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

3 July 2026

Joint Consumer Submission – Scam Prevention Framework codes and rules

This is a joint submission, co-drafted by Consumer Action Law Centre (Consumer Action) with CHOICE and the Australian Communications Consumer Action Network (ACCAN), and made on behalf of:

- Consumer Action
- CHOICE
- ACCAN
- Financial Rights Legal Centre
- Westjustice
- Financial Counselling Australia
- Consumer Credit Legal Service WA
- Consumer Advocacy Network WA
- Financial Counselling Western Australia
- Mob Strong Debt Help
- Brotherhood of St Laurence
- Victorian Aboriginal Legal Service

After almost five years of tough talk and promises, the Government has presented Australians with a weak and confusing set of proposals that will offer only basic protection against scams.

Government has chosen to implement a highly complex approach to protecting Australians from scams. Their chosen ecosystem model is proving immensely complicated, costly and time consuming to bring to life. At its absolute best, the

ecosystem approach could be highly effective at preventing and disrupting scams. However, this requires far more courage and ambition from Government than is evident in this proposal.

Furthermore, for this framework to succeed, regulated entities must genuinely invest in protecting Australians from scams and making this system work. In contrast, what we are seeing is industry negotiating to protect their own interests and reverting to harmful and deceptive victim-blaming narratives to distract from their own failure to prevent scams. Government must be prepared to force industry investment and concrete action to ensure this is a system that works for Australians, not one that minimises corporate liability.

Australians reported nearly $2.2 billion in scam losses last year, 8 per cent more than the year before. This is a reversal of the downwards trend we were starting to see and shows the scammers are getting ahead of us, again. It should be ringing alarm bells for the Government. Instead, we have seen scam prevention drop down and down on the Government's list of priorities.

At least half a million Australians are falling victim to these crimes every year. They deserve better than this from the banks they pay to keep their money safe from telecommunications companies and digital platforms that profit from consumers using their services. They also deserve much more from their government.

We get one go at this. If the Scam Prevention Framework is weak—which is its current trajectory—scam losses will continue to soar, victims of crime will have no chance at compensation or recovery and trust in the digital economy will erode. This will have been an expensive and time-consuming failed experiment.

We are at a cross-roads. Government has chosen this framework so it must demand much more from the corporations who can make the difference in getting Australia ahead of growing scam losses.

The recommendations in this submission are informed by the experience and expertise of consumer organisations across the country, many of whom work with scam victims every day who come to us with stories like Neville and Lillian's below. We urge the Government to listen and build a framework that meaningfully protects Australians.

We call on the Government to:

1. Establish robust, prescriptive, outcome-focused **code obligations** that specifically and clearly define what is expected of regulated entities, set a higher bar than current practice, and will actually prevent scams.
2. Develop and mandate a fair and transparent multi-party **internal dispute resolution** (**IDR**) system that functions effectively for consumers.

3. Mandate automatic **reimbursement** at a level that meaningfully supports consumers, particularly for low-value claims, to ensure fast and accessible compensation without requiring complex dispute processes.
4. Give consumers, the Australian Financial Complaints Authority (**AFCA**) and regulators the information and powers they need to hold regulated entities accountable when scam protections fail. This must include **clear compliance standards**, transparent reporting and enforceable obligations.
5. Move quickly to **expand coverage** to other high-risk sectors such as superannuation, dating platforms and non-bank services, where scam activity is already prevalent.

Stephanie Tonkin | CEO

Consumer Action Law Centre

Case Study

Neville and Lillian* are a married couple in their 80s living on a farm in regional Victoria.*

After seeing a pop-up message claiming to be from Microsoft, Neville called the number displayed and was persuaded to install remote access software. The scammers gained access to the couple's computer and online banking, and over the following 48 hours stole around $100,000 from their savings and a line of credit secured against their farm.

Despite more than 100 transactions occurring in a short period and the rapid depletion of the couple's funds, the bank did not intervene until alerted by a receiving bank. By the time recall requests were made, only $11.20 had been recovered.

AFCA ultimately found in favour of the bank. As a result, Neville and Lillian face the prospect of debt recovery from their estate, placing the future of the family farm at risk and causing significant financial hardship and emotional distress.

**Name changed*

Contents

1 Summary of key issues

While we support the intent of the SPF as a coordinated, system-wide response to scam harm, as currently drafted, the SPF codes and rules do not yet deliver the level of protection required to meaningfully reduce scam losses or improve outcomes for consumers.

Australian lives are being destroyed by scams and that can't be forgotten as the detail of the codes, rules and implementation of the SPF is developed.

