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

24 December 2025

Joint Consumer Submission – Scams Prevention Framework draft law package and position paper

Thank you for the opportunity to provide feedback on the package of Scam Prevention Framework (SPF) consultation materials published by Treasury on 28 November 2025. This is a joint submission made on behalf of:

- Consumer Action Law Centre
- CHOICE
- Financial Rights Legal Centre
- Financial Counselling Australia
- Westjustice
- Consumer Credit Legal Service WA
- Financial Counsellors' Association of WA
- Consumer Policy Research Centre
- Victorian Aboriginal Legal Service
- David Niven, Scams Solicitor

We also support the separate submission made by the Australian Communications Consumer Action Network (ACCAN) to this consultation.

We welcome the step forward this consultation represents. However, for the Scam Prevention Framework to deliver on its promise of world leading protections for Australians, Government must plug the holes in its coverage. Government must also be

genuinely ambitious in the actions it mandates the ecosystem of SPF businesses take to genuinely detect, prevent and disrupt scams.

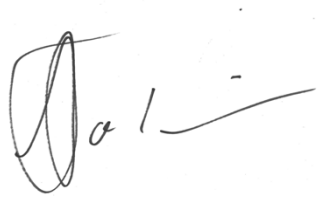
Crucially, the final SPF must guarantee access to fair compensation for victims when businesses fail to meet their obligations. The current proposal will not deliver this outcome, and we call on Government to lead the design of a functional and genuinely consumer-focused dispute resolution framework.

We stand ready to work with Government and industry to make the Scam Prevention Framework a system that truly protects Australians from scams.

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

Yours Sincerely,

CONSUMER ACTION LAW CENTRE



Stephanie Tonkin | Chief Executive Officer

Contents

Joint Consumer Submission – Scams Prevention Framework draft law package and position paper

Executive Summary

Scam losses in Australia are enormous and persistent, with the ACCC reporting over $2 billion lost in 2024 and losses rising in 2025. Consumers, especially vulnerable consumers, are bearing the brunt of this harm.

The Government's Scam Prevention Framework (SPF) promises a valuable step forward, but delays, gaps and deficiencies in its design mean Australians will remain exposed to scams for years and may never see a dispute resolution framework that delivers fair outcomes.

Key Issues and Recommendations

1. Timing: Delays Are Costly and Harmful

The SPF's full implementation is now pushed to the end of 2027. Every delay means continued harm. Immediate steps are needed:

- Mandate interim Actionable Scam Intelligence (ASI) obligations: Require businesses to maintain and uplift current information-sharing practices and act on publicly available scam intelligence.
- Introduce urgent protections now: Stronger hardship obligations for banks and a full ban on crypto ATMs.

2. Scope: Coverage Is Too Narrow

The proposed designations leave major scam channels untouched. Email services, online marketplaces, dating apps, app stores, and gaming platforms are excluded, despite being high-risk. This piecemeal approach undermines the SPF's effectiveness. Government must:

- Expand the definition of digital platforms to include these services.
- Future-proof the SPF by adopting broader definitions, similar to the UK and EU, to capture emerging technologies.
- Signal next steps now: Commit now to expanding the SPF to cover digital payment platforms and superannuation sector as a priority.

3. Code Obligations: Lift the Bar

Greater prescription and ambition in code obligations is required to genuinely move the dial on scam losses. Obligations must:

- Set clear, enforceable standards beyond existing industry practice.
- Clarify what constitutes reasonable steps and avoid unreasonably weakening protections based on complex calculations of proportionality.
- Embed vulnerability: Require businesses to identify and act on consumer vulnerability.
- No opt-outs: Consumers should not be able to waive scam protections, as this creates a systemic weakness.

4. Dispute Resolution: Put Consumers at the Centre

The proposed multiparty Internal Dispute Resolution (IDR) model is unworkable and risks leaving victims to navigate complex processes alone.

- Implement a fast-track small claims process for low-value scams.
- Create a central IDR body to coordinate multiparty complaints and deliver a single, clear outcome.
- Set strict timeframes: IDR outcomes within 15 days.
- Ensure transparency and fairness: Guardrails against low-ball offers and outcomes are reported and monitored to identify systemic issues.

A consolidated list of recommendations in this submission is provided at Appendix A.

1. SPF implementation delay is harmful and should be minimised and mitigated

1.1 Scam losses and harms are ongoing

The Australian Competition and Consumer Commission (ACCC) reports that scams losses in Australia are increasing in 2025[1] after more than $2 billion was lost across 2024[2].

Consumer Actions Law Centre's frontline data backs this up, showing scams consistently impacting our clients. In fact, we saw an increase of approximately 50% in scam related inquiries and services in August-September 2025 when compared to June-July.

Vulnerable consumers are being acutely impacted by ongoing scam harm

Those who can least afford it have experienced significant harm and losses to scammers over 2025. Our frontline services over the last 6 months have seen:

- Reimbursement from banks continues to be zero or very minimal.
- Vulnerability risk factors in almost all cases, including age, disability, domestic violence.
- Many cases of banks enforcing loans and debt which are the result of scams, resulting in extreme financial hardship.
- People being locked out of their banking services and accounts for protracted periods.
- Wide differences between the banks in their detection and disruption capabilities which means inconsistent outcomes for scam victims.
- The immense psychological toll with many people experiencing shame and self-blame, which can isolate people from seeking help.

The impact on vulnerable consumers is also reflected in ACCC data. In November the ACCC reported significant increases in scam losses for people experiencing disability, who speak English as a second language, with a 50% increase in scam losses for First Nations people[3].

[1] https://www.accc.gov.au/media-release/australians-report-nearly-260m-in-losses-as-shopping-scams-surge
[2] https://www.accc.gov.au/system/files/targeting-scams-report-2024.pdf
[3] https://www.accc.gov.au/media-release/australians-report-nearly-260m-in-losses-as-shopping-scams-surge

1.2 Further implementation delays must be avoided and risks of existing delay must be managed

Implementation of the Scam Prevention Framework (SPF) has already been significantly delayed. As indicated in the December 2024 Treasury Regulatory Initiatives Grid[4], designation of the SPF sectors was anticipated to occur in Q3 2025. A robust framework for the SPF sector codes, rules and dispute resolution were also intended to be operative in the first half of 2026.

As set out in the consultation's position paper, Australians will now be waiting until the end of 2027 for a functional SPF.

The Government must prioritise the implementation of the SPF and take meaningful steps to mitigate the risks and harms created by the staggered and delayed implementation proposed in the position paper. In particular:

- The delay of actionable scam intelligence (ASI) creates a significant risk of decreased intelligence sharing.
- Staggered implementation of internal dispute resolution (IDR) and external dispute resolution (EDR) will cause confusion and harm for consumers that should be managed.
- Lack of general protections before the full SPF comes online requires the immediate implementation of urgent interim scam harm minimisation solutions.

Delay to Actionable Scam Intelligence

Actionable Scam Intelligence is a crucial component of the SPF. The proposed delay will lessen the SPF's effectiveness.

We note that prior to full implementation of ASI, businesses will still be obliged to act on intelligence that they hold or may receive (position paper page 7). However, prior to the commencement of obligations under the SPF to report and share ASI, there is nothing that requires businesses to undertake a minimum standard of ASI gathering or sharing. This risks a decrease in information gathering and sharing between businesses as the obligation to act on any intelligence is turned on in advance of an obligation to seek or share information.

Any decrease of information flows to fight scams should be avoided and requires Government to mandate in the interim that, at minimum, businesses maintain and uplift current practices of information sharing and also act on publicly available sources. Businesses should be required to act on an expanded prescribed list of publicly available scam intelligence from commencement of the SPF including:

[4] https://treasury.gov.au/publication/regulatory-initiatives-grid-december-2024

- All Australian authorised deposit-taking institutions websites and customer alerts.
- Australian Securities and Investments Commission (ASIC) and ACCC websites.
- The International Organization of Securities Commissions (IOSCO) investor alerts portal.

Staggered IDR and EDR implementation

There is a significant risk of miscommunication, confusion and uncertainty for consumers associated with the delay of EDR commencement. Further guidance and guardrails are needed to prevent consumer confusion as to their rights between the 1 July 2026 commencement of SPF obligations and IDR and 1 January 2027 when EDR commences. AFCA must also be adequately resourced to better assist consumers during this transition.

To assist consumers during this interim period Government should:

- Ensure every SPF IDR complainant is given clear guidance as to their legal rights and dispute resolution options and pathways.
- Maintain a list of IDR complaints and require AFCA to contact the consumer to provide further assistance and re-engage once EDR comes online.
- Ensure a full statement of compliance, with access to supporting documentation is made is available for every IDR complaint from the commencement of the SPF.

Urgent scam protections must be progressed now

There are a number of actions Government can take immediately that would have a meaningful impact to minimise the harm of scams over the period before full implementation of the SPF. These include:

1. Mandating stronger hardship and reporting obligations from banks towards scam victims until 2028

We hear countless stories of banks continuing to charge interest on scammed funds, profiting from the hardship of their customers after their systems have failed to protect them. At a minimum:

- Banks should report on the levels of debt accruing interest where the customer has lost money to a scam.
- Banks should be prevented from charging interest on scammed funds.

2. A full ban on crypto ATMs

The Government can send an immediate clear message to scammers by fast-tracking a complete ban of crypto ATMs through its announced reforms[5] to provide AUSTRAC with additional powers to restrict or prohibit high-risk products.

