WEstjustice

25 January 2024

Scams Taskforce
Market Conduct and Digital Division
Treasury
Langton Cres
Parkes ACT 2600

Sent by email: ***scamspolicy@treasury.gov.au***

Dear Scams Taskforce

We are grateful to submit to the *Scams – Mandatory Industry Codes* consultation paper. As a community legal centre based in Melbourne's Western Suburbs, we have been positioned since 2021 to witness firsthand the severe impact that scams can have on the most vulnerable members of the community.

Our brief submission is intended to highlight some of the recurring issues we are seeing under the status quo (the "current approach to addressing scams") and offer our preliminary views on the Proposed Scams Code Framework. We have also joined a range of consumer advocate organisations nationwide on an additional submission on the consultation paper. This submission is intended to be complementary to that more substantial response to the Consultation Paper questions.

To forecast the remainder of our submission, we support mandatory and enforceable codes of a high standard but consider there is a central lack of detail for reimbursement of consumers. If the code is aimed at not just preventing scams, but also enforcing better outcomes for the victims of scams, then we believe a mandatory model premised on presumptive reimbursement will ensure the best outcomes for consumers through an escalation in standards to detect and prevent scams. This would need to be supported by clear IDR and EDR pathways in those limited cases where the presumption of reimbursement is disputed.

Our recommendations below are focused on vastly improving the models of fairness and safety for banking, telco and digital platform consumers and we urge the government enshrine any next steps with legislation. Anything less would risk presenting a heavily convoluted consumer experiences that leads to many of the same poor outcomes currently facing scams victims.

About Westjustice

Westjustice is a human rights and community legal centre in the Western Suburbs of Melbourne servicing the local government areas of Maribyrnong, Hobsons Bay and Wyndham, and the broader western suburbs community with a collective population of almost a million people. We provide free legal advice, representation, education, community development, advocacy, and systemic reform across four impact areas: people experiencing economic injustice; people experiencing family and gender-based violence; youth; and culturally and linguistically diverse (CALD) communities. Our service area incorporates the fastest growing and most multicultural communities in the country (as at the 2021 Australian Census).

Our services and programs focus on prevention and early intervention in the cycle of economic

precarity, criminalisation, violence and housing insecurity to produce benefits for the people we work with and save government significant investment in downstream impacts of social problems.

We regularly encounter members of the public who have been victims of scams through:

- Our Settlement Justice Partnership (SJP), an outreach program delivering civil law services to people from refugee backgrounds in situ at two Western suburbs settlement agencies;
- Our Consumer Advice and Advocacy Program (CAAP), a clinic funded by Consumer Affairs Victoria and open to members of the public experiencing disadvantage;
- Our Restoring Financial Safety (RFS) project, an outreach program which provides legal and financial counselling services to victim-survivors of economic abuse;
- Our International Students Employment & Accommodation Legal Service, delivered in partnership with Study Melbourne.

Profile of Our Clients

The clients we have assisted who have become victims of banking fraud have overwhelmingly (over 95%) come from culturally and linguistically diverse backgrounds. Recurring trends have included:

- in many cases, a low-level of digital and banking competency and English literacy, which may make them less adept at identifying potential scam indicators such as typographical errors in fraudulent messages; less likely to receive warnings about scam types and trends in an accessible format or language;and more dependent on the assumed expertise and authority of banks or other institutions. This can lead to elevated risk of falling victim to a impersonation scam where criminals purport to be from the customer's bank.

- clients experiencing family violence, which can manifest as pressure or coercion from a family member to contribute money toward a scam, or as a client falling victim to a scam while already under the significant cognitive and psychological load of managing their safety.

- clients living with an intellectual disability, which may also mean additional risk that scam warnings are not received, and that there is heavy reliance on the bank's authority or expertise.

Since 2021, the most common cases we have seen impacting our clients have been investment scams, followed by romance scams, impersonation scams and accommodation scams. The losses we have seen have ranged between $500 and $25,000, with losses of approximately $4,000 on average.

We note that the most recent ACCC Targeting Scams Report noted that people from CALD backgrounds made up almost 5% of all reports but almost 10% of all losses, with a 36% increase in overall losses in 2022.[1] We anticipate that due to the language barriers that present for a person from a non-English speaking background, this severely understates the true figure in terms of number of people affected and losses.

While the losses our clients have seen are lower than the reported average, this is generally a reflection of their low levels of savings and disposable income. They are more likely as a result to

[1] Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on scams activity 2022,*April 2023. Accessed at https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf on 12 January 2024.

face difficulties with recurring but essential living costs such as rental bonds, moving expenses, vehicle maintenance, mortgage repayment increases, and school fees.