To strengthen the SPF to effectively prevent and disrupt scams, the Government must:

- Urgently expand the scope of the SPF to additional, and within existing, high-risk sectors (including organic search, dating platforms, digital payment platforms, superannuation and crypto-related services) and publicly commit to a timeline for designation.
- Introduce a hybrid regulatory approach, combining principles-based obligations with clear, enforceable minimum standards to ensure consistent and effective application.
- Ensure industry code obligations are clear, outcome-focused and enforceable, with reduced reliance on vague terms such as "reasonable" and greater emphasis on timely intervention and prevention of harm.
- Strengthen accountability and transparency mechanisms, including requiring meaningful, evidence-based Statements of Compliance with case-specific disclosures.
- Establish an IDR system that works for consumers, including strong multi-party coordination requirements, a single pathway for complaints and reduced evidentiary burden on victims.
- Increase the automatic compensation threshold (to at least $10,000) and strengthen incentives for early reimbursement, including through the AFCA fee settings.

2 The SPF remains partial, delayed and risks failing consumers

Key points

- The SPF does not yet centre the consumer experience. This version focusses instead on compatibility with regulated entity processes, and leaves consumers to navigate complex, multi-party systems.
- Delayed implementation until March 2027 prolongs exposure to preventable harm, highlighting the critical need for stronger, enforceable minimum standards.
- Critical scam pathways remain outside scope, including major digital platforms, non-bank payment services, purchased payment facilities, dating apps and superannuation, creating exploitable gaps.
- Government should introduce a faster, transparent pathway for expanding the SPF, including a public timeline and mechanisms to designate high-risk sectors before detailed codes are finalised.

2.1 This SPF does not have consumers at the heart

While the SPF represents a significant step towards a coordinated response to scams, in its current form, it does not centre the consumer experience.

Many of the proposed obligations are framed around entity processes and inter-entity arrangements, rather than the practical needs of consumers who are exposed to scams or are navigating the system after a scam event. Scam prevention and disruption has become an indirect or assumed benefit, rather than a clearly enforced objective. In the absence of a consumer focus, there is a risk that the framework improves internal processes, without materially improving protection for consumers.

For example, the draft framework places a disproportionate burden on consumers to navigate complex, multi-party environments (discussed further in section 8.1). Under the current draft, victims may still be required to engage with multiple entities, repeat their account of the event and piece together evidence across different services, all the while facing powerful businesses that have significant interest in denying their claims and rights.

This is inconsistent with a consumer-centred model, which should instead place responsibility for coordination, investigation and resolution solely on regulated entities. This could be achieved through a legislated multi-party IDR model, or at minimum by requiring a single entity (such as the bank) to coordinate the process on the consumer's behalf. Without clear mechanisms to streamline processes in this way, we see a critical

risk that the framework replicates or exacerbates existing barriers for consumers in seeking redress for system failures.

The framework also continues to rely heavily on subjective concepts such as "reasonable steps" and "proportionate action" (discussed further in section 4.1), which can obscure whether consumer protections have been meaningfully applied in practice. Without clear, enforceable standards and transparent disclosure requirements, specifically including evidence of regulated entities' self-assessments, consumers will struggle to understand or challenge decisions made by entities. The system as proposed further perpetuates information asymmetry and limits a consumer's ability to effectively exercise their rights.

A genuinely consumer-centred SPF would ensure that obligations are designed around how consumers experience scams and seek redress. This includes:

- clear pathways for complaints
- strong coordination requirements between entities
- enforceable minimum standards, and
- transparency in decision-making.

Without these elements, there is a risk that the SPF adds complexity and confusion and fails to meaningfully improve outcomes for the people it is intended to protect.

2.2 Implementation delays leave consumers exposed

The unexplained delay in implementation of the SPF to 31 March 2027 leaves consumers exposed to ongoing and escalating harm for an extended period. This is particularly concerning given the SPF was passed by Parliament in February 2025, with designation originally expected to take effect in mid-2025.

On the current trajectory, consumers will remain without the protection of enforceable obligations for close to two additional years, during which we are observing first-hand scam activity continuing to grow in both scale and sophistication including increased use of AI which is proliferating across every aspect of our lives with limited guardrails to address potential harm. The delay in implementation of the SPF is having real consequences for consumers, who will continue to experience preventable financial and personal harm in the absence of stronger protections.

It is critical that the final SPF rules and code obligations set a significantly higher bar of obligations on regulated entities than current voluntary practice. The trade-off for the significant delay must be stronger, clearer and more enforceable requirements that drive meaningful changes in behaviour and investment across the banking, telecommunications and digital platform sectors.

We reiterate here and throughout this submission the need for the framework to include clear minimum standards and immediate intervention requirements, rather than relying heavily on flexible, subjective, principles-based drafting that will take years of judicial interpretation to clarify. It is essential that once it is implemented, the SPF delivers robust, consistent and enforceable protections that improve outcomes for consumers.