Part 1 Recommendations – staggered implementation and delays

- Prioritise the implementation of the SPF and avoid further delays, noting the already significant slippage on proposed timeframes. In the period before full implementation of ASI, mandate that, at minimum, businesses maintain and uplift current practices of information sharing and act on publicly available sources of scams intelligence.
- Meaningful measures, strong guidance and resources to AFCA to assist consumers before EDR commences, including about processes and legal rights for multi-party complaints, and to implement an automated process to ensure they do not miss out on their right to EDR.
- Urgent interim scam harm minimisation solutions must be progressed and implemented, including:
    - Mandating stronger hardship and reporting obligations from banks towards scam victims until 2028.
    - Implementing a full ban on crypto ATMs.

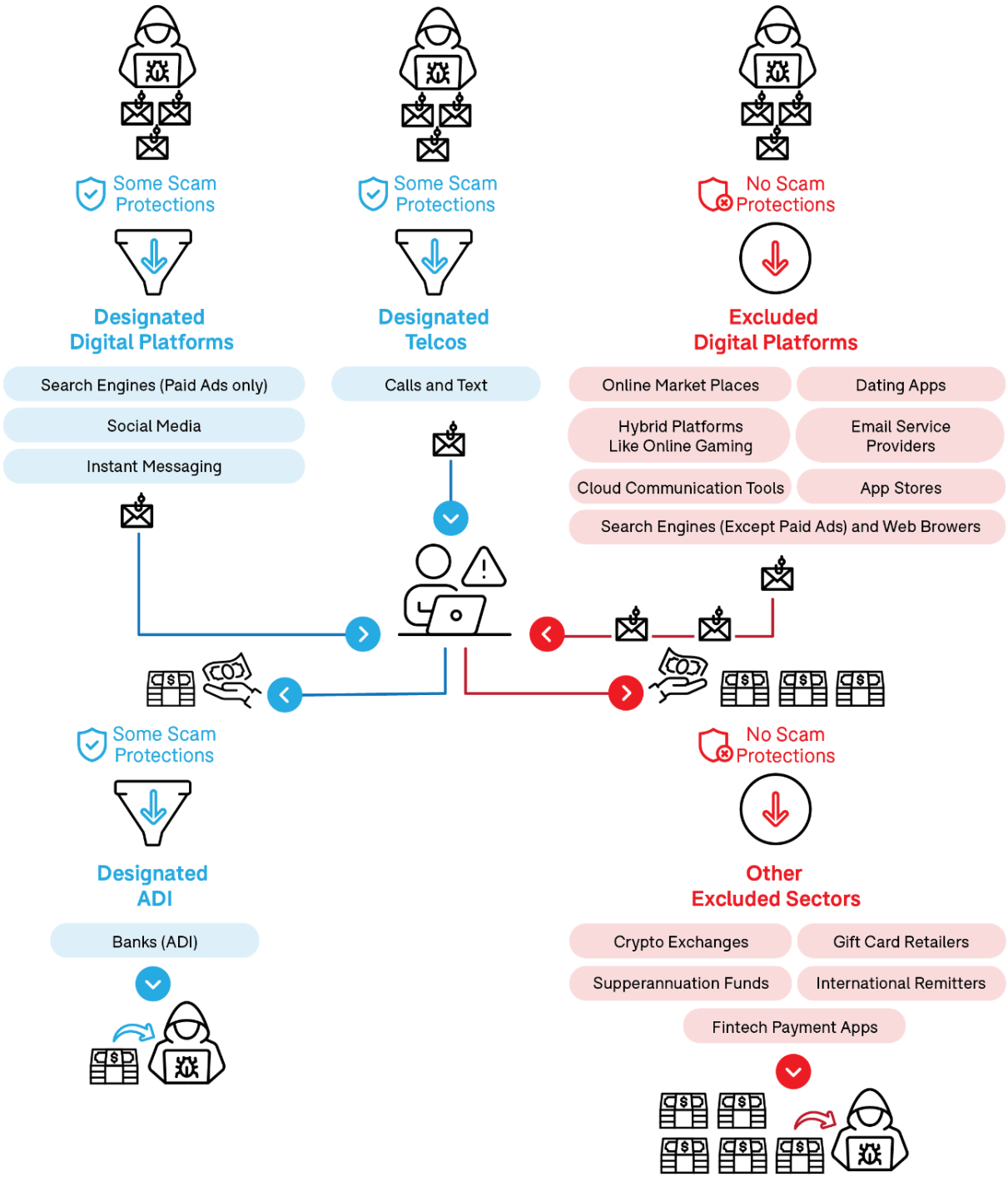
2. Coverage of the SPF is piecemeal and undermines effectiveness and functionality of framework

2.1 The Digital Platforms designation proposal is fundamentally too narrow

With this designation, the Government is proposing to protect Australians from scams on some digital platforms but not others (see Figure 1).

[5] https://minister.homeaffairs.gov.au/TonyBurke/Pages/national-press-club-address-16102025.aspx

Figure 1: SPF coverage leaves key gaps



Some of the biggest platforms enabling scam activity are left untouched

Instant messaging services, internet search engines and social media services are major platforms for scammers. However, so are email services, online marketplaces, dating apps, app stores, online job boards, web browsers and online games, none of which are covered by this proposal.

The decision to exclude these services from the definition of digital platform ignores the National Anti-Scams Centre's own analysis of how scammers are targeting Australians. This approach will also accelerate harms through platforms excluded from the designation.

- Scammers used email more than any other form of contact to target Australians last year[6], and with great success. Yet this proposal places no obligations on email platforms to prevent, detect or disrupt these communications.
    - Out of the $318.8 million in losses reported to Scamwatch last year, $49.6 million – or 15% – was lost in email scams.[7]
    - In the last year alone there have been numerous reports of people losing tens or even hundreds of thousands of dollars when scammers infiltrated email chains and convinced consumers to transfer entire house deposits or renovation funds into scam accounts.[8][9][10]
- More Australians reported a financial loss to a shopping scam than any other type in 2024[11], but online marketplaces have been excluded from this proposal.
- Romance scams ranked only behind investment scams for money lost in Australia last year[12], but dating apps and dating websites are not covered by these measures.
- App stores and web browsers are facilitating the rapid spread of 'scambling' in First Nations communities[13], but this proposal places no obligations on these platforms to do anything about it.

In addition, this proposal creates strange and unwarranted distinctions between different functions within the same platform. Meta, for example, will be required to

---

[6] https://www.nasc.gov.au/system/files/targeting-scams-report-2024.pdf

[7] https://www.scamwatch.gov.au/research-and-resources/scam-statistics

[8] https://www.news.com.au/finance/money/costs/gold-coast-couple-lose-250k-when-buying-house-in-devastating-email-compromise-scam/news-story/55f08cbe933ebebd4f40507582426a27

[9] https://www.sbs.com.au/news/insight/article/bank-account-scams-and-the-scams-prevention-framework/jw382pz2h

[10] https://www.news.com.au/finance/money/costs/traumatising-melbourne-couple-lose-50k-after-single-email/news-story/2bf1b4b844ad26c3db99d141304d9a5a

[11] https://www.nasc.gov.au/system/files/targeting-scams-report-2024.pdf

[12] https://www.nasc.gov.au/system/files/targeting-scams-report-2024.pdf

[13] https://www.abc.net.au/news/2025-08-29/scambling-the-online-gambling-scam-targeting-aboriginal-people/105709290

monitor and prevent scam activity on its main Facebook site and on Facebook Messenger, but not on Facebook Marketplace. There is a real risk that consumers will believe that because one part of Facebook is protected by these obligations, the rest of the Facebook ecosystem, including Marketplace, must be as well.

Google will be required to prevent scam content on its search function (paid only) but will have no obligations to do the same for its app store or extremely popular Gmail email service. Similarly, extensive digital advertising services provided by tech giants will only have obligations to prevent scams in certain places, not across their entire digital networks.

This could have the effect, for example, that Meta simply funnels known scam ads to appear throughout Facebook Marketplace, instead of the social feed. Internal Meta documents from late 2024 projected that they would earn around 10% of that year's total revenue – around USD16 billion – from running advertising for scams and banned goods.[14] They have a perverse incentive to find a home for scam content somewhere on their platforms.

It has been suggested that it would be too complex to design a sector code that spans all these platforms[15]. We do not share that pessimism. However, even if this was the case, it would not preclude the Government from at least designating all the relevant types of digital platform services, so that they are, at a minimum, covered by the overarching, principles-based obligations in the Scams Protection Framework Act, with specific codes to follow at a later date. Failure to do so gives organised scam networks a clear roadmap for continuing to scam Australians.

New technology will evolve while scams prevention stands still

This proposal also fails to future-proof the SPF with the flexibility to respond to technological innovation by new and existing platforms. This conflicts with the approach taken overseas.

For example, instead of reactively regulating platform by platform, the UK's Online Safety Act[16] covers all 'user-to-user services', which it defines as platforms where users can interact or upload content. Similarly, while the European Union's Digital Services Act[17] has additional obligations for a designated list of 'Very Large Online Platforms', its

[14] https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

[15] See section 5.5 of the SPF explanatory memorandum; https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr7275_ems_ec62fd87-d851-47d9-a2e5-8ec59b146297%22: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr7275_ems_ec62fd87-d851-47d9-a2e5-8ec59b146297%22

[16] https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

baseline obligations apply to all providers of intermediary services that store, transmit or disseminate user-provided information.

