obligations

We find it problematic that seemingly looser language is used for principle 1 in the Paper when describing the obligations of banks to prevent and recover payments via bank transfers, compared with other goals. We do not understand why the Government has decided to clarify that bank transfers should only be stopped or recovered "where possible", while all other specific goals listed under principle 1 are stated unequivocally.

[9] The media releases for these infringement notices can be found here: https://www.acma.gov.au/articles/2023-12/telnyx-breaches-anti-scam-and-public-safety-rules#:~:text=Telnyx%20Australia%20Pty%20Ltd%20has,scam%20and%20public%20safety%20obligations. https://www.acma.gov.au/articles/2024-01/medion-pays-259000-penalty-breaches-anti-scam-rules.

[10] AER. Stronger penalties demand energy businesses prioritise compliance with the law. 1 February 2021. Available at: https://www.aer.gov.au/news-release/stronger-penalties-demand-energy-businesses-prioritise-compliance-with-the-law

[11] AER. Stronger penalties demand energy businesses prioritise compliance with the law. 1 February 2021. Available at: https://www.aer.gov.au/news-release/stronger-penalties-demand-energy-businesses-prioritise-compliance-with-the-law

Under 'Response' on the table at page 20 of the Paper, there is a reference to banks being required to assist consumers to trace and recover funds, and for receiving banks to revert transfers within 24 hours. This is a positive step but, given the pace of payments today, we would like to see far more ambitious requirements here.

Based on challenges encountered by our clients following a scam, specific obligations for the victim's bank (sending bank), aimed at ensuring more stringent obligations, should include:

- Having a dedicated phone or other contact 'line' to assist people who have been the victim of fraud or scams, that is adequately staffed at all times, and other methods for consumers to report scams, such as via an app. Digital banking cannot be embraced by the banks if they are incapable of also dealing with the security issues it brings.
- Taking action to initiate recovery processes for scam payments within an ambitious timeframe (e.g. hours) set by the regulator.
- Proactively tell victims of scams about all avenues that may be available to them to seek compensation – such as via chargebacks.
- Reporting all confirmed scams to the police and the National Anti-Scam Centre (NASC).
- Keeping consumers regularly updated on the progress of recovery attempts and providing details explaining the outcome where unsuccessful.

Banks should also be required to inform each other, telcos and digital platforms where relevant, in real time, as they learn that their platforms were involved in a scam.

Obligations for receiving banks

A noticeable gap in current bank obligations is the role of banks housing the receiving accounts of scammers. This is how scammers gain access to the Australian financial system, yet currently victims of scams have no rights whatsoever against these banks and cannot even find out any details about the account to which their money was transferred – often cited to our clients as due to "privacy". This is routinely one of the things that clients calling our advice lines find most unjust and confusing.

The framework proposes receiving banks would have an obligation to process a recall request within 24 hours, but nothing more.

Specific additions that should apply to banks that receive scammed funds include:

- Reducing the timeframe for banks to process recall requests – scammers move money far quicker than the proposed timeframes, and banking platforms allow them to do so. If we are dealing with near-instant transactions, banks' systems must have safeguards that can be used at an equivalent rate, or they should slow down the system.
- Obligations around making further recall requests if scam funds have been transferred into other accounts. Banks tell our clients that funds will often be sent to many accounts near instantly. Obligations must require the first receiving bank to attempt further recalls where required and extend to those other banks involved.

2. Mandatory Reimbursement: Banks

We urge Treasury to consider the reimbursement model soon to be mandated in United Kingdom (UK), where banks will be responsible for reimbursing losses, unless consumers have been grossly negligent or are acting fraudulently.[12] This approach has the following significant advantages over the approach in the Paper because:

- Scam victims are provided with relative certainty, rather than a complex, opaque dispute resolution process;
- The bank is required to reimburse or provide a decision to the customer within 5 business days of the loss being claimed by the customer. The bank has the option to temporarily pause this time frame in limited circumstances, for example, to request further information from the customer to assess whether the claim is reimbursable;[13]
- Banks can determine disputes at IDR because the presumption is clear, and they can deal with the issue of apportionment later. Moreso, banks won't want to show their confidential policy or systems documents making the fairness of the dispute untenable.
- The demand on dispute resolution for both businesses and EDR schemes would be much lower, as it would only be relevant if the bank (which is far better placed to know whether it has grounds to dispute the outcome) considered it to have a basis to refuse reimbursement;
- Complaints costs and bank distrust would significantly reduce with certainty around responsibility for reimbursement and a far higher rate of reimbursement;[14]
- Disputes that did reach EDR would examine the actions of the consumer, making the process more navigable and transparent;
- The focus of the regime is on banks (and telcos and platforms – described below) effectively making their systems safer and impenetrable, as opposed to victim-blaming or creating a 'tick a box' approach;
- Vulnerability of the consumer is taken into account; and
- Banks would be incentivised to make their systems safer, as the threat of scams would lead to losses of its own bottom line – of which maximisation is the underlying goal for business.

3. Reimbursing vulnerable customers

Sector specific obligations need to be developed with the impacts on vulnerable customers front of mind, including those cohorts most susceptible to scams such as the elderly, culturally and linguistically diverse people (CALD) people and the disabled. Vulnerable consumers who are already facing significant financial, health and emotional challenges in their lives should not have to face an uphill battle to get their money back or identify relevant businesses or complaint pathways in the aftermath of being scammed.

[12] UK Payment Systems Regulator. 'Policy statement – Fighting authorised push payment scams: final decision'. December 2023. Available at: https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf

[13] 'APP scams reimbursement: Specific Requirement 1 (SR1) on Pay.UK'. December 2023. Available at: https://www.psr.org.uk/publications/legal-directions-and-decisions/app-scams-reimbursement-specific-requirement-1-sr1-on-pay-uk/

[14] In the UK under the still-voluntary bank reimbursement Code, 66% of scam losses were reimbursed in 2022. – UK Payment Systems Regulator 'Consultation CP22/4'. June 2023. Available at: https://www.psr.org.uk/media/rxtlt2k4/ps23-3-app-fraud-reimbursement-policy-statement-june-2023.pdf; This is compared to just 2-5% of scam losses being reimbursed in Australia – 'ASIC Report 761: Scam prevention, detection and response by the four major banks' 20 April 2023. Available at: https://download.asic.gov.au/media/mbhozopc/rep761-published-20-april-2023.pdf

Under the UK's new reimbursement model, the Payment Systems Regulator (PSR) has imposed extra requirements on banks to better assist and identify customers vulnerable to scams.[15] In the UK, a vulnerable customer is defined as 'someone who, due to their personal circumstances, is especially susceptible to harm – particularly when a firm is not acting with appropriate levels of care'. Accordingly, the PSR has imposed requirements for UK banks 'to take extra steps to ensure that vulnerable consumers are protected when making payments, and that the necessary tools are in place to prevent scammers exploiting consumers' vulnerabilities.'