2.3 Critical sectors and platforms remain outside the SPF

Entire high-risk sectors remain outside the SPF, despite playing a significant role in scam activity and consumer losses. It is critical to ensure work is already underway to expand the scope of the SPF to other high-risk sectors and that these sectors are on notice and taking action to prepare.

Our frontline experience demonstrates that a broader list of digital platforms, payment platforms and the superannuation sector are significant enablers of scam activity. Their absence from the framework creates an unacceptable gap in consumer protection.

Given the significant delays that have occurred in implementing the SPF for even the few sectors that have been designated, it is also important that the Government identify a more efficient and much timelier mechanism for expanding scam prevention obligations across the economy. For example, Government could designate additional sectors without codes, bringing them into scope of the SPF principles and ensuring they have a baseline of regulation and accountability.

Digital platform coverage should be expanded

The proposed definition of digital platforms falls well short of a world-leading scam prevention framework. It is built around a narrow and static list of services that reflects where scammers operated in the past rather than where they operate today or will operate tomorrow. Major scam vectors including online marketplaces, dating platforms, email services, app stores, job boards and non-paid internet search results are excluded entirely, creating obvious gaps that sophisticated scam networks can exploit.

This is particularly concerning given that many of these excluded services are already associated with significant scam harm. Romance scams remain one of the most financially and psychologically damaging forms of fraud in Australia. In 2025 alone, Australians reported more than $28.6 million in losses to romance scams, with more than 80 per cent of losses involving online contact methods, including dating platforms and social media.[1] Online marketplace scams are also increasing, with scammers routinely operating as both buyers and sellers to deceive consumers.[2]

---

[1] Australian Competition and Consumer Commission, *Understand How Criminals Exploit Online Relationships and Inflict Heartache* (Media Release, dated 5 February 2026).
[2] Yasmine Wright Gittins and Penny Travers, '*How to Protect against Scams when Buying and Selling Online on Facebook Marketplace and Gumtree*', *ABC News* (online, dated 30 December 2025).

Scammers adapt far faster than governments can update designation instruments, meaning the framework risks becoming outdated from the moment it commences. We already observe scammers innovating like water around protections, such as crypto blocks by banks, to find an alternative way to scam more victims. The three sector designations create a set of holes and roadmap for the scammers to exploit. A world-leading scam prevention regime should be broad, technology-neutral and capable of responding to evolving scam risks across the digital ecosystem. Instead, the current approach creates a regulatory perimeter that scammers can simply step around.

At a minimum, baseline SPF obligations should apply across all digital platform services, regardless of service type. More prescriptive obligations could then be applied proportionately based on the size, reach and risk profile of the service. This would ensure that scam prevention protections remain effective as technologies evolve, while recognising that larger platforms should be subject to stronger obligations commensurate with the risks they create.

The revenue and active Australian user tests further limit the scope of the digital platform designation. It is unclear which platforms would be included and excluded. Government should, at minimum, publish information on which platforms would be included under the proposed definitions.

All payment platforms must be included

Regulatory attention in recent years has rightly been focused on banks. However, as noted in our joint submission on the SPF draft law package and position paper of 24 December 2025[3], our services have seen a corresponding shift towards the use of fintech payment platforms and remittance services, such as Revolut and Western Union, to facilitate scam transactions. Risk exposure through remittance services is heightened for diaspora communities given their heavy reliance on these services. The continued exclusion of these services risks displacing scam activity, rather than reducing it.

Evidence from the UK Payment Systems Regulator shows that smaller and non-bank payment service providers receive disproportionately high levels of authorised push payment scam activity, relative to their transaction volumes.[4] This indicates that scam risk is not limited to traditional banks and may concentrate in alternative payment channels, particularly where regulatory controls are less developed. The UK's Payment Systems Regulator found that non-direct payment service providers received 34 per cent of authorised push payment scam value, despite handling only 19 per cent of consumer

[3] Consumer Action Law Centre *et al*, *Joint Consumer Submission – Scams Prevention Framework Draft Law Package and Position Paper* (24 December 2025) p14–15

[4] UK Payment Systems Regulator, '*Authorised Push Payment (APP) Fraud Performance Data*' (Web Page, undated).

Faster Payments[5] by value and accounted for 48 per cent of fraudulent transactions while processing only 10 per cent of transaction volume.[6]

Specific proposed exemption for purchased payment facilities

The draft rules include an exemption for providers of purchased payment facilities (**PPFs**), creating a gap in the application of the SPF within even the small scope of regulated payment services currently designated.

PPFs facilitate consumer payments and fund transfers and may be used in scam pathways in a similar way to other regulated payment services. Given PPF providers operate within the regulated payments framework, it is unclear why they should be excluded from SPF obligations. Excluding these services risks undermining the effectiveness and consistency of the SPF by allowing comparable payment activity to fall outside its scope.