Profile of the Most Significant Issues – Industry Response

At the **prevention** stage, we have observed the following issues:

- Private and public institutions (including all industries proposed to be covered by enforceable codes in the first phase of this process) offer confusing or inconsistent information about their methods of contact (for example: whether they use SMS or telephone calls, how they will validate themselves);

- Inconsistent use by industry (including banks) of existing 'Do Not Originate' lists to prevent fraud by impersonation;

- Continued fraudulent calls and SMS's received through telecommunications providers, notwithstanding the introduction of C661:2022;

- Opacity as to how digital platforms and online marketplaces identify and prevent fraudulent activity, including impersonation and identity theft;

- Opacity as to how suspicious bank accounts (or account activity) are promptly scrutinised by banks;

- Institutional education and awareness campaigns do not connect directly to the first-language media or platforms that CALD groups (particularly recently-arrived communities) use (including digital spaces like WhatsApp groups, but also community radio or faith organisations).

At the **point of being scammed** (ie., when a person transfers money to a scammer through their bank), we have observed that:

- The wording and design of in-app warnings for making banking transactions is often lacking, in some cases using jargon or intermediate vocabulary, and failing to provoke concern or pause on a customer's part;

- There has been widespread use of real-time payments, including to new payees, without any holds for new or unusual transactions;

- There is presently no industry wide confirmation of payee requirement (noting the ABA's November 2023 announcement that a system will be implemented across 2024 and 2025.);

- We have encountered situations where a client is a known customer of their bank who is registered as requiring special assistance or support (due to disability or access issues) and has consented to this - yet there is no support to identify or pause suspicious account activity.

At the **point of after-care** from banks, we have identified that:

- Significant barriers can apply to banking customers who require the assistance of an interpreter to communicate with their bank. This has included situations where an interpreter is not available in the first instance, but where no proactive attempts are made to return the customer's call once an interpreter is available, onerous authentication

requirements prior to an interpreter being provided, and inappropriate use of family members as interpreters;

- Customers can have difficulty knowing where to urgently raise a scam depending on the bank. This can include difficulty making prompt contact with the right department on a phone tree, or being bounced between a physical branch and a call centre to address an enquiry;

- There is no standard mandated procedure for the attempted recall of funds sent to a fraudster from one Australian ADI to another ('scams' are undefined by the current *E-Payments Code*, but that Code is explicit they are not captured by its provisions to recovery of mistaken transactions);

- Most pressingly, there is presently no clear obligation under Australian law for banks to compensate scam victims, irrespective of the manner by which the fraud was carried out (ie., whether it involved threats, phishing, payment redirection, grooming or other methods that deprived the consumer of agency over the transaction) and irrespective of whether there have been failings of the kind summarised above.

Our Feedback on the Mandatory Codes Model

Structure

Noting that the exact detail of the sector-by-sector obligations under mandatory codes will be crucial to their effective operation, we **support** the establishment of an overarching regulatory framework under the *Competition & Consumer Act* that more prescriptive industry-specific codes give practical effect to.

At page 8 of the Paper, it is stated that other sectors could be designated in the future by the Minister (including online marketplaces, which we have identified in our casework as places where fraud can regularly occur).

Scammers are likely to go where weaknesses in an existing system are and will do so rapidly. This is a particular risk with essential everyday market or financial platforms like superannuation and online buying and selling. We suggest that, even if urgency and resources did not allow for additional industry codes to be set up at this time, the overarching regulatory framework's high-level obligations apply to exchanges, non-ADI payment providers, superannuation funds and online marketplaces that have a certain amount of annual turnover.

Definition of a 'Scam'

We partly **support** the definition of a scam put forward in the Paper.

Our primary concern is that any definition not inadvertently carve out individuals who fall victim to scams (for example, by restricting it to scam type, scam medium, or getting into the nuances of whether an individual can be said to have 'authorised' the transmission of personal information or financial benefit).

We flag the following aspects of the definition wording:

- the use of "dishonest". It is unlikely that in most cases the victim of a fraud (or indeed, a bank, telco or digital platform) will be unaware of the true knowledge, belief or intent of the person inducing a fraudulent transaction. We are also aware of situations in which scam victims have given money to individuals who themselves are being defrauded. For this reason we suggest that the definition avoid any interpretation that requires victims to establish the mental state of a scammer.

- whether the definition effectively captures threats or extortion where this is used to induce the scam transaction. We suggest that the additional use of the word "demand" could be included, to encapsulate those scams.

- lastly, we suggest that the legislation somehow clarify that a "request" or "notification" should include communications that ask an individual to verify credentials such as passwords in order to steal these (ie., phishing).