The UK model also takes an approach where the expectation for reimbursement is even higher where the customer is experiencing vulnerability. The exception for customers acting with gross negligence (and the claims excess) does not apply where customers are experiencing vulnerability.

Like the UK, Australia should define and adopt a similar uniform and consistent approach towards assisting and reimbursing vulnerable customers who have been scammed and ensure banks are required to take 'extra steps' so that vulnerable customers are not targeted by scammers in the first place.

Mia's* story

Mia is a carer for her disabled child.

Last year, shortly after receiving a payment of slightly less than $3,100 from Centrelink, Mia received a call from someone claiming to work for her bank who advised her that her account had been compromised and she would receive a new card. The caller knew her name, date of birth and address, and advised her to transfer her funds into a new account which had been opened for her.

Mia believed the caller was from her bank because she had received a legitimate call a year earlier when her card had been compromised. Her bank had proactively reached out to let her know that a new card had been issued and she felt this call was very similar.

Immediately after transferring the funds Mia felt that the caller hadn't been quite right and called her bank's fraud number. After waiting for 45 minutes she gave up and drove down to her local branch. A staff member confirmed Mia had been scammed.

Mia contacted the receiving bank who told her they had frozen the account, but Mia's bank told her they weren't able to recover any of the stolen funds. She lodged an internal dispute resolution complaint but her bank refused to offer any compensation. She doesn't know how the caller had her personal details.

*Name has been changed

4. Fair, simple, fast and effective dispute resolution pathway for scammed victims

Our short answer to question 33 in particular, is no – we do not see a clear pathway for consumers to seek compensation under the framework.

The proposed model would be extremely difficult for victims of scams to be able to identify whether a business has complied with their obligations under the codes, due to unavoidable information asymmetry. It also presents a novel approach to consumer redress by sending the consumer to at least three different IDR points and three different EDR schemes. For example, how could a consumer ever know if a bank had information that put it on

[15] UK Payment Systems Regulator. 'Policy statement – Fighting authorised push payment scams: final decision'. December 2023. Available at: https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf

notice that a transaction they made was likely part of a scam? How could a consumer identify which telecommunications business allowed a scammer to use a bank's phone number?

The primary issues we see with the proposed complaint and dispute resolution process in the Paper are that:

- it would be extremely difficult for a consumer to know upon being scammed whether businesses in any sector had breached their duties, and sometimes may even have trouble identifying relevant businesses;
- it appears to contemplate scam victims navigating through multiple IDR and EDR with different businesses that were involved in the scam;
- it is very difficult to imagine how any dispute resolution process would be able to overcome likely information asymmetries between the parties, and scam victims would accordingly be extremely limited in being able to argue their own case;
- further, banks and other businesses will understandably want to keep their systems and policies confidential so they are not revealing their safeguards to the scammers, but this means the fairness of any dispute is undermined, unless you begin with a presumption of reimbursement;
- It is unclear on what basis a business would unilaterally determine their proportion of liability at IDR, and risks victims being sent on a referral roundabout; and
- even if dispute resolution processes could fairly and transparently identify a breach of the obligations by a business, it is not clear from the Paper if this would entitle scam victims to any remedy.

These problems are fundamental and go to the heart of the concerns we have with the framework. We urge the Government to take on the below recommendations that are some of the most important we make in the submission.

We propose the following model for a consumer to seek reimbursement for their scam losses:

1. A consumer is required to lodge an IDR complaint only with the bank institution(s) or financial service provider (FSP) where their funds were held or lost.
2. Scam-specific IDR is a simplified process with compressed timelines. We strongly recommend that the Treasury to advise the Government to adopt a similar IDR timeframe like the UK model of 5 days.
3. A strong presumption of reimbursement applies.
4. After a consumer has been reimbursed by their bank or FSP, an external mechanism for determining how to share liability between all scams code regulated entities can apportion liability and direct other entities to reimburse the bank or FSP.
5. If IDR fails, a single-door EDR needs to be available. The single EDR scheme can consider the actions of all scams code regulated entities. AFCA could be this EDR scheme.
6. The single door EDR can also be part of a regime for apportionment of liability for the loss. The consumer's bank or FSP should be the single source of remediation, with other contributing entities to 'repay' or in some way contribute funds to the bank or financial services provider.

The human impact of scams must be front of mind when developing the principles and systems of dispute resolution. Traumatised and confused consumers, whose lives in many cases have been instantly altered after they have been scammed, should not have to wait more than 5 days for their bank to make a decision and reimburse them for scammed funds after the bank has been notified of the scam. A compressed IDR timeframe is especially important for victims of scams who are already, or as a consequence of the scam, experiencing vulnerability and

may be unable to put food on the table as a result. After all, scammers are exploiting weaknesses in banking platforms to steal the funds of their vulnerable customers.

We would also strongly oppose any system requiring individuals to lodge multiple complaints to have a scam dispute heard. Consumers who are victims of scams are almost always under a significant amount of distress when they are scammed. They should not have to think about the complexities in identifying relevant businesses and navigating multiple EDRs in the aftermath. Some people we speak with still have no clear picture on how they were scammed, and this is quite conceivable for example, given the complexity of scams and the mass data breaches occurring all the time[16], only some of which are notified to affected consumers. Those consumers would only be able to prosecute their cases if they have access to expert resources to represent their interests.

The framework **must** only require consumers to lodge their complaint once to have all their rights for reimbursement fully assessed. In our view, as the need for the customer to contact their bank (or business from which the money was lost) will always be a reality of reporting scams (and the best chance of recovering any lost money), it absolutely makes sense for this to be the point of entry.

The below is an example of a scam scenario across banking, telecommunication and digital platforms that has been directly informed by the experiences of clients who have presented to our services. Navigating the multiple complaint avenues proposed in the Paper to try to obtain a remedy for such a matter would be highly unworkable for most consumers.

Sarah's story

Sarah is a single mother, with an intellectual disability and in receipt of Centrelink who was desperately running short of money to pay for essentials including food and medicine.

Sarah was groomed by a male scammer who cold-contacted her on Whatsapp (romance scam). Over a period of time and during online interactions the scammer groomed and tricked her into providing some of her personal details and her credit card number from one of the big 4 banks.

The scammer then sent her a link to a Facebook page for a business he said he ran, and groomed her into making several transfers of money she had accessed from her credit card account and buy now pay later loans to an account the scammer had helped her to set up. The scammer then assisted her to transfer the scammed funds to a crypto trading website as he convinced her it would immediately provide a financial return to assist her and her children.

Sarah's bank picked up the unusual transactions and called to query the transaction and promised to monitor her account. Despite this the transfers were processed. After she had transferred the money, she messaged the man for an update on the money she had transferred but she did not hear back from the man.