Case Study

Mario was the victim of an online financial scam that used multiple communication channels. The scammer contacted Mario on Instagram, Discord, WhatsApp, Messenger and via phone calls.*

In February 2026, the scammer called Mario and left a message requesting a prompt return call, noting that there was an urgent matter to discuss. When Mario returned the call, the scammer claimed to have been diagnosed with lung cancer and said they faced losing their USA visa unless they received a large amount of money quickly. The scammer's story created urgency and while Mario initially refused the scammer's requests for money, the scammer was persistent and eventually persuaded Mario to send the funds.

Mario first attempted to transfer money to the scammer through a major bank, but when that transaction remained pending, Mario followed the scammer's instructions to use the Wise money-transfer app and made multiple transactions beginning in late February 2026. Mario had never used Wise prior to being told to use it by the scammer.

Some money was returned to Mario by the scammer in partial amounts. The scammer also provided Mario with a photo of what he claimed to be his passport and visa information, which may have been used to create the appearance of legitimacy. Despite some partial repayments, Mario lost approximately $10,000.

**Name changed*

[5] The UK payment system that provides near real-time payments, as well as standing orders and forward-dated payments.
[6] Ibid.

Our superannuation is a sitting duck for scammers

Similarly, the superannuation sector remains a significant vulnerability.

The sector has repeatedly been called out and put on notice[7] for the millions of Australians' superannuation savings being lost to scammers, yet under the proposed SPF, they remain subject to no scam obligations. Given the size of assets held ($4.3 trillion) and the severe, lifelong impact it can have on victims, there is a strong case for designating this sector as a matter of urgency.

Case Study

Genevieve lost approximately $130,000 after being persuaded by scammers to invest her savings in a fraudulent cryptocurrency investment scheme.*

She withdrew the money from her superannuation balance and subsequently transferred the full amount to accounts controlled by the scammers. Despite the unusually large withdrawal of retirement savings and the transfer of the entire amount to a high-risk investment, neither the superannuation fund nor the bank intervened or identified the transactions as potential scam activity.

Geneivieve lost their retirement savings and was unable to recover the funds.

**Name changed*

Recommendations:

1. Apply SPF obligations across all digital platform services, regardless of service type.

2. Remove the exemption for PPFs so SPF obligations apply consistently across regulated payment services that facilitate consumer fund transfers and present scam-related risk exposure.

3. Commit publicly to a clear timeline for expanding SPF designations to additional high-risk sectors (including non-bank payment platforms, dating apps and superannuation).

4. Consider alternative approaches to expanding the SPF to prevent ongoing significant delays.

[7] Australian Securities and Investments Commission, *ASIC urges super trustees to step up and address serious gaps in anti-scam and fraud protections* (Media release, dated 4 February 2026).

3 SPF rules

Key points

- The proposed Statement of Compliance framework is inconsistent with the legislation and will not reduce information asymmetry as it allows high-level assertions of compliance without case-specific evidence, such as timelines, alerts, intervention steps or internal decision-making.
- The proposed Statement of Compliance framework may weaken accountability compared to existing IDR requirements, particularly for banks under RG271, leaving consumers without enough information to understand, challenge or escalate decisions.
- Short form Statements of Compliance should only be permitted where full compensation is offered to the victim. Otherwise they create additional risks, including automated responses, low-value settlement offers and pressure on consumers to resolve complaints without full information.
- The definition of a scam should remain broad and flexible. Further exclusions risk creating gaps in SPF coverage and excluding conduct that commonly forms part of scam activity.

3.1 Proposed Statement of Compliance will not fulfil its intended purpose

The proposed Statement of Compliance framework will not deliver on the intended purpose of the SPF Bill, that is, lifting and delivering strong protections for consumers.[8] In fact, it undermines it.

The Revised Explanatory Memorandum makes clear that Statements of Compliance are intended to reduce information asymmetry by providing consumers with sufficient information to assess whether to pursue external dispute resolution (**EDR**).[9] It further provides that where a regulated entity provides a Statement of Compliance that does not meet SPF obligations, it must assess whether this caused loss to the consumer.[10] Where loss or damage is identified, the entity is expected to provide compensation or another appropriate remedy.[11]

[8] Stephen Jones, *Second Reading Speech, Scams Prevention Framework Bill 2024*, House of Representatives, dated 7 November 2024).
[9] Explanatory Memorandum, *Scam Prevention Framework Bill 2024* (Cth) [para 1.275].
[10] Ibid, [para 1.276].
[11] Ibid.

However, the draft rules allow for high-level, self-described assertions of compliance without requiring disclosure of underlying evidence, metrics or incident-specific information or data. This represents a significant departure from the original policy intent, and risks entrenching, rather than reducing, existing information imbalances.