Were these to be addressed, we are satisfied the definition is sufficiently broad to capture a range of behaviour.

Noting common misconceptions or mis-uses of the word “scam” of the kind described at page 9 of the Paper, we also suggest that the legislation should distinguish that a “scam” does not include:

- an ‘unauthorised transaction’ for the purposes of the *E-Payments Code;*

- ‘misleading and deceptive conduct’ for the purposes of the *Australian Consumer Law;*

- various other forms of unauthorised access to personal information or accounts other than by way of a scam (ie., hacking or cybersecurity attacks).

We think this clarification is important so that victims are not diverted into the wrong stream for rights and remedies where they are the victim of wrongful or illegal conduct.

Proposed eco-system wide obligations under the CCA.

We are largely in agreement with the proposed eco-system wide obligations, but believe that in finalising these Treasury and the ACCC must give serious consideration to at what level consumer remedies will be enshrined for people who have suffered loss for a scam (ie., a presumptive right to compensation from one's bank). Our view is that setting out this expectation in legislation now will ensure that Industry Codes are not diluted in the future.

A further relevant consideration is the extent to which CCA provisions need to set out an expectation for how different sectors will remedy or compensate breaches between themselves (ie., the allocation of reimbursement to a customer).

We believe it is essential that any arrangements for redress where different sectors have failed to meet their scam detection or prevention obligations are easy for a consumer to navigate and do not lead to a person being repeatedly redirected between different services providers who each blame one another for the loss (for example, their bank and their telecommunications provider).

If these processes will not be set down in legislative amendment, then at the very least the industry codes should have consistent ''mirrored'' provisions for establishing the process for apportionment of liability.

Effective EDR for multiple sectors

Our biggest concern, as above, is that any scheme avoids our client base having to approach successive different EDR providers to have a complaint resolved.

As one EDR scheme is unlikely to make determinations about members of another EDR scheme, thought should be given to some kind of cross-sector External Dispute Resolution arrangement for scam matters involving multiple sector participants, which could be convened on either a standing or 'as needs' basis and be comprised of existing ombuds or delegates from the current schemes to share relative expertise and make findings about shared responsibility for failing to prevent a scam loss.

We consider that if such a ''cross-EDR body'' was essentially looking to efficiently and fairly resolve matters which would be coming to at least one EDR scheme in any event, the associated costs are likely to be minimal, particularly if it was housed in one ombudsman's capacity (ie., AFCA receives the complaints and can engage with other sectors).

Sector-specific codes and standards

Noting that we and other members of the consumer sector hope to have the opportunity to consult and feedback on draft codes later in 2024, Westjustice makes a few minor observations at this time.

Telco Obligations

Our biggest concern is that scammers are continuing to use telecommunications provider's networks for fraudulent phone calls, and that numbers associated with legitimate organisations continue to be spoofed. A code that recognises that telcos have active obligations to prevent this where possible, and gives direct remedies to consumers, would be welcomed.

Noting that telecommunications providers themselves are often impersonated by scammers, we think it would be prudent for an industry scams code to also require telcos to provide clear, consistent guidance on how they or their service suppliers will contact their customers.

We consider that establishment of an industry code for telcos should also involve Ministerial direction under section 125AA of the *Telecommunications Act 1997.*

Banking Obligations

The proposed banking obligations would address a number of the key issues which we summarised above. However, we also recommend:

- An obligation on banks to publish clear, consistent guidance on how they contact their customers;

- That any obligation on banks to take "appropriate action" to warn a customer are fleshed out to contain Effective Warning obligations similar to those set out in the United Kingdom Lending Standard Board's *Contingent Reimbursement Model Code for Authorised Push Payment Scams*, noting the expectation that such warnings be understandable, clear, impactful, timely, and specific;

- That any obligation on user-friendly and accessible methods to take action on a scam outline specific ways in which this should be enabled (for example, interpreter access, appropriate training or support to identify family violence risk, a ''no wrong door'' approach to notifying a bank);

- Most importantly, that the requirements for how and when banking customers are compensated for scam losses are explicitly set out in the Code. Westjustice advocates a system whereby customers should be compensated for their losses by their bank in the first instance, **excluding** a situation where there has been 'gross negligence' by the customer over a certain monetary amount (ie.,$5000.00). This could encompass situations where a customer is explicitly warned they are making a payment to a scam but choose to proceed, or where a customer who has previously been compensated then pays money to an identical or very similar scam.

- Lastly, we note that we have seen situations in which the sums lost to scams arose under consumer credit contracts. Examples include the provision of credit card details to impersonation scammers, and consumer loans taken out by people who are prospective or ongoing victims of investment or romance scams. The obligations on banks should be clear that in these situations relief for a customer should include presumption of waiver in most circumstances (as opposed to compensation).