In practice, this means that new platforms will likely still be captured by the UK and EU Acts so long as they meet these broad criteria, rather than only being covered if they fit within one of the narrower moulds specifically set out in the definitions. This is plainly preferable to a system which requires new provisions to be continually bolted on to the law to respond to new types of scams from new types of platforms.

As well as covering a much broader range of digital platforms that already exist, these overseas laws are much better placed to apply to new types of platforms that may arise in the future. In Australia, we appear destined to play perpetual catch-up.

2.2 Government should be preparing for and signalling expansion of the SPF

While working to get the designation instruments for the first three sectors right, the Government's attention should already be turning towards designation and activating comprehensive scam protections across other industry sectors, to fortify the ecosystem. Digital payment platforms and the superannuation sector should be prioritised as our frontline services show them to be existing and growing enablers of scam activity.

Making a public commitment to the scope and timing of this expansion would signal ongoing commitment to the SPF and put these sectors on notice of their upcoming inclusion.

Digital Payment Platforms

With all the focus on the regulation of banks under the SPF, scammers are rapidly innovating and shifting more efforts to take advantage of the growing list of fintech sectors operators[18] that offer similar services to banks. The UK already captures many of these types of firms through its reimbursement model[19] and we note that the United States Federal Trade Commission has previously enforced consumer fraud protection measures at Western Union.

Our services regularly see Australians falling victim to scams using these payment platforms and remittance services (for example Revolut and Western Union). Scammers regularly groom consumers to use the lowest friction pathways available and the longer these services remain outside the SPF, the greater the risk of scam

[18] See: https://moneytransfer.com.au/guides/best-international-money-transfer/
[19] UK Payment Systems Regulator. 'Authorised push payment (APP) scams performance report'. July 2024. Available at: https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/;

exposure for consumers. Risk exposure through remittance services is heightened for diaspora communities given the heavy reliance on these services.

Victorian Aboriginal Legal Service Solicitor – "The client received money through the Stolen Generation Redress Scheme. The client believed she had found a stock trader, the scammer, on TikTok and made contact with him and then continued communications via Whatsapp. The scammer asked her to make payments via Revolut which she did. The scammer had also asked her to purchase and use a number of Prepaid VISA cards. The client has paid more money to 'restart' her account after it was closed, and 'recover' her earnings. The client has stopped sending money since contacting VALS, however, suspects she has transferred approximately $20,000."

Consumer Action Financial Counsellor Case – "After the bank prevented a customer from transferring hundreds of dollars to an account after being told it was a scam, the customer who had been socially engineered as part of a romance scam just went to the nearest Western Union to transfer the money to the scammer."

Superannuation

The superannuation sector has repeatedly been called out and put on notice[20] this year for the billions of Australians' superannuation savings being lost to scammers and fraudsters, yet they remain subject to no scam obligations.

The Government must not hesitate in designating the superannuation industry as a matter of priority. The immense superannuation losses we regularly hear about from scam victims cannot be permitted to go on.

Consumer Action Financial Counsellor – "Consumer Action Law Centre was approached by an extremely vulnerable and traumatised person who lives alone with an acquired brain injury, who lost their entire superannuation savings of approx. $200,000 across 2024 to a scammer after their Australian bank and superannuation provider easily facilitated the transfers, including in amounts over $10,000 at a time. As part of the highly sophisticated romance scam, the person was emotionally and psychologically manipulated by the scammer who requested to transfer the funds to many different Australian bank accounts. The person was also coached by the scammer to take out personal loans and credit cards which were drawn out and lost to the scammer leaving them with approx. $100,000 of debt that they are being forced to pay interest on to those financial institutions. The person's credit record has been

[20] https://www.asic.gov.au/about-asic/news-centre/news-items/asic-calls-out-superannuation-trustees-for-weak-scam-and-fraud-practices/; https://www.apra.gov.au/news-and-publications/apra-reinforces-expectations-on-authentication-controls-superannuation-sector

tarnished, and they are relying on their credit cards to survive, being unable to afford and pay for food."

Part 2 Recommendations – coverage of the SPF

- Expand the definition of a covered digital platform in the designation instrument to cover email services, online marketplaces, dating apps, app stores, online job boards, web browsers and online games.
- Recast the definition of a covered digital platform in the designation instrument at a higher level, in keeping with the approach taken in the United Kingdom and the European Union.
    - Such a definition would not only capture a broader range of relevant platforms now but would also ensure that the SPF applies to relevant new types of digital platforms as technology evolves.
- Prioritise expanding designation of the SPF to other sectors with high scam activity including digital payment platforms and superannuation and publicly commit to a timeline for doing so.

3. Proposed SPF codes obligations are insufficient to shift the dial on scam losses

Australians were promised a significant uplift in the scam prevention and protection measures under the SPF. But there remains little change in the proposed obligations under codes to the original limited obligations contemplated during the exposure draft consultation[21] of the SPF. Throughout development of the SPF, the codes of practice have been referenced as doing the 'heavy lifting' of the SPF and therefore we believe much more ambition and work is needed.

Scammers will not hesitate to exploit the gaps in the SPF if the current lack of specific protections is permitted to remain. The proposal will also make it very easy for Australia's banks, telcos and digital platforms to avoid taking the needed action to prevent scams while still avoiding any liability to compensate scam victims. We fear businesses may simply self-assess as having taken 'reasonable steps' to avoid any scrutiny or liability to their customers and users who have been harmed by ineffective prevention, detection and disruption measures. This feels like the status quo, or worse.

There are several crucial components that need to be addressed in the codes if the protections they purport to provide are going to amount to more than statements of good intent:

[21] https://consumeraction.org.au/wp-content/uploads/2024/10/2024-10-04-Consumer-Organisations-SPF-exposure-draft-submission.pdf

- A higher bar on businesses, including more specific prescriptive obligations to protect consumers from scams.
- Greater clarity on what constitutes 'reasonable steps' to support a high standard of scam protections, and to ensure that required protections are not unreasonably limited by the use of concepts like proportionality and scalability or leading to denial of liability.
- The codes must do more to consider vulnerability.
- Consumers should not be able to opt out of scam protections.

This part provides feedback related to the high-level components of code design as described in the position paper. To inform ongoing drafting of the individual sector codes, consideration of possible detailed and sector-specific obligations can be found in Appendix B.

3.1 Greater prescription and ambition is required

Greater prescription is required to ensure an uplift in protections

The SPF primary law principle-based protections largely rely on the standards to be set in the SPF Codes. The Act provides a framework based around business taking "reasonable steps" to prevent, detect, disrupt and respond to scams. Clear and specific obligations placed upon businesses are needed to give meaning and strength to the SPF obligations.

We generally agree with high level policy approach that the position paper sets out: "the SPF Codes will include both **prescriptive** and principle-based obligations" (page 5).

However, there are few prescriptive standards stated in the position paper with respect to preventing, disrupting and detecting scams. Also absent is any requirement that measures a business might introduce to prevent, disrupt and detect scam activity are effective (the only outlier is businesses must take 'effective steps' to protect their brand from being used in scams – page 26 position paper). The result of this lack is that the paper continues the same approach as the SPF primary law in only imposing a high-level standard that businesses must act reasonably.

For example, the obligation for banks to have "systems in place to monitor all transactions for suspicious activity that might be a scam" (page 14) is so high-level as to render it meaningless. Banks will already have such a system. The effectiveness and use of that system is what must be mandated and monitored to assess whether reasonable steps have been taken to protect consumers from scams. These prescriptive obligations must not be limited to "timeframes", "references to existing industry standards" and "actions in relation to high-risk scam threats" as page 5 and 6 of position paper references. Instead, as detailed in Appendix B of this submission, there is significant scope for prescriptive and ambitious obligations to be applied.

We also noted the statement in the position paper that the: "SPF Code and rules may reference existing standards to ensure obligations are in alignment" (page 6). While we understand the Government would want to minimise unnecessary overlap and duplication, existing standards are clearly inadequate in preventing scams harms. Reliance on existing standards belies any commitment to best, or at least better, scam protections.

Greater prescription is required for consumers to enforce their rights

Under the SPF, a business only contributes to the compensation of a scam victim if it is proven that the business breached its obligations under its sector code, or the overarching obligations under the Act, or both.

It is crucial that the codes introduce a significant uplift in prescriptive obligations to ensure consumers are sufficiently protected as the "sector codes will serve as the primary factor for assessing whether a business has taken reasonable steps" (page 5) under the SPF.

3.2 Codes must provide more clarity on reasonable steps

Many of the requirements provided in the position paper to prevent scams involve generalised steps that are "proportionate to the scam risk" (page 10). This indicates that, for example, if the scam is not widespread the bank has a lower obligation to protect the consumer.