Scam victims are victims of crime, yet many never report a scam incident due to feelings of shame or futility. The current approach to Statements of Compliance risks reinforcing this dynamic by providing conclusions without sufficient explanation or evidence, which may lead victims to internalise blame or believe they have no rights and deter them from progressing their complaint to EDR. The Statement of Compliance framework must provide consumers with the information needed to meaningfully understand or challenge decisions and reverse the onus of proof onto entities, when it comes to accessing dispute resolution.[12]

Proposed Statements of Compliance will not rebalance information asymmetry

The proposed Statement of Compliance framework sets a low IDR bar for regulated entities and indeed requires nothing additional of banks than existing IDR obligations under the ASIC's RG271. RG271 already requires banks to investigate complaints, provide consumers with a written response explaining the outcome and reasons for a decision, and support escalation to AFCA. These obligations exist alongside detailed record-keeping and reporting requirements.

More transparency is needed in the context of a scam because consumers are largely in the dark on what has transpired and they have no access to scam intelligence, as compared with regulated entities.

Statements of Compliance must include case-specific evidence

Statements of Compliance should include case-specific evidence showing how the regulated entity complied with its relevant SPF obligations. This should include timelines, scam indicators, alerts triggered, warnings issued, intervention steps taken, recall or disruption actions, and the reasons for any decision not to intervene or compensate.

For banks, this should include (but not be limited to): confirmation of payee outcomes, warning information, recall notices, time stamps and transaction monitoring records.

For telcos and digital platforms, this should include (but not be limited to): equivalent evidence about scam content and pages the user interacted with, traffic disruption, user/ad/account verification, content removal, direct notification and information-sharing.[13]

---

[12] Zali Steggall, *Parliamentary Debates*, House of Representatives, (*Scams Prevention Framework Bill 2024*, Second Reading) 6 February 2025.

[13] Noting the detailed information required to make Statements of Compliance useful documents, steps must be taken to ensure they are only provided to the scam victim or an authorised representative.

There is also a risk that claims of commercial confidentiality may be used to withhold relevant data that would be central to a victim's decision on whether to pursue their claim at EDR.[14] The Statements of Compliance should offer consumers tools to dispute such claims, rather than reinforcing entities' rights to withhold.

Conditional support for short Statement of Compliance

The proposed option for short Statements of Compliance worsens these risks by creating the potential for highly standardised, automated responses. This may increase pressure on consumers to accept early settlement offers without having all the information required to make an informed decision.

Quote from Anna Meulman, Managing Solicitor, Consumer Action Law Centre

'On the frontlines, we routinely hear from people who have lost huge sums of money – often their life savings – to scams. This immediately places people into drastic financial hardship. Despite this, time and time again we hear that banks fail to respond in a timely way, and with compassion or care, let alone take responsibility for the failures of their systems to protect their customers' money.

In particular, we hear that in dispute resolution, banks make paltry and miniscule offers of compensation. They expect consumers to be grateful for these token offers so that they can wash their hands of liability. Scam victims tell us they find these responses by banks galling, insensitive and insulting, particularly given they trusted these institutions to look after their money in the first place.'

While we see the benefit of encouraging early resolution and settling of complaints, reducing delays and providing a simplified pathway for consumers, without additional safeguards, short Statements of Compliance could come at the expense of transparency, empowerment and fairness for consumers. On this basis, their use should be limited to matters where the consumer is made whole, they have provided informed consent and non-disclosure agreement clauses do not apply.

[14] In our frontline casework, it is almost universal that banks refuse to disclose information about their internal processes, fraud detection systems or decision-making when responding to scam complaints.

Recommendations

5. To achieve Government's intended policy outcome, Statements of Compliance should require regulated entities to provide the consumer with case-specific evidence to assist them to understand and assess how the entity has met its obligation, including timelines, alerts, warnings, intervention steps, recall or disruption actions, and reasons for any decision not to compensate.

6. Confidentiality claims should not be used to withhold evidence consumers need to assess or challenge an outcome.

7. The use of a short Statement of Compliance should be limited to circumstances where the consumer is made whole through reimbursement and they have provided informed consent.

8. The use of non-disclosure agreements should be prohibited in all cases.

9. Regulated entities should be required to publicly report on the number of Statements of Compliance they issue, and the consumer outcome for each.

3.2 Definition of a scam

The proposed definition of a scam should remain broad and flexible. Scams continue to evolve rapidly, and any further exclusions should be carefully considered to ensure scam conduct is not unintentionally excluded from the SPF.

Treasury's consultation paper proposes excluding misleading or deceptive conduct by legitimate businesses and Australian Financial Services Licensees from the definition of a scam. We do not support any further exclusions.