We also consider that the industry code should emphasise that as part of the existing legislative requirement to assess requirements and objectives for a consumer who applies for a credit contract, a bank must be alert to any red flags which indicate the customer may be at risk of being scammed and that these will justify further inquiries and verification prior to approval.

Digital Platform Obligations

To ensure account integrity and minimise the risks associated with impersonation, we also suggest that digital platforms are required to have clear, accessible information on how they will contact a user.

Otherwise, our chief interest is in seeing that any obligations which apply to digital platforms and hold them accountable for criminal use of their services are suitably robust. We strongly urge that ACMA develop any applicable industry standard, rather than allowing the industry to develop such a code itself. As it stands, we are concerned as customer advocates that digital platforms regularly inhibit an ability of an affected person to raise an issue directly or escalate an unsatisfactory response, compared to telcos and banking providers.

Lastly, we note the ACCC's ongoing Digital Platform Services Enquiry is currently considering a very wide ambit of digital platform trends and practices and is not set to issue its final report until 31 March 2025.

If there is a longer-term body of work that will involve developing a more expansive regulatory architecture for digital platforms which encompasses scam obligations, we ask that work on prescriptive standards for banks and telcos is not delayed by this and that if need be these are finalised first, with digital platform obligations to be introduced at a later date.

The Appropriateness of Civil Penalties

While Westjustice supports appropriate penalties where legal obligations are being ignored by the regulator, we recognise that actions to bring such penalties are often relatively rare and strategic.

We maintain that a presumption to compensate a scammed customer under the law and applicable industry codes is the most effective way to provide direct and effective remedies to the public and ensure that a constant focus on preventing and combatting scams is a part of everyday business and innovation for banks, telcos and digital platforms.

Comments on Other Models

We note the models summarised in Attachment A, and make the following comments:

- We **strongly endorse** any legislative and code-based anti-scam structure being supported by a Reimbursement Scheme where customer money is generally reimbursed by that customer's bank, with some restrictions based on a customer's bearing clear responsibility for that loss (ie., where the customer has been negligent). The UK scheme has specific timelines under which a customer can expect a decision on reimbursement (15 business days from reporting a scam to one's bank in ordinary circumstances, with an upper deadline of 35 business days in exceptional circumstances), and confines allocation of liability in varying degrees between the customer's bank and the receiving bank for the funds.

- We do not have any issue in principle with a reimbursement model's allocation involving *other* sectors where there is a real suggestion that a non-bank organisation has enabled or contributed to the loss. However, it is imperative that this not delay or complicate the outcome for the affected customer given the significant personal and financial impact of scam losses. Notably, the UK scheme separates out the decision on whether and how much a customer is to be reimbursed from the decision on allocation of liability. This means, in other words, that a customer does not have to wait for companies to reach accord among themselves before receiving relief.

- We do not have any issue in principle with a 'waterfall' approach akin to that proposed in Singapore that assesses banks in the first instance as having the first line of responsibility as the custodian of customer monies, then looks to other organisations, but we emphasise that co-investigation and dispute resolution between banks and non-bank sectors should not come at the expense of prompt initial decisions about customer compensation.

- Additionally, we would not want to see a situation where unambiguous matters are regularly sent to EDR because (for example) a bank does not have an argument against the customer's right to reimbursement but believes it could gain a more favourable decision on who must provide that reimbursement at the EDR stage. The UK scheme sets out a basis under which banks should settle their own disputes (including arbitration if needed). While it is theoretically possible that all scam reimbursement decisions could go direct to EDR and have a decision on apportioning liability made alongside a decision on customer reimbursement by an external panel, it is likely that such a scheme would be inundated extremely quickly, continuing to strain existing ombudsman schemes from which it would be drawing resources.

- One alternative to reimbursement being determined and applied each time through the negotiation of multiple businesses would be a combined fund which participants (banks, telcos and digital platforms) paid into and which an affected customer could directly apply to. Such a fund would need to be carefully managed to ensure it had sufficient reserves to cover refundable scam losses, and that industry contributions reflected proportionate responsibility for prevention and

response to scams. It is possible that civil penalties which involved a breach of the CCA provisions (and similar civil penalties, such as those for an organisation allowing serious or repeated privacy breaches) could involve payment into such a fund.

Thank you for your consideration. If you have any questions about this submission, we can be reached on 03-9749-7720 or joe@westjustice.org.au. We would be more than willing to discuss our practice experience and recommendations with you further, or at any public hearings that may be conducted on the issue.

Sincerely,

Caitlin Caruana
Acting CEO
WEstjustice