Similarly, the position paper refers to obligations under codes being "scalable". At page 5 it states, "larger businesses may be required to implement more robust standards". This suggests, for example, that customers of the many, very profitable, smaller banks will have less rights under the SPF than those of the top four large banks. The result will be that a customers of a large bank may be entitled to compensation while a customer at a small bank will not receive compensation for the same scam. Banking law has never made such a distinction. ASIC recently found that the size of a bank did not necessarily impact its ability to implement prevention measures. Rather, leadership and culture played the decisive part.[22]

The SPF primary law and explanatory memorandum[23] only require that the "reasonable steps test recognises that different sized entities may appropriately meet their obligations in different ways." This should not accommodate different obligations and a lesser standard of protection from banks, telcos and digital platforms who are not

---

[22] ASIC (2004) REP 790 *Anti-scam practices of banks outside the four major banks* - https://download.asic.gov.au/media/eiahqnwn/rep790-published-20-august-2024.pdf, page 11

[23] Scams Prevention Framework Bill 2025 - https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr7275_ems_ec62fd87-d851-47d9-a2e5-8ec59b146297%22

considered to be the largest, but who also service the bulk of Australians, including those who are owned by larger conglomerates.

Additionally, the sector codes should provide more guidance to count for all the relevant factors stated under section 58BB of the SPF[24] to determine what constitutes 'reasonable steps', such as sufficiently accounting for the 'consumer base' (including for vulnerable consumers). Instead, the current broad, vague and ill-defined approach to scalability would likely lead to reduced scam protections based on business size, at the expense of the various other factors that must also be considered under section 58BB of the SPF.

3.3 Codes must consider vulnerability

The SPF needs to require more from business to identify and protect vulnerable consumers from scams. Incorporating the concept of vulnerability is required to:

- Increase prevention of harm from scams for vulnerable consumers.
- Ensure the highest level of scam protections is effectively targeted at consumers who are most at risk of scams and will most benefit.
- Provide businesses with certainty and clear guidance about their obligations towards vulnerable consumers under the SPF.
- Lessen the social and economic costs that result from vulnerable consumers not receiving tailored responses when impacted by scams.

Vulnerability should be incorporated into the SPF via three underlying obligations:

1. An obligation on businesses to proactively identify vulnerable consumers who use or seek to use their products and services, including groups who are likely to be vulnerable to particular scams.
2. An obligation for businesses to take extra steps to protect vulnerable consumers from scams.
3. Response and dispute resolution systems are safe and accessible.

Figure 2: Approach to vulnerability under the SPF Pillars

Prevent	Detect and disrupt	Response
SPF businesses must proactively identify vulnerable customers. Definition of vulnerable customer is broad and includes consideration of personal and situational vulnerability as well as vulnerability created or	SPF businesses must act to protect identified vulnerable consumers from harm. Higher level obligations apply on SPF businesses with respect to actions that must be taken to be considered compliant with	All consumers are vulnerable at this stage. Safe and accessible IDR is provided to all scam victims, with response tailored to individual vulnerability (whether previously identified or

[24] Section 58BB of the of the Competition and Consumer Act 2010

exacerbated by the SPF businesses' scam environment.	the SPF where a vulnerable consumer is involved. Increased obligations will differ between SPF sectors.	emerging in response phase). SPF businesses must prove compliance with SPF, including compliance with obligations to proactively identify vulnerability and act on that identification prior to the scam.

Further detail on how we propose vulnerability should be incorporated in the SPF is at Appendix C.

3.4 Protections should not rely on warnings

SPF minimum protections must not be left with an outweighed reliance on warnings and consumer education.

For example, we are concerned by the reliance on targeted warnings by banks to prevent scam risks to customers before high-risk payments (position paper, page 11). Currently if a bank detects a high-risk payment it may be obligated to block the transaction and contact its customer, as in the Lipkin Gorman principle[25]. Although this may not be the intended result, under the SPF, banks will rely on providing this warning to avoid liability.

Furthermore, the position paper states that banks must issue targeted scam alerts to consumers where there is a reasonable suspicion that a specific scam threat may impact them (page 16). The principle can be read to suggest that where a fraud alert is triggered the bank is not required to block the transaction and discuss it with their customer. This would effectively impose a lesser obligation than is current good practice and expectation.

3.5 Consumers should not be able to opt out of scam protections

Consumers should not be given the option to opt out of scam protections as suggested in the position paper.

This option will be exploited by scammers. Scammers routinely coach people on how to get around scam protections. An opt-out ability would provide another way for

[25] In Lipkin Gorman v Karnale and Lloyd's Bank [1987] 1 WLR 987 the court held that the test was: "whether, if a reasonable and honest banker knew of the relevant facts, he would have considered that there was a serious or real possibility, albeit not amounting to a probability, that its customer might be defrauded."

scammers to exploit people and create an existential weakness in the coverage and effectiveness of the SPF. It would also severely limit consumers rights in respect to dispute resolution and compensation under the SPF.

Part 3 Recommendations – principles guiding design of code obligations

- The Codes should provide a higher bar on businesses, including more specific prescriptive obligations to protect consumers from scams.
- The Codes must provide more clarity on what constitutes 'reasonable steps' to support a high standard of scam protections and to ensure they are not unreasonably limited by the use of concepts like proportionality and scalability.
- The Codes must do more to consider vulnerability, including requiring businesses to identify customer vulnerability and to tailor scam protection measures and the responses they provide accordingly.
- Consumers should not be able to opt out of scam protections.

4. Consumer-centred dispute resolution and an effective path to compensation is essential

We note and support several positive developments that will improve the fairness and accessibility of dispute resolution in the SPF. In particular:

- AFCA's jurisdiction will be retrospective once EDR comes online, with AFCA able to hear SPF related complaints whether the complaint, or the matter resulting in the complaint, arose before, on or after 1 January 2027.
- The possibility for a streamlined IDR process for high volume low loss scam cases.
- The incentive for businesses to provide timely resolutions of scam matters created by the exemption from providing a statement of compliance if the complaint can be resolved within 5 days.
    - Note: the default should be that the consumer is made whole for their scam loss under any expedited resolution process, with sufficient deterrence mechanisms so that inappropriate low-ball offers of settlement by businesses are eliminated or strongly disincentivised.

However, we stress that consumer-centred dispute resolution is long way off under the current SPF proposal.

The SPF must, in practice not just in rhetoric, provide **a fast, fair and straightforward pathway to compensation for victims**. Key components of such a system are:

- No wrong door dispute resolution where consumers are not left to co-ordinate with multiple entities.
- The consumer is made whole for their scam loss where at least one entity has not met its SPF obligations.
- Clear and binding IDR timeframes for businesses.
- A solution for fast compensation for high-volume, low-loss scam cases.
- Transparency of, and appropriate guardrails for, offers of settlement.
- The consumer always has access to independent External Dispute Resolution.

We acknowledge the value of industry-backed solutions and stand ready to collaborate with all parties. However, in such a complex landscape, a fair and functional dispute resolution system will not eventuate without Government acknowledging responsibility and taking leadership of its design.

We call on Government to immediately commence active design of a functional dispute resolution framework. This should be led by Government and must involve cross-sector collaboration with key stakeholders including consumer advocates, regulators, dispute resolution schemes and industry.

4.1 IDR as proposed is unworkable

The proposed dispute resolution pathway and diagram provided in the position paper entrenches existing unfairness, information asymmetries and establishes extra hurdles, further restricting scam victims' access to fair compensation.

Some of the more problematic issues with the proposed dispute resolution model include that it:

- Allows complaints to be made to any business in the scam chain but provides no guardrails to ensure scam victims are not left to co-ordinate IDR and chase all businesses involved in the scam, including any compensation owed by each.
- Only asks that businesses "should" work together to resolve complaints to "encourage" cooperation and timeliness in multi-party disputes (page 21-22), with no specific proposal given for co-ordination or arbitration of disputes between IDR members or about who decides apportionment.
- Limits scam victims' compensation (economic and non-economic) by letting business decide what "reasonably represents" a scam victim's loss (page 21).
- States apportionment of compensation can change if businesses agree (page 21) but provides no solution as to how the decision would be made and by whom.
- Leaves it to businesses to agree to invest in a "third-party administered IDR solution" (page 21) but provides no guardrails to ensure this is a solution that will benefit consumers.

- Creates no clear enforceable obligations for businesses with respect to IDR meaning it's unclear what, if any, regulatory action a regulator could take to combat systemic poor outcomes.
- Places no guardrails on businesses undertaking extended disputes between themselves about liability and apportionment at the expense of scam victims.
- Allows for the continued use of inappropriate low-ball offers of settlement, including before Statements of Compliance are issued, with no mandatory default requirements to make a victim whole for their losses where appropriate.
- Permits protracted IDR timeframes of more than 30 days.
- Risks scam victims giving up or accepting less unfair outcomes due to fatigue.
- Does nothing to stop businesses denying liability and dismissing scam victim complaints as a default.
- Does not require businesses to provide any proactive hardship assistance after a scam.
- Provides no limits on businesses continuing to demand that scam victims sign broad and restrictive confidentiality and non-disclosure settlement agreements (NDAs) before they can receive compensation.