While not all misleading or deceptive conduct is a scam, many scams involve misleading or deceptive representations that induce a consumer to authorise a payment or transfer funds.[15]

Many scams involve misleading or deceptive conduct that appears legitimate to consumers, including fake investment opportunities, fraudulent online businesses, business email compromise scams involving apparently legitimate invoices, and

[15] National Anti-Scam Centre, *Targeting Scams: Report of the National Anti-Scam Centre on Scams Data and Activity 2025* (March 2026) 3–5. The top five scam types by loss in 2025 were investment scams, payment redirection scams, romance scams, phishing scams and remote access scams. These categories accounted for 60% of total reported scam losses.

impersonation scams where consumers believe they are dealing with a genuine organisation.[16]

Any further exclusions should therefore be approached cautiously to ensure scam conduct is not intentionally excluded from the SPF. Broad exclusions risk creating gaps in SPF coverage and weakening the effectiveness of the framework by allowing scam conduct to fall outside its scope.

Recommendation

10. The definition of a scam should remain broad and flexible. No further exclusions should be introduced unless it can be demonstrated that they will not create gaps in SPF coverage or unintentionally exclude scam conduct from the framework.

[16] Australian Competition and Consumer Commission, *Beware of fake invoices from scammers impersonating businesses*, (Webpage, 4 April 2024).

4 SPF codes

Key points

- The codes rely heavily on vague undefined terms (e.g. “reasonable steps”, “as soon as practicable”) without clear minimum requirements, risking inconsistent implementation and poor accountability.
- The codes focus too much on whether processes exist, rather than whether they are effective to prevent, detect and disrupt scams, encouraging tick-box compliance instead of real consumer protection.
- Stronger obligations are needed for faster, proactive intervention across all sectors, including direct consumer notification, accessible reporting pathways, trauma informed human support and safeguards for vulnerable consumers.
- Sector-specific obligations need to be stronger and more prescriptive, including high-risk transaction triggers for banks, robust verification and takedown duties for digital platforms, and stronger identity, trust marking and blocking obligations for telcos.

4.1 All codes must create robust and enforceable obligations

As mentioned throughout this submission, a consistent concern across all sector codes is that they rely too heavily on broad, principles-based obligations without setting clear, enforceable minimum standards. Terms such as "reasonable steps", "appropriate measures", "proportionate action" and “risk based” are used extensively[17] but are not well defined.

Reasonable processes do not mean effective processes. Throughout the proposed obligations, reasonableness must be replaced with effectiveness tests.

While a degree of flexibility across regulated entities is fair given differences in size, resources and customer profiles, some activities are so central to effective scam prevention that they require clear minimum standards.

4.2 Vulnerable consumers require proactive protections across all sector codes

While scam methodologies are increasingly sophisticated and there is effectively a scam targeting every segment of the community, Scamwatch data shows that consumers

[17] For example: the term "reasonable" is used 44 times in the body and a further 9 times in headings and definitions in the draft common code.

experiencing vulnerability are often disproportionately exposed to scam harm and may experience more severe financial and non-financial consequences.[18] Our frontline services also reflect this reality.[19]

The SPF codes should:

- Require all regulated entities to proactively identify and support consumers who may be at higher risk of scams.
- Adopt a scams-specific understanding of vulnerability that recognises that vulnerability may arise from personal, situational or market-related factors, and may be temporary, sporadic or ongoing.
- Require regulated entities to proactively identify indicators of vulnerability and treat vulnerability as a relevant scam-risk factor when monitoring activity, assessing scam risk and deciding whether intervention is required.
- Require banks to provide trauma-informed customer support by a specialist team including follow up and guidance to customers with clear next steps and referrals (IDCARE, etc.) and extra care for those identified as vulnerable.

Scam vulnerability is not confined to one sector: consumers may be exposed to heightened risk through banking transactions, telecommunications contact, digital platform activity, or a combination of all three. A framework that only responds when a consumer asks for help places too much burden on victims and fails to reflect how scams operate in practice.

The codes should therefore include clear obligations for regulated entities to identify indicators of vulnerability and provide tailored support before, during and after scam exposure. This should include staff training, proactive identification processes, additional intervention steps for higher-risk consumers, and accessible pathways for urgent assistance and hardship support where relevant. These obligations should apply consistently across banking, telecommunications and digital platforms, while allowing for sector-specific implementation.

Scams acutely and specifically impact First Nations consumers. Measures used in the SPF to identify and respond to scams must also consider the special needs of First Nations consumers, especially in remote communities. This would include cultural awareness training from top to frontline staff and availability of specialised staff to receive First Nations complaints and respond accordingly.

---

[18] Australian Competition and Consumer Commission, *Targeting Scams: Report of the National Anti-Scam Centre on Scams Data and Activity 2025* (March 2026) 37-40.

[19] Consumer Action Law Centre, '*Ongoing and Significant Harms': New Data Shows Millions Still Lost to Scams in Late 2025* (Media Release, January 2026).