Shortly after, Sarah was cold-called from someone representing her bank's fraud team who advised that her account had been hacked. The number was spoofed to look like the bank's phone number. The caller confirmed Sarah's name, date of birth and address. She was advised by the scammer to transfer her remaining bank funds into a secure account which the bank had opened for her. Sarah was also talked through increasing her transaction limit from $1,000 to $5,000.

Immediately after transferring the funds, Sarah became suspicious and attempted to call her bank but was put on hold for 2 hours.

Sarah also received an email from her bank saying the transfer was put on hold for 24 hours and immediately sent a number of emails and requests via bank app asking her bank to cancel the transaction.

[16] For example, the Medibank, Optus and Latitude data breaches – none of which consumers are adequately compensated for or businesses are made liable for considering the harm from the potential misuse of their private information (e.g. from credential stuffing. See: https://www.abc.net.au/news/2024-01-11/the-iconic-payments-system-security-leaves-customers-vulnerable/103309260)

With the help of a community legal centre, Sarah initiated a complaint with her bank but they refused any liability.

Sarah has been assisted to lodge a complaint to the Australian Financial Complaints Authority (AFCA). Her bank has since said they were unable to recover the funds from the receiving bank and said they were not liable due to Sarah authorising all the payments and that they followed all their security procedures including calling her to check on the initial bank transfer.

Mapping Sarah's story to the proposed framework

The first, and most important thing for a victim of any scam involving a bank transfer to do is contact their bank as quickly as possible. The bank is the only entity that can possibly get their money back – something a telco or digital platform will never be able to do.

Presumably, the bank will then try to get their money back. At present this often takes many weeks or months before there is an outcome. If the victim's money was not able to be recovered, their bank would tell them about this, and then under the framework (or current banking laws) would perhaps be obliged to offer to help them make a complaint.

Under the model proposed in the Paper, the victim could now lodge a complaint against both their bank and a telco and digital platform. However, there may even be challenges in identifying which companies are involved. The call was spoofed, but it would be hard to know if this was due to inaction by the bank, or if it was an issue with their telco? If they responded to a fake ad online – which digital platform should they go to and how do they contact them? Alternatively, it could be a failure by another telco carrier to properly protect their infrastructure. It also may be that the bank used by the scammer had failed to meet their Anti-Money Laundering and Counter-Terrorism Financing (AMLCTF) obligations, and this allowed the scammer to gain access to the banking system.

This lack of information makes it hard for the individual to even know who to complain to in the first instance. If a consumer came to us and sought legal advice about their options, our only recommendation would likely have to be to commence the IDR process against both their bank, their telco and a digital platform. This would mean virtually every single scam victim will be making at least two to three complaints. This is not a desirable outcome for businesses or consumers.

5. A Single Door for External Dispute Resolution (EDR)

It is likely that under the framework proposed by the Paper, we would also be advising every scam victim who received an unsatisfactory IDR outcome to lodge disputes in relevant EDR schemes. For our hypothetical scam victim Sarah, under the framework proposed in the Paper, this would mean going to both AFCA and the Telecommunication Industry Ombudsman (TIO). Additionally, we currently do not have a sector appropriate EDR scheme to direct them to for any failures by the digital platform involved.

If the whole framework is predicated on the idea that scams require an ecosystem-wide response, it would follow that there is no point in EDR schemes undertaking an analysis limited to a single sector. It would not benefit consumers, and would make it near impossible to form a complete understanding of how a scam was allowed to succeed.

For any IDR process to offer a complete assessment of the satisfactory ecosystem response to scams, it would likely require extremely open and proactive sharing of information between businesses across different sectors. In reality, we think this is unlikely to ever be a comprehensive process – it is hard to imagine businesses in different sectors being fully transparent with one another about whether they made errors. Accordingly, EDR will still have a big role to play in resolving disputes.

Under the proposed framework, we struggle to see how any victim of a scam could be satisfied they have had a fair hearing without seeking review through EDR – and possibly even multiple EDR services, if (for example) the scam originated via a telco, but the money was lost by bank transfers. Requiring one (or more) complex EDR processes for every single scam where money is would create an unrealistic burden on EDR regimes.

In Sarah's scenario above, she would have to:

- lodge multiple IDR applications;
- retell her story – multiple times; and
- probably provide a range of documents and answer further questions from multiple EDR schemes.

For this framework to have any hope of success, we firmly believe that one EDR body would have to be equipped to critically assess the entire path of the scam, from first contact to final loss. As the financial services industry is where a consumer would first complain, at present this would make AFCA the most logical choice for this.

6. A mechanism for apportionment of liability

We would support other industries being required to share the bill for the cost of scam losses, with a critical caveat that this cannot slow down any progress in establishing mandatory reimbursement and obligations under the scams regulation. Apportionment would make for more comprehensive incentivisation in scam prevention across the ecosystem. If introduced alongside the presumption of mandatory reimbursement, introducing a cross-sector apportionment mechanism in Australia's scams regulatory framework could make our system one of the most effective, globally. However, this is a process that should not require a consumer to enforce their rights under the code. It must happen after they have been reimbursed.

Victims of scams should not have to wait while industries duke it out over who failed the consumer more. In some cases (such as the bank impersonation scam described above) some of the businesses that are at fault may not even have a contractual relationship with the victim.

Principles for apportionment

While the mechanisms and negotiation over the apportionment system are for government and industry to settle (with consultation), there are some principles that must be observed if we are to introduce a robust scheme. Apportionment is not a new concept, and we can adopt lessons and effective components from other sectors.

- The scams regulation and mandatory reimbursement must be introduced without delay. Apportionment may need to be introduced down the track, as negotiated between government and industry.
- The presumption of reimbursement must sit alongside the apportionment. The presumption simplifies the entire dispute resolution process and reimbursement occurs first between the sending bank and the victim.
- After reimbursement the bank can be compensated by receiving banks, telcos, platforms (and other sectors like crypto as regulation develops) without the victim's input.
- The settings of apportionment must be fine-tuned to driving incentives for businesses to stop scams.
- Apportionment might be developed on a more systems/high level basis informed by the regulator about the performance of a sector, rather than for every case by case which could be difficult to administer. An analogous example could be the knock-for-knock arrangements between insurers in motor vehicle disputes.[17]

[17] See: https://treasury.gov.au/sites/default/files/2019-03/ch9.pdf

The National Anti-Scams Centre could be an effective agency to oversee, implement and monitor the apportionment arrangements due to its position within the ACCC, access to information and work across sectors to disrupt and respond to scams.

7. Broader definitions needed - scams and digital communications platforms

The Government should not shy away from defining sectors subject to scam codes broadly. Scammers are known to exploit the weakest links available to them. If companies that are vulnerable to scammers are not captured by these codes, that is where scammers will turn to next. The risk of excluding companies from responsibility is greater than any perceived regulatory burden risk from defining sectors too widely.