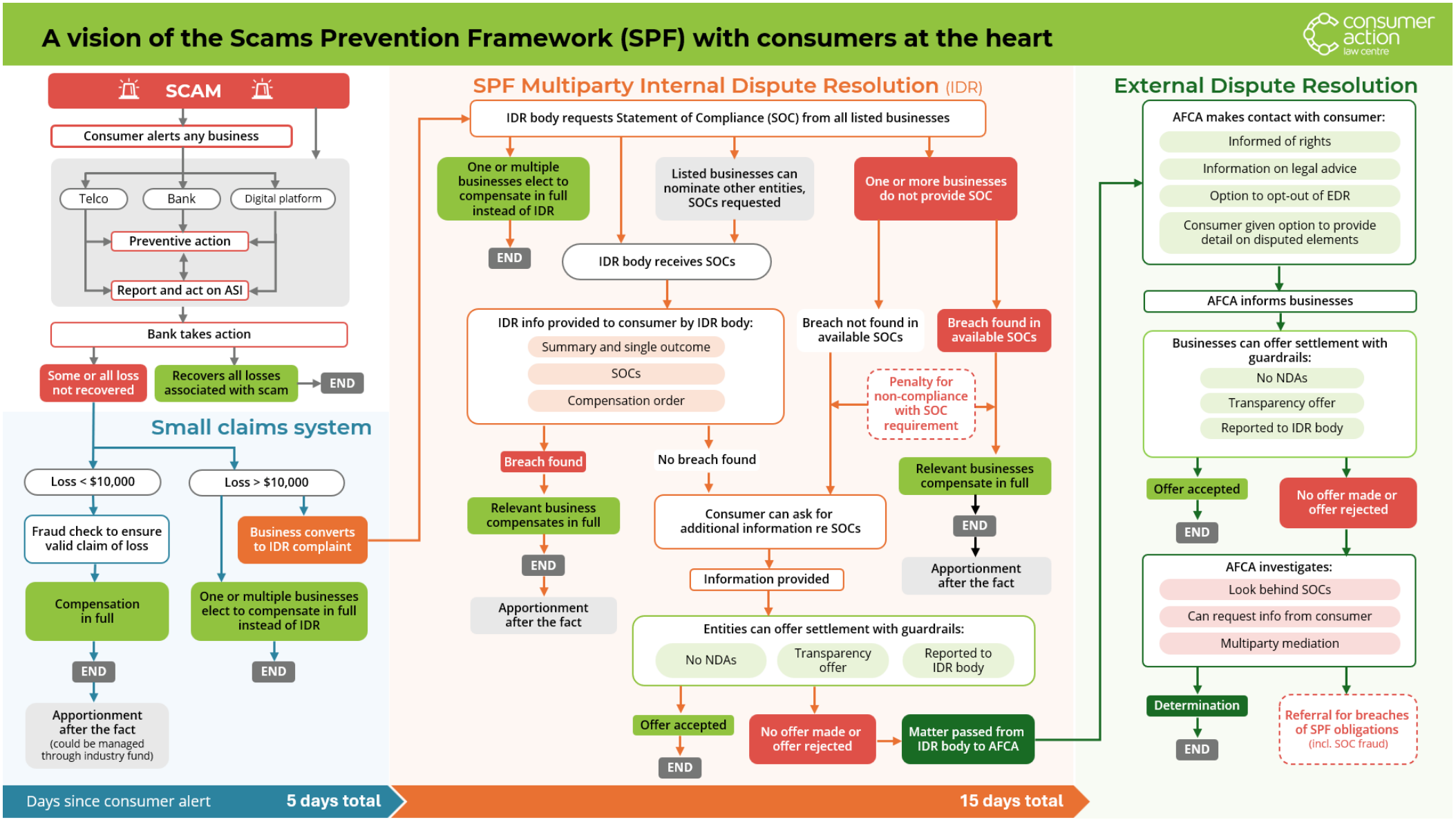
4.2 Putting consumers at the heart of SPF dispute resolution

The dispute resolution model we propose at Figure 3 would minimise the risks and extra hurdles created by the current proposal. This consumer-centred pathway is more than possible if accommodated and supported by the SPF rules and codes.

This dispute resolution pathway will ensure:

- A fast resolution of low-value claims through a simple, fast-track **small claims system**.
- The burden of coordination of IDR is removed by the consumer and is instead undertaken by a **centralised IDR body**.
- Consumers receive a single and intelligible IDR outcome, compiled by the IDR body.
- Consumers receive a resolution to an IDR complaint within a maximum of 15 days.
- Guardrails mean businesses are disincentivised from making inappropriate settlement offers.
- Transparency, accountability and consumer agency – consumers know about their rights and legal options, are keep informed throughout the complaint process and outcomes are reported and monitored to ensure system is delivering fair outcomes overall.
- Consequences for businesses who do not meet IDR obligations and timeframes, with delays not coming at the expense of scam victims.

Figure 3: Proposed consumer-centred dispute resolution pathway



Small Claims IDR Process

The development of an alternate fast-track process for low-value scam complaints is an effective way to handle the high volume of low-value scam complaints that is expected once the SPF comes online.

Low-value scams are the vast majority of scam complaints. Such a proposal has the potential to significantly reduce SPF compliance costs for businesses while increasing a scam victim's chances of fast and fair compensation after a scam.

We support the development of a fair process that would operate to separate out low-value scams to automatically compensate scam victims (with limits) for scam losses under a reasonable threshold (i.e. $10,000). For these low-value cases, no assessment of liability under the SPF is attempted and businesses are not required to produce a statement of compliance.

Central IDR body as facilitator of multiparty SPF

Multiparty internal dispute resolution is a new concept and presents significant risks for consumers. The proposal as presented in the position paper would involve a consumer navigating multiple different systems and independently attempting to enforce their rights against multiple large entities. There would be multiple outcomes of these processes, all delivered at different times and in different formats. Each outcome would also impact the others, creating ongoing disputes and negotiations.

This structural flaw innate to multiparty IDR can be addressed by the creation of a central IDR body to facilitate the administration of claims.

Regardless of which regulated business the victim approaches with a scam complaint (though it will almost always be their bank), the business would be required to register the complaint with the IDR body.

The IDR body would issue requests to all businesses for statements of compliance (including providing an opportunity for listed businesses to nominate additional businesses). The IDR body would then provide a single, consolidated outcome to the consumer. This outcome would:

- summarise the findings of the statements of compliance
- provide the statements of compliance in full
- clearly express the compensation to be paid to the consumer as a result of identified breaches of the SPF and a timeline for payment.

IDR timeframes

A final single IDR outcome/reimbursement order or offer should be provided within a maximum of 10 to 15 days from the initial IDR complaint being raised (under Malta's scams model a final IDR decision response timeframe is 15 days[26]).

Existing mandatory IDR response times in Australia (such as those that currently apply to financial services under ASIC's RG271) are not suitable for a modern-day scam environment. They were not developed to meet the needs of scam victims or ensure the urgent action required to effectively mitigate the financial and non-financial harm from scams that can escalate over a relatively short period of time.

Swift resolution at IDR is also important to mitigate the risk of secondary and recovery scams. Highly personal information gained in a scam is being used to initiate blackmail and perpetrate further scams (e.g. in romance or sextortion scams). This risk is exacerbated where a victim feels they are not being assisted in a timely or efficient manner after alerting a business about a scam. Scammers quickly exploit any gaps, delays or disorganisation in action by businesses responding to the needs of scam victims.

A period of around 5 days for a business to provide a statement of compliance to the central IDR body is reasonable as the system is likely to be largely automated (noting the requirement in the SPF for genuine oversight and sign off of final statements by an authorised representative of the business).

Apportionment of liability between businesses should occur after the consumer is compensated (see below) and should not prolong the IDR timeframe. In addition, the timeframe should not be prolonged by one or more parties failing to engage in the IDR process. For example, where a statement of compliance is not provided the consumer should be reimbursed in full where a breach is found on other statements. Relevant businesses can then seek reimbursement from any entity who did not provide a statement of compliance as needed.

Apportionment of liability

The position paper envisages IDR outcomes defaulting to equal share apportionment of compensation between businesses for scam losses where multiple businesses are at fault.

Additionally, the position paper states where one party is more culpable and agreement is reached, the default apportionment may be changed.

[26] https://consumeraction.org.au/wp-content/uploads/2025/01/Joint-Consumer-Organisations-SPF-Senate-Submission-9January2025.pdf

Tailored apportionment of compensation at the IDR phase is not a problem in itself. However, the expectation that a business will *agree* to an increase in their compensation owed is a fiction.

Any calculation of apportionment of compensation must not restrict the overall amount due to the consumer and it must not delay the payment of compensation to the consumer. Variable apportionment of compensation that meets the consumer's needs could be achieved by:

- establishing mandatory rules and tables of percentages to determine liability between businesses, and/or
- requiring that the consumer is compensated first using the default system and that any variation of apportionment be agreed by businesses after the fact.

Under Government's proposed IDR model, businesses are not incentivised to reach an agreement on liability and apportionment. As a result, more complaints will progress to EDR as they will not be resolved within the IDR timeframes. This risks undermining the fundamental purpose of EDR, overwhelming AFCA, and forcing consumers into long and unnecessary EDR complaints to receive the compensation they were already found to be owing.

Adopting a best practice consumer vulnerability approach when responding to scams

All scam victims are likely to experience some level of vulnerability after the scam event. The SPF codes and rules can and should be employed to do far more to mandate or encourage safe (including culturally safe) and accessible dispute resolution approaches to customer vulnerability during IDR through to EDR.

Responses and engagement with scam victims should acknowledge and be sensitive to customer vulnerability and be tailored to the specific circumstances of the consumer. Recognising that the psychological and emotional impact of a scam may lead to delayed reporting of the crime and its impact or resulting hardship, businesses should also be required to take proactive steps to identify their customers who are scam victims, to offer financial and non-financial support.