Case study

Lily is a scam victim who lost more than $385,000 over a two-year period. Lily has an acquired brain injury, partial deafness, epilepsy and severe depression as a result of a car accident.*

Around November 2024, a scammer befriended Lily on Facebook. The scammer then took the conversation to WhatsApp. Once he had gained Lily's trust, the scammer started requesting money from Lily for various reasons. Lily was assured by the scammer that she would be paid back.

The scammer instructed Lily to purchase Apple gift cards, remove the protective strip on the back of each card and send photos of the revealed codes. Most of the money Lily used to purchase the Apple gift cards was obtained when she withdrew cash, typically between $1,000 and $5,000, from a major bank. She would then proceed to a nearby post office to complete the gift card purchases.

In early 2025, Lily went to her bank to withdraw money as usual. A bank employee spoke with her privately and asked whether she was being scammed. Lily initially denied it but then started crying and admitted that she was. The bank manager said that if she was being scammed, they would need to close her account and would not be able to continue doing business with her. By this point, Lily had slightly less than $55,000 left in her account. The bank manager wrote Lily a cheque for the remaining balance in her account. Lily then took the cheque to another major bank across the road, where she opened a new account and lost further money through the scam.

**Name changed*

Recommendation:

11. All regulated entities should be required to proactively identify and support vulnerable consumers, adopting a scams-specific understanding of vulnerability (further detail in section 4.2).

12. Measures used in the SPF to identify and respond to scams must also consider the special needs of First Nations consumers, especially in remote communities. This would include cultural awareness training from top to frontline staff and availability of specialised staff to receive First Nations complaints and respond accordingly.

4.3 Broad discretion undermines accountability and consistency

A lack of prescription creates a risk of inconsistent and weak implementation across sectors, which may require years of judicial interpretation to establish clear case law and precedent. This creates two related concerns:

- **Reduced accountability and enforceability** - broad discretion makes it more difficult for consumers, AFCA and regulators (including through the Statement of Compliance) to assess whether obligations have been met and distinguish between compliant and non-compliant conduct. This creates enforcement challenges. In practice, determining whether a system was "reasonable" may become highly dependent on expert evidence and institution-specific assessments. This will further entrench the power and information asymmetries throughout dispute resolution between victims and multiple regulated entities

- **Inconsistent consumer outcomes** - consumers facing similar scam risks may receive different levels of protection depending on the institution involved. ASIC Report 761 identified significant differences in scam prevention, detection and response practices across major banks.[20] The purpose of the SPF codes is to fundamentally overcome this and deliver clarity and consistency in outcomes for consumers.

4.4 Processes must be effective, not merely exist

The codes place greater emphasis on the existence of processes, such as monitoring, verification and investigation, rather than whether those processes are effective in preventing scam harm.

This risks encouraging "tick-box" compliance, where entities can point to systems and procedures without demonstrating that those systems are actually preventing, detecting or disrupting scams – again, contrary to the purposes of the SPF legislation. This issue is particularly clear in the telecommunications context, where the code often allows providers to determine for themselves whether identity verification, traffic monitoring or disruption processes are adequate, without setting clear minimum standards. Across all sectors, the codes should require regulated entities to demonstrate that their systems are effective in reducing scam harm, not merely that those systems exist.

The codes should include clear expectations for how entities identify recurring failures, improve systems after scams occur, and report on outcomes such as scams detected, actions taken, consumers notified, funds recovered, scam content removed, traffic disrupted and response times.

[20] Australian Securities and Investments Commission, *Scam prevention, detection and response by the four major banks*, Report REP 761 (dated April 2023), p24

4.5 Timely and proactive intervention is essential

The codes do not sufficiently require timely, proactive intervention, which is critical in the context of scams. The repeated use of vague standards such as "as soon as practicable" fails to ensure that entities act quickly enough to prevent harm, particularly given how rapidly funds can be transferred or scam content can spread.

4.6 Direct notification should be the default across all sectors

Regulated entities should be required to notify consumers directly and promptly, as timely, specific information is critical to preventing further harm. Public communications should only be used where direct notification is not practicable. Notifications should be meaningful and tailored, explaining why activity is high-risk (e.g. based on actionable scam intelligence, fraud alerts or transaction indicators for banks), rather than generic warnings, and should support consumers to take protective action, report scams and pursue redress. Communications should take into account known vulnerabilities such as language barriers or prior victimisation.

Case study

Tom transferred $300,000 to a scammer relating to a fake investment. The bank identified the payment as a high-risk transaction which raised a fraud alert and appropriately blocked the payment and contacted Tom. The fraud alert recorded the transaction as high risk of fraud. The alert noted that the transaction was suspicious as:*

- *There was an abnormally high interest rate, and*
- *The investment was found on a fake comparison website.*

The bank rang Tom, who asked why the transaction was blocked and was told that it was probably because it was a large amount to a 1st time payee. Tom proceeded with the transaction. Tom instructs that had he been told that the rate was very high and the featured on a fake comparison website, he would not have proceeded. AFCA found the warning to be sufficient.