Aligning the definition of 'scam' with 'fraud'

The main risk we see in aligning the definition of scam as a subset of the legal definition of fraud is the requirement in the proposed scam definition to prove intent on the part of the scammer. In the absence of a reimbursement presumption, proving mental intent would pose a significant barrier to a consumer proving they have been scammed—an apparent unintended drafting consequence.

An essential part of the legal crime of fraud is intent – it must be proven that the perpetrator has intentionally deceived the victim.[18] This has been established as a reasonably high bar by the courts, even when the perpetrator is actually identifiable and present before the court.[19] Applying a similarly high bar to establish that someone has been scammed could pose a problem, particularly considering many scams involve criminals that are not identifiable or are otherwise beyond reach of the law.

Instead, the question asked should be whether the customer transferred funds or provided their credential but was deceived in sending them, or that they sent funds for what they thought was a legitimate purpose but was in fact fraudulent. While in many cases dishonesty or an intention to deceive may be reasonably clear from the facts, such a requirement should not act as a barrier in less clear-cut cases or provide an area of contention between consumers/regulators and affected industry participants. It also should not risk reducing the scope of the obligations of relevant industry members under this regime.

We expect that most scams involve an 'invitation, request, notification or offer', however as these terms remain undefined in the Paper, as above, we urge the Government to test this against all reported types of scams to ensure that this aspect of the proposed definition will not create unexpected barriers. Some other examples we also urge the Government to consider include:

- Ensuring the inclusion of 'dishonest' in the definition does not create problems. If there are doubts about whether an entire scammer's story was fabricated, will this impact the classification of a scam? We would also be concerned if this required proof of subjective dishonestly by the scammer (see comments above about proving state of mind);
- Extortion or threat-based scams – if a victim is directed to make a bank transfer by a scammer (rather than asked to), will this conduct fall within one of these categories? Is it still a request or a notification? Is it dishonest?

The substantive impact of all scams will always involve the scammer obtaining a financial benefit or personal information, or both.

[18] *Criminal Code Act 1995* (Cth), Schedule 1, Part 7.3

[19] See for example the discussion in Alex Steel, "General Fraud Offences in Australia" [2007] *UNSWLRS* 55, available at: https://www8.austlii.edu.au/cgi-bin/viewdoc/au/journals/UNSWLRS/2007/55.html

Consistent with our points above, a primary goal of defining scams should be ensuring all scams now and in future are picked up by the wording. Should the regulation not take a presumption of reimbursement model, then victims of scams must not face unreasonable or impractical barriers in proving they have been the victim of a scam when seeking to assert their rights under the new laws.

Digital communications platforms should be more broadly defined

The proposed definition of a 'digital communications platform' is too narrow in scope and should be defined more broadly. Carving out certain digital platforms, or particular functions, from digital platforms, will create confusion for consumers about where their consumer protections start and end, as well as creating potential weak links for scammers to exploit. It is also out of step with international approaches to scam consumer protection.

The Government should expand the proposed definition to reflect the scope of digital platforms covered by the Digital Platform Services Inquiry, which includes electronic marketplace services.

'Primary function' is too ambiguous

It may not always be clear how to sort digital platforms into the proposed categories, as many digital platforms offer multiple services. For example, many digital platforms have introduced their own online marketplaces alongside other functions, such as Facebook. More and more platforms are seeking to provide all-in-one services such as WeChat.

The Government should remove the reference to 'primary' from the definition to avoid confusion, to ensure that all digital platforms that simply provide the services listed are captured.

Online marketplace services should be captured by the Framework and be subject to industry-specific obligations

The proposed definition of a 'digital communications platform' excludes digital transaction-based platforms like online marketplaces. The Framework obligations and proposed industry-specific obligations should apply to all digital platforms, so that there aren't gaps in the ecosystem that scammers can exploit – particularly where there's the ability for the seller and buyer to communicate directly with each other. Consumers should be able to expect the same protections no matter the platform because there's little distinction between them for consumers.

It's unclear if online marketplaces like Facebook Marketplace would be captured by the proposed definition, so it should be made clear that these types of services are included. Facebook Marketplace requires a user's Facebook profile to either post items or message sellers about buying items. The digital communication functions and marketplace functions are integrated seamlessly. As one CHOICE supporter explains:

> *"I bought two products, a camera and a laptop, that were advertised on Facebook Marketplace. These were unrealistically cheap and I would never have bought them except I trusted Facebook not to display scam ads. I received emails notifying me that the items had been shipped and giving me tracing info. When I remembered, much later, to check, I found the tracking info indicated that the items had been delivered. What I believe happened was that I was sent, in each case, a small metal tube. I took no note of this and just thought it was some kind of fake item from Wish."*

Facebook is one of the two major digital platforms in Australia[20], and it is critical that any regulation works for all aspects of how consumers interact with these platforms and all services offered by the platform to users. Including one function of a digital platform (e.g. communication) while excluding another (e.g. online marketplace) will lead to consumer confusion about what is and what is not protected and offer less certainty to businesses.

[20] Digital Platforms Inquiry - Final Report, ACCC, June 2019 https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf p.2

Encompassing all functions of a platform, including online marketplaces, in the definition of digital platforms will also encourage better cohesion in the anti-scams strategy of platforms like Facebook. Businesses will have more certainty about obligations across the platform, opposed to needing to develop anti-scam strategies piecemeal as different functions are slowly included.

This would also mirror more closely what is happening in similar jurisdictions. The United Kingdom's Online Safety Act imposes legal obligations on, amongst other services providers, 'user-to-user services' which includes online marketplaces.[21] Similarly, the European Union's Digital Services Act regulates the obligations of digital services including marketplaces.[22]

As outlined, the proposal fails to address significant losses to scams on these platforms. In 2022, the ACCC reported a loss of more than $8 million to classified scams, where scammers use classifieds and auction sites to advertise popular products for sale at a cheap price.

The Government should include online marketplaces in the initial round of code development under a broader 'digital platform' definition.

All services and functions of digital platforms should be captured

The definition of a digital communication platform should extend the obligations to all functions and services, including those provided off-platform. For example, Google display ads can be served on non-Google web pages as part of an advertising system. These ads must be subject to the same anti-scam regulations as the ads that are shown on Google itself. If they aren't captured, this will create implementation complexity and continue to expose consumers to scam ads.

It's currently unclear from the definition if the proposed Framework and sector-specific obligations will apply to services not covered by the digital platforms definition provided by digital platforms where the digital platform also provides services that meet the definition. The Government should amend the definition of digital communications platforms to explicitly include all services provided by digital platforms, including off-platform services.

8. Interactions with ePayments Code and unauthorised transactions

As outlined above, the definition of a scam should be cast as wide as possible. Therefore, the ePayments Code should be subordinate to the scams regulation for clarity and consistency and to ensure that no cases fall between the gaps.