Building on the other relevant recommendations throughout this submission in relation to vulnerability, the SPF should require businesses to use the customer vulnerability indicators that they already hold, and/or others that they are proactively required to obtain, to support and create more positive consumer outcomes after a scam. Additional detail regarding the incorporation of vulnerability in the Response pillar of the SPF is available at Appendix C.

Part 4 Recommendations – consumer-centred dispute resolution

- Government should immediately commence active design of a functional dispute resolution framework.
    - This should be led by Government and must involve cross-sector collaboration with key stakeholders including consumer advocates, regulators, dispute resolution schemes and industry.
- Implement a fast, fair and straightforward dispute resolution system with scam victims at the heart, in line with our proposal. The pathway must ensure:
    - A fast resolution of low-value claims through a simple, fast-track small claims system.
    - The burden of coordination of IDR is removed by the consumer and is instead undertaken by a centralised IDR body.
    - Consumers receive a single and intelligible IDR outcome, compiled by the IDR body.
    - Consumers receive a resolution to an IDR complaint within a maximum of 15 days.
    - Guardrails mean businesses are disincentivised from making inappropriate settlement offers.
    - Transparency, accountability and consumer agency – consumers know about their rights and legal options, are keep informed throughout the complaint process and outcomes are reported and monitored to ensure system is delivering fair outcomes overall.
    - Consequences for businesses who do not meet IDR obligations and timeframes, with delays not coming at the expense of scam victims.

APPENDIX A – Consolidated list of recommendations made in this submission

Part 1 Recommendations – staggered implementation and delays

- Prioritise the implementation of the SPF and avoid further delays, noting the already significant slippage on proposed timeframes.
- In the period before full implementation of ASI, mandate that, at minimum, businesses maintain and uplift current practices of information sharing and act on publicly available sources of scams intelligence.
- Meaningful measures, strong guidance and resources to AFCA to assist consumers before EDR commences, including about processes and legal rights for multi-party complaints, and to implement an automated process to ensure they do not miss out on their right to EDR.
- Urgent interim scam harm minimisation solutions must be progressed and implemented, including:
    - Mandating stronger hardship and reporting obligations from banks towards scam victims until 2028.
    - Implementing a full ban on crypto ATMs.

Part 2 Recommendations – coverage of the SPF

- Expand the definition of a covered digital platform in the designation instrument to cover email services, online marketplaces, dating apps, app stores, online job boards, web browsers and online games.
- Recast the definition of a covered digital platform in the designation instrument at a higher level, in keeping with the approach taken in the United Kingdom and the European Union.
    - Such a definition would not only capture a broader range of relevant platforms now but would also ensure that the SPF applies to relevant new types of digital platforms as technology evolves.
- Prioritise expanding designation of the SPF to other sectors with high scam activity including digital payment platforms and superannuation and publicly commit to a timeline for doing so.

Part 3 Recommendations – principles guiding design of code obligations

- The Codes should provide a higher bar on businesses, including more specific prescriptive obligations to protect consumers from scams.

- The Codes must provide more clarity on what constitutes 'reasonable steps' to support a high standard of scam protections and to ensure they are not unreasonably limited by the use of concepts like proportionality and scalability.
- The Codes must do more to consider vulnerability, including requiring businesses to identify customer vulnerability and to tailor scam protection measures and the responses they provide accordingly.
- Consumers should not be able to opt out of scam protections.

Part 4 Recommendations – consumer-centred dispute resolution

- Government should immediately commence active design of a functional dispute resolution framework.
    - This should be led by Government and must involve cross-sector collaboration with key stakeholders including consumer advocates, regulators, dispute resolution schemes and industry.
- Implement a fast, fair and straightforward dispute resolution system with scam victims at the heart, in line with our proposal. The pathway must ensure:
    - A fast resolution of low-value claims through a simple, fast-track small claims system.
    - The burden of coordination of IDR is removed by the consumer and is instead undertaken by a centralised IDR body.
    - Consumers receive a single and intelligible IDR outcome, compiled by the IDR body.
    - Consumers receive a resolution to an IDR complaint within a maximum of 15 days.
    - Guardrails mean businesses are disincentivised from making inappropriate settlement offers.
    - Transparency, accountability and consumer agency – consumers know about their rights and legal options, are keep informed throughout the complaint process and outcomes are reported and monitored to ensure system is delivering fair outcomes overall.
    - Consequences for businesses who do not meet IDR obligations and timeframes, with delays not coming at the expense of scam victims.

APPENDIX B – Consideration of sector-specific code obligations

We note that the position paper states that stakeholders will have an opportunity to comment on exposure draft codes and rules during public consultation in early to mid-2026. However, to inform the development of these draft codes, this Appendix includes consideration of detailed sector specific obligations that should be included to ensure codes are ambitious and genuinely uplift scam protection in Australia.

Matters relating to the telecommunications code are considered in a separate submission made by ACCAN.

Banking Code

The position paper provides only limited prescriptive obligations for banks to prevent scams. The requirements to:

- Provide targeted warnings before customers make high-risk payments
- Use name checking technology, and
- Use Multi-Factor Authentication (MFA) for log attempts from a new device.

Almost all our organisations' calls about scams are from people experiencing high levels of personal and situational vulnerabilities who have told us they have been scammed on a bank's platform. The SPF must demand a significantly higher standard from banks who act as gatekeepers and custodians of people's money.

There are many other baseline prescriptive obligations that should be required by all banks to protect consumers and stop scams, including:

- MFA should not just be required for adding a new device, but for first time payees and daily payment limit changes – major banks do this and it clearly represents good banking practice.
- Delaying payments to first time payees – 24 hour delay on payments to first time payees. Again, this is standard practice by the major banks.
- Detecting and acting on simultaneous logins – Bank transaction logs identify the IP address of each transaction and so must identify logins using the same login from different location. Multiple logins using the same login credentials from different locations should trigger extra friction and checks on transactions.
- Restricting any and all crypto related transactions.
- Extra checks on transfers coming out of an account created within a 6-month period.
- Extra checks on transfers after a new phone number is added to an account or phone number is ported within a 6-month period.

- Recalling scammed funds – we note the reference on page 17 of the position paper to making payment requests to recall scammed funds. Again, this is the current practice. The issue that occurs, and must be addressed sufficiently, is the urgency of banks initially making such recall requests which is often far too late as highlighted in the case study above.
- The obligation to identify consumers who have made a scam payment should include a specific obligation for the bank to take action as soon as possible, rather than simply having systems in place to do this.

Furthermore, as noted elsewhere in this submission, if adopted, bespoke obligations in response to identified vulnerability would differ according to sectors. However, some potential specific tailored obligations or actions under the Banking Code in response to identified vulnerability could include:

- Cross-check unusual transactions (e.g. large amounts or transfer of recently loaned funds to unverified/risky accounts).
- Cross-check sudden frequent transactions (e.g. unusual payment patterns of smaller amounts anytime within a 12-month period).
- Cross-check transfers with the customers long-term transaction history, flagging discrepancies with payment size, payment frequency, method of payment and type of receiving entities.
- Further checks/inquires of receiving bank or entity before permitting transfer if there is no confirmation of payee match/payee verification.
- Extra checks for transfers to non-SFP businesses e.g. non-bank payment providers, fintechs, organisations involved in high scam report data from real-time actionable intelligence provided by scam regulators.
- Individualised warnings and engagement tailored to account for specific vulnerability.
- Unique interventions in response to different scam environment events such as specific market events/disruptions, natural disasters, critical or catastrophic data breach.
    - This may include requiring business to turn on tailored protections such as extra friction/pausing payment over a certain amount for customers who may be targeted.
    - It may be appropriate to infer that many or all customers are impacted by an event and should receive the benefit of these extra protections for a certain period.

Digital platforms code

The obligations that are proposed in the position paper are unclear

Many of the proposed obligations for digital platforms, as set out on page 31 of the position paper, are vague and unclear. There are a number of issues which need to be considered more fully in order for these obligations to have a meaningful impact.

How far will authentication go?

Requiring digital platforms to have authentication processes to ensure that accounts are legitimate is a worthy principle, and permanent bans for users and advertisers running scams is a worthy ambition, but it is not clear what types of checks these obligations will require. VPNs, new devices, and new accounts are just some of the ways scammers can re-appear on a platform from which they have previously been banned or blocked. For example, in 'scambling', we see scammers automatically phoenix their operations within minutes. The current proposal does not specify what identity or device checks will be expected, or how far they will be expected to go.

What content should be removed, and when?

Similarly, it is obviously critical that scam content is removed or de-listed, but this proposal does not set out the practicalities of that removal, such as the timeframe within which content should be taken down, and what the threshold is for content to be considered 'linked to a scam'.

The UK's Online Safety Act imposes a duty on platforms to use systems and processes designed to 'minimise the length of time for which any priority illegal content is present', and '*swiftly* take down such content' once notified of it. It is not apparent that the proposed approach in Australia will place even this relatively vague time pressure on digital platforms.

What constitutes 'high-risk'?

The term 'high-risk' is used frequently in these proposals, but it is not entirely clear what is meant by it. The SPF makes reference to 'consumers who have a higher risk of being targeted by a scam', and the position paper talks of 'customers who are at a high-risk of providing scammers with access to their accounts', but does not thoroughly detail who the Government considers this cohort of people to be. Accordingly, it is not clear which customers digital platforms will be expected to treat as 'high-risk', and this raises the possibility of each platform working from its own interpretation.