We generally support the apparent intent of the Government not to restrict or impact the allocation of liability for unauthorised transactions under the ePayments Code. Where consumers are already entitled to reimbursement under the ePayments Code, this should not be reduced. However, if intending for the definition of a scam to exclude all fraud involving unauthorised payments, the Government should engage closely with AFCA and banks to agree the practical boundaries of cases where the ePayments Code applies and to ensure consistent practice.

Consumer Action has been involved in cases before AFCA where the question of liability under the ePayments Code was disputed by both AFCA case managers and banks, despite our strong view that it should have applied. Examples include cases that involve phishing or remote access and there also appears to be inconsistency across different institutions on the classification of these scams (or fraud – depending on who you speak to).

[21] UK Online Safety Act: What Does It Mean for Your Business?, Ogletree Deakins November 2023, https://ogletree.com/insights-resources/blog-posts/uk-online-safety-act-what-does-it-mean-for-your-business/

[22] Questions and Answers: Digital Services Act, European Commission, December 2023 https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

Clear definitions and the presumption of bank reimbursement will assist where the application of the ePayments Code is less clear. After our examination and analysis of 50 AFCA final determinations between 18 September 2023 to 12 December 2023 (nearly one determination per day) in relation to scams (or potentially fraud), we found that consumers were successful in only 4 matters (approx. 8% of determinations). The bank was entirely successful in 42 and largely successful in the remaining 4.

We acknowledge the changing environment that AFCA needs to navigate. However, some themes that arose out of our analysis of decisions – again, that call for brighter lines and definitions for AFCA to take into account – include:

- AFCA regularly places the onus of proof on the consumer to prove that the transaction was unauthorised, despite the customer saying they did not authorise the transaction. AFCA determination 942440 states: "*the onus is on the customer to show, that on the balance of probabilities, they did not authorise the transaction*". However, there are other AFCA decisions (for example AFCA determination 938799), that seem to follow a different approach. In our view, the ePayments Code clearly places this onus on the bank as set out in AFCA determination 938799.
- AFCA has taken the view that it can't review the adequacy of the banks fraud detection system: see AFCA determination 960896.
- Where the scams involved bank impersonation and the bank's spoofed phone number or a fake login was used, a number of AFCA decisions seem to assume that the customer always authorised the disputed transactions, voluntarily disclosed passcodes or knew that the scammer could see them making the transaction. However, AFCA determination 938799, for example, went the other way and determined that putting your password into a purported bank website was not "voluntary disclosure".

In these cases we would strongly argue that under the ePayments Code, these should be unauthorised transactions for which the customer is entitled to reimbursement. However, if this is not the approach consistently taken by AFCA or banks, there runs a risk that if excluding these cases from the definitions of a scam, those considered to have 'voluntarily disclosed' their passcode would suddenly be left worse off than any other scam victim. It could leave these people without any entitlement to reimbursement under the ePayments Code, and outside any rights they have under the scams framework.

We reiterate that we do not consider this should be the case, but it may be the reality based on misguided application of the ePayments Code.

Accordingly, to prevent confusion and misapplication under the new scams regime, the appropriate legislative amendments should be made by Government, including ensuring that the ePayments Code is made mandatory and operates in line with the overarching scams legislation, to prevent any scam victim falling though the gaps, such as in the circumstances discussed above.

Other ePayments Code considerations

Separately, there are aspects of the industry obligations under the scams framework – such as the banking specific code as proposed in the Paper and in our recommended obligations – that would be valuable to expand to cover unauthorised transactions like phishing or remote access. In particular, it is essential for digital platforms or telcos to be obliged to do everything they can to prevent calls, texts, advertisements or emails that lead to phishing or remote access risks.

In addition, we see no reason why receiving banks should not be obliged to urgently deal with recall requests and assist with attempted fund recovery where someone has fallen victim to a phishing scam or a remote access scam. While these are likely unauthorised transactions, there is still presumably a bank account on the other end that is being used by a scammer.

Receiving banks should have obligations in these situations as well if they do not already exist, and our recommendation regarding liability for loss, could also be appropriate to incentivise increased security efforts and friction in the payments system. While unauthorised transactions may differ in that customers are often entitled to a refund in any event, this is not always acknowledged by banks and the process to reimbursement can be very difficult for consumers.

Similarly, the experience of consumers in recovery attempts for some unauthorised transactions can be the same as for scams. In these cases, many of the obligations on sending banks should also apply just the same, such as being required to report any information to other banks as quickly as possible, and enabling customers to report scams and prevent further transactions quickly.

9. Timeframe: Fast-track mandatory codes for banking, telcos and digital platforms

Many of the proposals in the Paper are still clearly in their early stages, with the new regulatory regime envisioned to be finalised in 2025. Consumers desperately need an effective framework to be implemented before then. The Paper also appears to contemplate a long lead time designed to cater to the timeframes industries have indicated suit them. For example:

- The Paper and other comments by the Government suggest that the self-imposed timeline proposed by the banking industry to introduce confirmation of payee has been treated as acceptable without further inquiry, despite its absence being a known weakness with the payments system for years.
- While ACMA's progress on developing a SMS ID registry is welcomed, we are concerned that the scheme is intended to be voluntary until at least late 2024.[23]

Conceptually and practically, these are not groundbreaking concepts or changes – in other countries industry players are already taking such measures for years.[24]

Parts of the Paper appear to suggest that development of sector specific codes would be a heavily collaborative process. We support collaboration with industry, but in areas like telco regulation where industry has had final say about commitments it makes (such as with the TCP Code), it has led to years of shortcomings that let down consumers.[25]

Yet, it appears the industry will be given the time they say they need to implement new measures and these forms of technology without question, while consumers continue to wear scam losses in the interim. Accordingly, there needs to be more forceful action to bring security against scams in these industries up to standards that the community rightfully expects.

Information sharing requirements

We strongly support the need to urgently establish mandatory scam information sharing obligations upon businesses in regulated sectors. Sharing information about scams will make the possibility of preventing and disrupting them far more realistic and is key to achieving consistent and concerted ecosystem-wide efforts to preventing scams. The experiences of our clients make it apparent that currently communication and information

[23] The Hon Michelle Rowland MP, Minister for Communications media release: 'SMS Sender ID Registry set to protect more Australians from scammers'. December 2023. Available at: https://minister.infrastructure.gov.au/rowland/media-release/sms-sender-id-registry-set-protect-more-australians-scammers

[24] Major banks in the UK have already established confirmation of payee functionality: https://www.psr.org.uk/publications/consultations/cp22-2-confirmation-of-payee-requirements-for-further-participation-in-cop/, and in Singapore the SMS ID registry is already mandatory: https://www.sgnic.sg/smsregistry/overview

[25] CALC media release. 'Consumer fail: New Telco Code proposal delivers little for vulnerable consumers'. January 2024. Available at: https://consumeraction.org.au/consumer-fail-new-telco-code-proposal-delivers-little-for-vulnerable-consumers/

sharing between banks, and between banks and other sectors, is not done particularly well, contributing to significant delays in response times for consumers. There needs to be consistency in terms of the circumstances where information about scams is shared, how information is shared and the format in which it is provided.

The Government needs to require businesses to make information sharing a standard part of their response to all scams, and businesses should report on this to the regulator. The success rates of scammers in many situations would dramatically decrease if the first time a bank account was identified to be associated with a scammer, all transfers to it from other banks were blocked, and the account was frozen to allow for investigation. While a lot of these transfers happen very quickly, the time leading up to the transfer can vary greatly, meaning that advance warning can help prevent many scams. In banking, sharing intelligence about suspected blocked scams should also be encouraged.

ASIC and ACCC need to be empowered to act in this area. If data (eg information sharing rates) indicate that a business is not providing information as quickly or as often as other businesses in the sector, this should be grounds for the ASIC or the ACCC to investigate and impose penalties, where appropriate. Public accountability should also be considered – such as the option of naming businesses that are falling short on data sharing.

It is very important that businesses are properly motivated to take information sharing seriously. Businesses should also work to share information in the fastest way possible. For example, if banks can share information that might help other banks stop scams fastest via the fraud reporting exchange, it should be the expectation that all data is fed into this system.

Accountability needs to work both ways as well, and so we also welcome the statement in the Paper that businesses would be expected to take reasonable steps to act on scam intelligence shared with it by another business. Businesses should be accountable to customers who fall victim to scams on this front. For these obligations to be effective and there to be transparency in dispute resolution, there again needs to be a way for victims of scams and the EDR body to learn whether any information relevant to the scam was available to the business when the scam occurred.

Evidence that a business is systemically failing to act quickly on, or making use of, relevant information it is receiving from other entities about scams as soon as possible, should also be the basis for strong enforcement action by regulators.

Scams regulation for the superannuation and cryptocurrency sectors

We agree that superannuation and cryptocurrency sectors should also be the next industries to be brought within the regime as a priority. Bringing both these industries in should not be contingent on progress or implementation of the new laws on banks, telcos or digital platforms first. It is already clear that scammers will target the point of least resistance, so if banks do improve their performance, other industries holding funds will likely see increased attention from scammers.

For most Australians, superannuation is one of their biggest assets. It is therefore an attractive target for scammers. There are many different forms of scams circulating the $3.5 trillion super system, including:

- Self-managed super fund (SMSF) scams, where a scammer facilitates a member to create a self-managed super fund. The member's super is then transferred into a bank account controlled by the scammer, or the member is convinced to transfer some or all of the SMSF balance to the scammer.
- Post-preservation investment scams, where a member of post-preservation age is convinced to withdraw some or all of their funds and transfer them to the scammer.

- Early access scams, where a scammer encourages a member to fraudulently access their super under extreme financial hardship or compassionate grounds, and then the scammer takes a cut, or steals the funds or the member's identity.

Recent super fund data breaches and high value scam losses demonstrate the need for urgent government intervention to protect people's hard earned retirement savings. There are common sense system-wide improvements that the super industry could adopt to make it harder for scammers to steal people's super. However, these require a degree of collaboration and adoption that the superannuation industry has not initiated to date. It is therefore essential that the government takes further steps to incentivise super funds to fight scams via the development of a super industry anti-scam code. For more detail on recommendations for this consultation specific to superannuation, please refer to the submission made by Super Consumers Australia.

Crypto platforms should also be subject to the same obligations as banks in regard to scams from the moment the licensing regime the Government is developing comes into effect.[26] A significant (and growing) portion of scams reported to us now involve crypto platforms in some way, and it is an area where consumer awareness is low.

Accordingly, any obligations on banks relating to reimbursement and apportionment of liability of losses may not only be appropriate to replicate for the crypto industry, but also for the superannuation industry, where money is taken by scammers from super accounts.

Finally, as the Paper treats consistency between industries as an important factor, while it is important that progress is made on all fronts, we stress that delay due to an excessive focus on consistency between sectors just means consumers unfairly wear the whole of the burden of scams for longer. This should not be an acceptable outcome for the Government, nor for consumers and the Australian people who have made it clear that they overwhelmingly demand quick and effective action by their Government to prevent their money and livelihoods being put at risk by scammers.

[26] Crypto platforms is intended to have the same meaning as digital asset platforms in Treasury's *Regulating Digital Asset Platforms* consultation paper, October 2023

APPENDIX A – Digital Platforms

Possible digital communications platform specific obligations

We welcome the proposed sector-specific obligations on digital platforms. These obligations should be mandatory and should be strengthened further to address the harms caused by the failure of digital platforms to address scams exploiting their systems.

Prevention

Authentication and verification of users

We support the proposal to require *"a provider of a digital communications platform to implement processes to authenticate and verify the identity and legitimacy of business users to prevent users from selling or advertising scam products and services on the platform."*

The proposal should be strengthened by detailing the specific processes digital platforms must (at a minimum) take to authenticate and verify the identity and legitimacy of all users who sell or advertise on their platform (excluding personal sellers on marketplaces). This will ensure that these processes are effective and standardised across the industry. For example, specific authentication and verification processes could include:

- Step 1: application for advertising and selling etc. licence including 100 points of identity documents
- Step 2: review by digital platform
- Step 3: close monitoring of ads, posts or websites placed by a user on a digital platform during trial period
- Step 4: final approval
- Step 5: re-approval required every 2 years

If the obligation does not detail specific processes, the obligation should be amended to provide that process must be effective. More concrete guidance on processes required should then be included in regulator guidance.

The Government should amend the obligation to cover all users selling or advertising products or services on the platform, not just business users.

A CHOICE investigation found a number of advertisements across Google, Facebook and Instagram promoting scam retailer websites, including examples highlighting issues with Google's policies to prevent scam ads, as some advertisers did not appear to be verified.[27] Many of the scam ads seen by CHOICE were advertised by individuals, not companies.

> Penelope's* story
>
> I bought a pair of sandals online after seeing them advertised and apparently well reviewed on Facebook. I am now $59.00 poorer and there is still no sign of the sandals. A click to the 'website' discloses an error message as does trying to send an email. I have been scammed.

[27] Scam ads rampant on popular social platforms, CHOICE, September 2023, https://www.choice.com.au/shopping/online-shopping/buying-online/articles/scam-ads-on-facebook-google-instagram.

* Name changed for privacy.

Personal sellers on marketplaces

The Government should also require digital platforms to monitor red flags from personal sellers who are on marketplaces. Personal sellers are users with personal accounts who are not affiliated with a business and do not advertise their products. The red flags should include:

- a user has been noted for fraud elsewhere online;
- a user sends a high volume of direct messages to different accounts;
- a user impersonates a company in any aspect of their account;
- a user messages many sellers about their listings immediately after they are posted (suggesting bot behaviour)

Digital platforms should regularly monitor their marketplaces for scam accounts. In cases where red flags were identified, digital platforms should immediately suspend accounts and notify users who were affected. The platform should then investigate the suspected account to determine whether it is fraudulent within 5 days of identifying a suspected scam account.