Similarly, the position paper proposes to require digital platforms to verify advertisers of 'high-risk products', but beyond a high-level reference to 'financial services and health care products', it is not clear how this risk assessment will be made, how verification will take place, and how international advertisers with different licensing regimes to those in Australia will be treated.

Proving a breach by a digital platform could become a Kafkaesque nightmare

Under the SPF, a business only contributes to the compensation of a scam victim if it is proven that the business breached its obligations under its sector code, or the overarching obligations under the Act, or both.

This will be a significant challenge in any of the designated sectors, but the combination of weak transparency obligations, complex pathways, and a particularly massive information asymmetry means that it is likely to be especially difficult for a consumer to prove a breach by a digital platform.

There is a considerable risk that the current proposal incentivises platforms to devote their energies to making their own culpability for scams harder to prove, rather than preventing the scams in the first place.

It would be optimistic indeed to expect that businesses like Meta, who right now are profiting from scam activity, will diligently abide by code obligations that are not only uncertain, but seem near impossible for the ordinary Australian consumer to enforce.

Government needs to provide more clarity on how consumers will be expected to prove a claim against a digital platform. We recommend Government provide multiple examples for the different real-life scam scenarios consumers will face, including specifying the obligations that they can rely on in each example. These scenarios should be tested with scam victims and consumer advocates before obligations are finalised.

The standard of protection should meet the scale of the risk

In their most recent Digital Platforms Complaints Insight Report, the Telecommunications Industry Ombudsman noted that some scam complaints related to losses arising from hackers seizing social media, email, and app store accounts.[27] As the report points out:

> *Google, Apple and Microsoft all offer a range of hardware and software products including smartphones, email and cloud products, and digital wallets. […] The integrated functionality of technology and online services is a competitive advantage for companies. But when something goes wrong and consumers are unable to receive the help they need, this can have wide-reaching impacts across devices and data in our work and personal lives.*

These very large, integrated companies are now deeply embedded in our lives, and often have custody of a huge range of our most sensitive personal information. A hacker

[27] https://www.tio.com.au/sites/default/files/2025-12/TIO_Digital_platforms_complaints_insights_report_December_2025.pdf

or scammer who infiltrates one of these integrated accounts can cause an enormous amount of personal and financial damage.

This elevated risk should be met with elevated protections for consumers. Australians must be able to have confidence that their most sensitive information is receiving the best possible protection. Large digital platforms like Google, Microsoft and Apple should be held to higher mandatory consumer protection standards, in recognition of the many tools, devices and services they currently provide, and the wide range of avenues this integration presents to bad actors.

To achieve this, it may be necessary to create a specific class of very large, diverse businesses, who are required to observe the SPF's obligations across all their platforms, to reflect the fact that a breach in one of those platforms, for example through a phishing scam, may enable further breaches across the others.

APPENDIX C – Incorporating vulnerability into the SPF

As business transition to new technologies and modern markets, they have a responsibility not to leave any of their customers behind. Increased business efficiency, cost savings and transactional speed can improve the lives of many but has also left a significant portion of society already operating at a disadvantage bearing the risk and cost of scams.

An increasing number of our organisation's calls are from scam victims experiencing high level of personal and situational vulnerabilities and whose lives are impacted the most when they are scammed. Scammers are also increasingly targeting specific groups and communities, particularly those experiencing vulnerabilities.

This proposed approach to incorporating vulnerability into the SPF is built on three underlying obligations:

1. An obligation on businesses to proactively identify vulnerable consumers who use their services.
2. An obligation for businesses to extra steps to protect vulnerable consumers from scams.
3. Response and dispute resolution systems are safe and accessible.

Prevent	Detect and disrupt	Response
SPF businesses must proactively identify vulnerable customers. Definition of vulnerable customer is broad and includes consideration of personal and situational vulnerability as well as vulnerability created or exacerbated by the SPF businesses' scam environment.	SPF businesses must act to protect identified vulnerable consumers from harm. Higher level obligations apply on SPF businesses with respect to actions that must be taken to be considered compliant with the SPF where a vulnerable consumer is involved. Increased obligations will differ between SPF sectors.	All consumers are vulnerable at this stage. Safe and accessible IDR is provided to all scam victims, with response tailored to individual vulnerability (whether previously identified or emerging in response phase). SPF businesses must prove compliance with SPF, including compliance with obligations to proactively identify vulnerability and act on that identification prior to the scam.

Definition of vulnerable consumer for the SPF Codes

- As discussed further below, we propose a tailored definition for 'vulnerable consumer' that would be responsive to their needs under the Scam Prevention Framework (SPF) would be:

  "Someone who, due to the presence of one or more personal, situational and market environment factors, which can be temporary, sporadic or permanent, is especially susceptible to harm – particularly when a firm is not acting with appropriate levels of care."

- It is important to acknowledge that anyone can be vulnerable to a scam. Vulnerability is also dynamic and variable. Specific to the SPF, circumstances that may make someone especially susceptible to scam harm can emerge from personal vulnerability, situational vulnerability, or from transactional and market-based vulnerability.
- The SPF definition of vulnerability must be broad to allow for the variable nature of vulnerability, but relevant to the SPF to make a meaningful impact on scam prevention and response.
- One way to approach this is developing a single broad definition; supported by a non-exhaustive list of vulnerability indicators which SPF businesses would need to proactively identify in context of their market offering and scam environment.
- We note that across the regulatory environment, multiple definitions of vulnerability are being developed (e.g. within ATO hardship arrangements, insurance code).
    - Existing and emerging definitions of vulnerability should be kept in mind in developing SPF-specific vulnerability requirements to reduce fragmentation and complexity for industry. However, vulnerability within the context of the SPF needs to go beyond general definitions of vulnerability and also be scam-specific.
- We support Government incorporating the best practice elements from the two definitions provided below (and from associated policy/guidance materials).

1. The United Kingdom's (UK) scams framework and Payment Systems Regulator's (the PSR) definition[28] for 'vulnerable consumer':

   *"Someone who, due to their personal circumstances, is especially susceptible to harm – **particularly when a firm is not acting with appropriate levels of care**."*

[28] See: https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf

2. The international standard ISO 22458:2022 definition of vulnerability[29]:

   "state in which an individual can be placed at risk of harm during their interaction with a service provider due to the presence of ***personal, situational and market environment factors****"*

   - The ISO also defines 'vulnerable situation' to mean a *temporary, sporadic or permanent circumstance which places a consumer at risk of harm or disadvantage, if an organisation does not act with appropriate levels of care*.

- Elements of these approaches and definitions should be incorporated into a best practice definition of vulnerability[30], resulting in something similar to:

  "Someone who, due to the presence of one or more ***personal, situational and market environment factors****, which can be temporary, sporadic or permanent, is especially susceptible to harm –* ***particularly when a firm is not acting with appropriate levels of care****."*

- This definition would incorporate broader concepts of vulnerability that are relevant in a scams context.
  - I.e. This definition would incorporate market environmental factors, rather than limiting to personal characteristics. Vulnerabilities can arise from, for example:
    - the complexity of products and services
    - rapid market-driven technological advances with little consumer input/insight
    - scam trends leveraging specific products or services
    - marketing practices
    - information/power asymmetries
    - market cycles/disruptions
    - data breaches.
  - The definition also accounts for vulnerability being dynamic. For example:
    - a person or class of person who is not usually vulnerable in terms of their personal circumstances will be particularly exposed when managing something like a house deposit or engaging after a natural disaster

[29] See: https://www.iso.org/obp/ui/#iso:std:iso:22458:ed-1:v1:en

[30] Some other relevant, though less appropriate, examples of definitions include: The now superseded UK's Contingent Reimbursement Model (CRM) Code also provided a clear benchmark and a case-by-case approach to considering vulnerability; As noted in the joint consumer organisations scams submission to Senate Economics Legislation Committee, Dr Sophie Scamps MP proposed an amendment to the SPF Bill to incorporate a definition of vulnerability.

        - a person or class of person who is financially and technologically astute will be exposed to a new scam trend (e.g. the HSBC scam where customers believed their bank was trying to contact them and avoid account compromise).
    - Market factors can also, paired with existing personal and situational vulnerabilities, create a greater scam risk for those customers.
- This definition also requires expectations of 'appropriate' care from business in response to consumer vulnerability. The 'appropriate' level of care could include consideration of other element (e.g. diligent, careful, thorough etc) to guide business approaches.

Preventing, detecting and disrupting scams for identified vulnerable consumers

- SPF businesses should be required to proactively identify vulnerable consumers without consumers having to self-identify.
- When vulnerability has been identified, higher obligations and extra steps will be required from SPF businesses to prevent scams for vulnerable customers.
    - There is existing precedent incorporated into regulatory frameworks internationally and in Australia that supports requiring additional proactive best practice scam/harm prevention steps for vulnerable consumers[31].
- These obligations should be responsive to specific vulnerabilities, including a cross-analysis of personal, situational and market/transactional vulnerabilities.
- These obligations will also be different according to the SPF sector.
- The level of action and care taken on those obligations will contribute to the determination of whether a business has satisfied 'reasonable steps' under the SPF, resulting in compliance or non-compliance in the SPF 'statement of compliance'.