As scammers are evolving, digital platforms should also be required to consistently monitor and analyse scammers' behaviour online to effectively identify fraudulent accounts.

Amelia's* story

I am a mother of two young children and last year posted an ad on Gumtree to sell a breastpump. I was contacted by a girl named Jess (AU telephone number) who wanted to buy the item and asked if we could transact via Australia Post. She provided screenshots of how the transaction works, several screenshots to show that she was attempting to transfer payment and a link to an AusPost website. The website stated that I was receiving $300 and asked for my bank card details. I thought this was normal as I provide my bank card details to receive refunds in retail shops. I then received a text from the bank saying there was unusual activity on my account. I rang them immediately and they advised that over two transactions, I had lost $9100. The bank also charged me two international transaction fees. My total loss was just under $9400. My bank advised that they had to allow the transaction to process as per Mastercard rules. I tried relentlessly to get onto Mastercard and only had success via Twitter of all places. They directed me back to the bank. I submitted a police report and tried everything I could to hold the transaction pending investigation to no avail. I submitted a dispute to the bank, which they declined. I then escalated it and they declined again stating that I had provided my one time pin. They never requested or considered the circumstances surrounding the transaction. My dispute is now with AFCA. I experienced disassociation as a result. I was extremely upset for months afterwards and I am still mentally impacted by what happened and the lack of support offered from the bank. What happened to me goes against the ASIC ePayments code and what it is trying to achieve - ultimately to promote consumer confidence with online transactions. I had the opposite experience. I have not been protected in any way - including my daily transaction limit (which was $3000) or any insurances to cover a payment for something I never received.

Recommendations:

The Government should strengthen the proposed obligation to verify and authenticate all users (excluding personal sellers on marketplaces) by:

1. Detailing the specific processes digital platforms must take to authenticate and verify the identity and legitimacy of users (excluding personal sellers on marketplaces).

2. Amending the obligation to cover all users selling or advertising products or services on the platform (excluding personal sellers on marketplaces).
3. Require digital platforms to monitor and immediately act on individual users' accounts with red flags on marketplaces.

Detecting and disrupting risky interactions

We support the government to require: *"a provider of a digital communications platform to have in place processes and methods to detect higher risk interactions, and take action to warn the user, block or disrupt the interaction, or take other measures to reduce scam activity, content or profiles such as blocking or disabling accounts based on shared intelligence*."

The Government should strengthen this obligation by defining 'higher risk interactions', as it is unclear what falls under this category. The definition should be broad and capture common characteristics and behaviour of scammers when they interact with users. The definition should be regularly reviewed and adjusted as scams develop to ensure that people are still protected.

This obligation should also be strengthened by defining the processes and methods required (at a minimum) to detect and disrupt risky interactions. This could include:

- monitoring for red flags as outlined in the marketplace section;
- taking action (i.e. blocking, suspending and/or deleting) against scam accounts promptly once flagged by a consumer, regulator or an industry;
- responding to consumers and regulators promptly;
- flagging an identified scam account with other digital platforms and the NASC;
- monitoring for similar fraudulent content closely in the 5 days following the detection

If the obligation does not detail specific processes and methods, the obligation should be amended to provide that processes and methods must be effective. More concrete guidance on processes required should then be included in regulator guidance.

The Government should strengthen the obligation by requiring digital platforms to act within an hour after detecting a higher risk interaction with a scammer to warn users, block or disrupt the interaction, or take other measures to reduce scam activity, content or profiles.

Once an interaction between a user and a suspected scammer has been disrupted, a digital platform should also follow up with the user to inform them about what happened and if any further steps should be taken.

Ben's* story

Google Play Games where there are videos and statements of cash payments for playing games [*Google Play allows advertisements of games that offer cash payments for playing them*]. After playing the required number of games I received a cash payment approval and a request for a processing fee of $3.00 which I promptly paid only to be told I was now on a waiting list with 10,0000 people in front of me in their payment queue. I contacted Google Play who said my claim did not meet their Scam criteria for a refund. I contacted the game developers via their published email address, a Gmail account but the email bounced No user found. I have exposed about 20 Google Play Games that promise Cash payments but deliver nothing but excuses for non payment. Google needs to be held accountable for Games that are so called Google Play approved.

Recommendations:

The Government should strengthen the proposed obligation to detect and disrupt risky interactions by:

1. Defining 'higher risk interactions'.
2. Requiring digital platforms to act within an hour after detecting a higher risk interaction with a scammer to warn users, block or disrupt the interaction, or take other measures to reduce scam activity, content or profiles.
3. Requiring the digital platform to follow up with the user about the outcome and further steps that may need to be taken.

Preventing hacking and restoring user accounts

We strongly support the requirement that *"a provider of a digital communications platform must have in place processes and methods to prevent user accounts from being hacked by scammers, and to restore user accounts to the correct users in a timely manner."*

The Government should strengthen the obligation by detailing the processes and methods digital platforms must (at a minimum) use to prevent user accounts being hacked, which could include:

- blocking or disrupting the interaction of scammers with users,
- taking other measures to reduce scam activity, content or profiles such as disabling accounts based on shared intelligence, before they have the opportunity to scam users.
- providers of over-the-top messaging services (such as WhatsApp) must also identify, trace and block scam messages, similar to the requirements that apply to telcos in relation to SMS messages.

If the obligation doesn't detail specific processes and methods, it should be amended to provide that processes and methods should be effective. More concrete guidance on processes required should then be included in regulator guidance.

The obligation should also specify a timeframe to restore users' accounts, such as within 48 hours.

Recommendations

The Government should strengthen the proposed obligation to prevent hacking and restore accounts by:

1. Detailing the processes and methods digital platforms must use to prevent user accounts from being hacked.
2. Specifying 48 hours to restore user accounts.

Information sharing

We support the obligation that *"a provider of a digital communications platform must have in place effective methods or processes to identify and share information with other digital communications platform providers and the NASC that a user operating in Australia is likely to be or is a scammer."*

The proposal should be strengthened to require digital platforms to share information within three hours of becoming aware that a user is likely to be or is a scammer, as timeliness is critical in detecting and disrupting a scam. Similarly, the NASC should quickly communicate information to other businesses and organisations, such as banks and telcos where relevant.

The proposal should be strengthened by detailing what information is the most helpful for disrupting scams which should be promptly shared with other digital platforms and the NASC. This information could include:

- details of the suspected or confirmed scam activity
- user names and/or emails an account was registered with;
- how many people were reached;
- the type of scam;
- what actions a digital platform is going to take;
- whether people were scammed;
- what victims of a scam were told by a digital platform.