Identifying a vulnerable consumer

- SPF businesses should be required to proactively identify vulnerable consumers without consumers having to self-identify. The SPF could build on the number of

[31] UK Scams regulator, the PSR - "we expect firms 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". See: https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf
Responsible lending laws (RLOs) and current RLO regulatory guides (e.g. RG 209) require when making reasonable inquiries and verifying the consumer's financial situation, providers must have regard to red flags that are signs of 'financial vulnerability' before advancing credit.

existing enforceable Australian regulatory precedents requiring proactive identification of vulnerability32.

- SPF businesses must have a detailed knowledge of both their customer base and their scam environment to identify how product and services they offer could make their customers particularly susceptible to harm from scams.
- SPF businesses should take steps to support self-identification of vulnerability from consumers by communicating increased protections that will be available.
- Vulnerability can be hidden, and consumers are likely to be reluctant or unable to self-identify. SPF businesses must be sensitive to vulnerability indicators and act on indications received in all interactions with consumers or through other sources of information.
- Businesses should obtain consent from customers (where necessary) to address privacy concerns.
    - Business terms and conditions already permit the gathering and analysis of customer data to profile their customers for a range of purposes such as marketing and sales or to 'enhance' or 'monitor' customer experience. This could be expanded and applied under a vulnerability lens to understand, segment and better protect their customers from scams.

Information to identify and obtain from vulnerable consumers

- Institutions already hold a range of information about consumers that could be used to proactively identify vulnerability including:
    - Age, gender, post code, customers who have identified as living with a disability or as Culturally and Linguistically Diverse (CALD) including First Nations, and communication preferences (e.g. require interpreters).
    - Bank account balance, fee/charges/interest history, essential and discretionary spend patterns, credit and debit providers historical details (e.g payee details, Centrelink income, payday/BNPL debts).
    - Types of transactions and services used by consumers.
- A potential non-exhaustive list of vulnerability indicators that could be appropriate and responsive to the needs of a diverse cohort of customers experiencing or impacted by vulnerability in a scam context includes:

> age, mental or physical disability, illness or impairment, domestic and family violence, cultural minority/practices/behaviours, language difficulty, newly arrived non-English speaking migrants, poor digital

[32] For example, 'Financial vulnerability' in the Treasury Laws Amendment (Responsible Buy Now Pay Later and Other Measures) Act 2024 and indictors outlined in ASIC Regulatory Guide 281: Low cost credit contracts; the Telecommunications (Financial Hardship) Industry Standard 2024; the Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025.

literacy (coupled with on-line dependence), low income/low financial resilience, insecure and precarious employment, unsecure housing, low savings, financial hardship, overdue debts, carer/parental responsibilities, addictions, overseas family responsibilities, isolated living situation, single parent, minimal assets, lumpsum/rapid/frequent superannuation/savings withdrawals, adverse credit report listings, location of residence, affected by a natural disaster, previous data breach, victim of a previous scam or being scammed repeatedly.

- The level of action taken to identify vulnerability will contribute to the determination of whether a business has satisfied 'reasonable steps' under the SPF, resulting in compliance or non-compliance in the SPF 'statement of compliance'.
- This framework should be coupled with stronger collection and data protection requirements for SPF businesses of information they collect for the purpose of assessing vulnerability. Consumers may be unwilling to self-disclose if they are not confident that their information will be safe and secure.

Continual improvement towards approaching vulnerability under SPF 'Governance' principle

- Both the definition and identifying the understood markers of vulnerability should be dynamic and assessed regularly, informed by trends in scam harms.
- Through implementation of their policies, procedures and performance metrics, SPF businesses must be required to regularly report on how they are taking vulnerability into account and demonstrate the effectiveness of their actions.
- Scammers aren't static and will innovate rapidly to groom victims to avoid boilerplate interventions and questions from SPF businesses. This is compounded by the sense of urgency they place on their victims in different circumstances (e.g. sextortion in romance scams).
- The National Anti-Scam Centre should play a key role as a cross-sector collaborator, sharing ideas and best practice approaches to vulnerability based on the real-time scam intelligence it will receive.
- SPF businesses must be ready to quickly adjust to evolving approaches in identifying and intervening for vulnerability according to the scam intelligence they receive.

Responding to scams

- All scam victims are likely to experience some level of vulnerability after the scam event. Responses and engagement with scam victims should acknowledge and be sensitive to customer vulnerability and be tailored to the specific circumstances of the consumer.

- Businesses must provide safe (including culturally safe) and accessible dispute resolution (IDR through to EDR) tailored to the individual needs of vulnerable scam victims.
- Businesses should use vulnerability indicators that it has already obtained from their customers to remove/minimise evidentiary burdens on scam victims. Businesses should also be sensitive to vulnerability indicators that emerge during the response phase.
- Businesses should recognise that the psychological and emotional impact of a scam may lead to delayed reporting of the crime and its impact or resulting hardship.
- Businesses should take proactive steps to identify their customers who are scam victims to offer financial and non-financial support.
- Elements of a safe and accessible response are below, grouped into actions to build:
    - accessibility and additional care and support
    - access to fair compensation, and
    - holistic and proactive hardship response.
- These elements could be incorporated as baseline safety or scaled in response to specific vulnerability.

Accessibility and additional care and support at dispute resolution

- Plain language summary of information provided in 'statement of compliance'.
- Shorter timing for IDR response and streamlined access to redress or compensation.
- Automatic escalation/notification to AFCA (customer to be provided sufficient information/documentation/free advocate assistance to proceed to EDR, and can opt out) if consumer does not respond to an IDR outcome offering no/minimal compensation.
- Direct referral pathways and streamlined authorisation process and documentation requests for free third-party representative assistance including CLC lawyers and financial counsellors.
- Free interpreters.
- Policies and procedures to recognise where a consumer is unable or unwilling to respond, or adequately respond, to an information request by their provider, this may be indicative of vulnerability.
- Keeping consumers regularly updated on the progress of recovery attempts and providing details explaining the outcome where unsuccessful.

Access to fair compensation

- Lower culpability and thresholds for negligence for vulnerable consumers to access fair compensation (See UK approach for vulnerable customers33).
- Fair compensation weighted towards customer made whole, even if some customer negligence found.
- The prohibition of, or strong limits on, non-disclosure settlements, such that no offer of settlement from a SPF business can be made that is conditional on non-disclosure by the scam victim.
- Limits on settlement offers less than 50% of scam loss.

Holistic and proactive hardship response

- Any credit amount lost to a scam should be waived (including interest).
- Stop, reduce and waive any other debt (or interest) that is compounding the scam harm for victims.
- Limits on debt enforcement of scammed funds.
- Limits on requiring evidence of vulnerability (the Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025 is an example were evidence of DFV can only be requested in exceptional circumstances).
- Overarching principle/protections not to de-bank vulnerable scam victims.
- Where a person has had a financial account or other account compromised as part of the scam (e.g. used to process scammed funds) businesses should be cautious about blocking and denying their access in a way that causes them financial or economic hardship.
- Use technology to proactively identify warning signs/patterns of scammed customers in financial hardship (e.g. withdrawal of the majority of bank savings anytime within a 6-month period, sudden low account balance, sudden interest accumulation/default fees, increase in funds transfer to fringe lenders/firms, credit report indicators).

The following hypothetical consumer scam outcome (using a real-life case study) represents an example of some ideal best practice protection and response standards that business should be required to adopt under the SPF for vulnerable scam victims.

[33] See: https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf; https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf

Example of obligations across the SPF for vulnerable consumer (using case study provided in previous SPF consultation)

Mia's* story – Consumer Action Law Centre

Mia is a carer for her child living with a disability.

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

Obligation	***Example actions (in addition to baseline SPF actions)***
PREVENT	
Business to proactively look for and cross-analyse indicators of vulnerability, including but not limited to personal, situational and market/transactional vulnerabilities	Bank identifies customer's difficulties through Centrelink income, identified carer responsibilities, low savings balance/net debt position to record personal/situational vulnerability data. Bank also has recorded previous fraud occurrences on customer/compromised card. Shares data with SPF regulators to provide market/transactional vulnerability data, including in settings relevant to individual customer's engagement where available. (If personal details have been released due to data breach) Telco shares data breach information with SPF regulators so other SPF businesses are aware of the vulnerability
DETECT AND DISRUPT Business to act on extra obligations to protect vulnerable consumers that are tailored according to the customers vulnerability	Bank flags customer's savings will be depleted more than 50% (or by 50% within a relatively short period of time) if it permits the transactions and adds friction until further checks are undertaken Confirmation of payee indicates name and receiving account don't match or account is unverified. Mia is unable to override and proceed with transaction without further friction, because identified as vulnerable consumer Bank acts on known vulnerability and provides tailored engagement and intervention to customer
RESPOND Business to provide safe and accessible response and dispute resolution (IDR through to EDR) tailored to the individual needs of vulnerable scam victims	*If scam was not prevented* Bank technology reports customers savings have been depleted over a relatively short period of time.

Bank proactively offers tailored scam hardship support, including shorter timing for IDR response and streamlined access to redress/compensation.

Financial support comprises offers to hold/waive interest on any scammed funds or other debt obligations with the bank

Non-financial support comprises of offer to make warm referrals to free support services (e.g. NDH/IDCARE) with easy third-party authority/document request processes