Recommendations

The Government should strengthen the proposed obligation on information sharing by:

1. Requiring digital platforms to share information within three hours of becoming aware that a user is likely to be or is a scammer.
2. Detailing the types of information that should be promptly shared with other digital platforms and the NASC.

Acting on likely scams

We support the obligation that: *"a provider of a digital communications platform must have in place effective processes to act quickly on information that identifies a user or interaction is likely to be or is a scam, including blocking or disabling the account being used by the scammer and taking down the fraudulent content.*

The Government should strengthen this obligation by requiring digital platforms to have effective processes for monitoring for, and acting on, similar users/similar fraudulent content once they become aware of the scam. This will ensure that the scammers are not simply able to copy-and-paste the fraudulent content to a new ad or account once the first ad or account has been taken down. We note that automation technology (including generative AI) means that scammers will quickly be able to create similar new ads. Verification, as detailed above, will also help prevent new accounts by the same scammer.

The obligation should also require digital platforms to act within an hour or less of becoming aware of the information.

Recommendations:

The Government should strengthen the proposed obligation to act on scams by:

1. Requiring digital platforms to have effective processes for monitoring for, and acting on, similar users or similar fraudulent content once they become aware of the scam.
2. Requiring digital platforms to act within an hour or less of becoming aware of the information.

Response (obligations to consumers)

Methods for consumers to take action for suspected compromised accounts and scams

We support the obligation that "*a provider of a digital communications platform must ensure that its platform has user-friendly and accessible methods for consumers to take action where they suspect their accounts are compromised or they have been scammed."*

A user should be able to take immediate and effective action when they believe they have been scammed. A digital communications platform must have methods that are easy to use when someone is stressed or vulnerable. This should include dedicated, adequately resourced and accessible processes to report scams, including clear pathways for support and redress.

The obligation should be strengthened by specifying the methods digital platforms must provide for consumers to take action. This should include requiring digital platforms to offer phone support so consumers are able to speak to a person who can offer help and support, rather than being directed to a chatbot or asked to fill in a form. Digital platforms should also be required to provide ongoing support for scam victims as they navigate the redress process. This obligation will ensure that consumers have support and agency.

The Government should specify that digital platforms must respond to consumers within an hour or less of the consumer using the method to take action.

Recommendations:

The Government should strengthen the proposed obligation to take action for suspected compromised accounts and scams by:

1. Specifying the methods digital platforms must provide for consumers to take action, which should include a phone option to speak to a person.
2. Requiring that digital platforms must respond to consumers within an hour or less of the consumer using the method to take action.

Additional Code obligations for digital platforms

Preventing the hosting of fraudulent ads

The Government should introduce an additional obligation to require digital communication platforms to prevent the hosting of fraudulent ads on their platforms, as per the United Kingdom's Online Safety Act[28]. The Act places a legal duty on certain digital platforms to prevent paid-for fraudulent adverts appearing on their services. Currently, digital platforms are not incentivised to take effective action on fraudulent ads as they charge fees to run the ads. This could be a significant revenue stream for some digital platforms given the volume of fraudulent ads we see. Introducing strong penalties for failing to prevent fraudulent ads will incentivise digital communication platforms to ensure that the advertisements hosted on their platforms are legitimate.

Accessible, searchable ad libraries

The Government should require digital platforms that run ads to maintain an accessible and searchable ad library for users and organisations to cross-check ads. This means that if a user is unsure about an ad they will be able to determine if a similar ad has been taken down for fraud previously. Meta's ad library is a good example of a user-friendly ad library, but Google's Ad Transparency Centre does not allow keyword searching, only searching by registered advertiser. This makes finding scam ads by keyword search impossible.

Recommendations

The Government should include additional obligations to:

1. Require digital communication platforms to prevent the hosting of fraudulent ads on their platforms.
2. Require digital platforms that run ads to maintain accessible and searchable ad libraries.

[28] Major law changes to protect people from scam adverts online, Department for Digital, Culture, Media & Sport, Home Office, The Rt Hon Chris Philp MP, Julia Lopez MP, The Rt Hon Nadine Dorries MP, and The Rt Hon Damian Hinds MP, March 2022, https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online

APPENDIX B – CHOICE nationally representative and supporter survey key results

Banks:

- 95% of people in Australia say that banks should be legally required to quickly follow set steps to assist people who have been scammed.
- 90% of people in Australia say that banks should be legally required to confirm the name matches the account to which money is being transferred to.
- 88% of people in Australia say that banks and financial institutions should be subject to strong penalties like fines if they fail to take appropriate steps to detect and prevent scams.
- 85% of people in Australia say that banks should be legally required to prevent the withdrawal of funds that are likely to have been received as the result of a scam.
- 74% of people in Australia say that banks and financial institutions will not protect people from scams, unless they are forced to do so by law.

Telcos:

- 86% of people in Australia say that telephone, mobile and internet companies should be subject to strong penalties like fines if they fail to take appropriate steps to detect and prevent scams.
- 81% of people in Australia say that telephone, mobile and internet companies will not protect people from scams, unless they are forced to do so by law.
- 71% of people in Australia say that telephone, mobile and internet companies can't be trusted to do enough to stop scammers.

Digital platforms:

- 90% of people in Australia say that social media and digital platforms such as Google, Facebook, Twitter / X should be subject to strong penalties like fines if they fail to take appropriate steps to detect and prevent scams.
- 88% of people in Australia say that social media and digital platforms such as Google, Facebook, Twitter / X will not protect people from scams, unless they are forced to do so by law.
- 88% of people in Australia say that social media and digital platforms currently don't do enough to protect people from scams such as allowing scams to be advertised or promoted.
- 83% of people in Australia say that social media and digital platforms such as Google, Facebook, Twitter / X can't be trusted to do enough to stop scammers.

Reference:

"CHOICE Consumer Pulse September 2023 is based on an online survey designed and analysed by CHOICE. 1,035 Australian households responded to the survey with quotas applied to ensure coverage across all age groups, genders and locations in each state and territory across metropolitan and regional areas. The data was weighted to ensure it is representative of the Australian population based on the 2021 ABS Census data. Fieldwork was conducted from 29 August to 18 September 2023."

APPENDIX C – June 2023, CHOICE nationally representative survey key results

Attitude to scams:

- Almost 8 out of 10 (79%) people fear for other people in their life that they might not spot a scam.
- 88% of people believe that scams have become more sophisticated or harder to spot recently.
- 84% of people admit that scams make them more cautious doing anything financial online.
- Support for greater government intervention is high; 80% of people agreeing that the government should legally force businesses to do more to stop scams.
- 64% of people worry they could lose money to a scam.

Reference:

"CHOICE Consumer Pulse June 2023 is based on a survey of 1,087 Australian households. Quotas were applied for representations in each age group as well as genders and location to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was conducted from 7th to 22nd of June 27, 2023".