**Name changed*

4.7 Accessible scam support must be a cross-sector minimum standard

Scam victims often need immediate assistance to prevent further loss and understand what steps to take next. All sector codes should therefore require regulated entities to provide accessible scam reporting and assistance channels, including prompt access to trauma-informed human support. This is essential to ensure consumers are not left navigating automated systems or fragmented processes in urgent, high-stress situations.

4.8 Stronger accountability mechanisms are needed

The absence of strong accountability and enforceability mechanisms makes it difficult for regulators to assess compliance and for consumers to challenge failures. Taken together, these issues risk limiting the effectiveness of the framework and undermine its ability to deliver consistent, real-world improvements for consumers. Stronger codes would combine high-level principles with defined minimum standards for key activities, improving consistency, enforceability and consumer protection. This approach aligns with the *Banking Code of Practice*,[21] where broad commitments are supported by more specific operational requirements.

4.9 Actionable scam intelligence obligations must be future proof across all codes

The codes should ensure that all regulated entities are required to act on actionable scam intelligence, regardless of the form it takes or whether it fits neatly within sector-specific categories. Scam intelligence may relate to a bank account, phone number, digital platform account, advertisement, message, URL, crypto wallet, identity credential or other emerging scam indicator.

If obligations are too narrowly framed, there is a risk that the codes will quickly become outdated as scammers change tactics or exploit intelligence gaps between sectors. To remain effective, the codes should require banks, telecommunications providers and digital platforms to monitor, assess and act on all relevant scam intelligence, including intelligence that does not fall within a prescribed or anticipated category.

[21] For example, *Banking Code of Practice* (2025), paras 52–54 &167–185.

5 SPF banking code

Key points

- Banks are often the final point to prevent scam losses, but the draft SPF banking code leaves too much discretion about when and how they must intervene.
- The SPF banking code should prescribe high-risk indicators and require stronger intervention, including tailored warnings, enquiries, delays, pauses or blocks.
- Recall, notification and risk assessment obligations need clearer timeframes, direct consumer warnings and safeguards to ensure risk assessments do not delay action.
- Cryptocurrency transactions and vulnerability indicators should be expressly treated as high-risk and trigger enhanced protections.
- Banks should be required to monitor and act on defined scam intelligence sources, including warnings from regulators, other banks, law enforcement and industry information-sharing.

Banks play a critical role in scam prevention. They monitor transactions, identify suspicious activity, intervene before funds are transferred, and support recovery. As the sector authorising payments, they are often the last point at which losses can be prevented.

Banks are already subject to significant legal and regulatory obligations, including in relation to fraud. For example, s 912A(1)(a) of the *Corporations Act* 2001 (Cth) requires financial services licensees to provide services "efficiently, honestly and fairly", which has been interpreted as requiring adequate systems, controls and active risk management.[22] This obligation was reinforced just weeks ago by the Federal Court of Australia in *ASIC v HSBC*.[23] Legal principles relating to fraud recognise that banks may need to act where there is a serious or real possibility of fraud.[24] In these circumstances, the focus is not merely on whether appropriate systems exist, but also on whether the institution responds appropriately to the risks it has identified.

[22] *ASIC v RI Advice Group Pty Ltd* (2022) FCA 496; *Lipkin Gorman v Karnale Ltd* [1989] 1 WLR 1340 [Para 65].
[23] *Australian Securities and Investments Commission v HSBC Bank Australia Ltd*, FCA, 18 June 2026.
[24] *Lipkin Gorman v Karnale and Lloyd's Bank* (1989) 1 WLR 1340. The court stated 'it was an implied term in the contract between a bank and its customer that it owed him a duty of care which required it not to pay his cheque without inquiry where it knew facts which would have led a reasonable and honest banker to consider that there was a serious or real possibility that the customer might be being defrauded by the drawing of the cheque'.

By contrast, while the draft SPF banking code requires banks to identify and take action to limit high-risk transactions, it leaves substantial discretion regarding when intervention occurs and what action should be taken once a scam risk is identified.[25]

Banks have made positive strides in disrupting scams through their payment channels, including through measures implemented under the 2023 *Scam-Safe Accord*[26]. For example, the rollout of Confirmation of Payee across the banking sector through 2024–25 has delivered significant baseline protections providing consumers with greater confidence in knowing who they are dealing with, materially reducing the risk of being manipulated into paying a scammer when the name does not match the account details they have been given.

While this is important progress, each bank's approach to scam prevention continues to vary significantly, highlighting the gaps in consumer protection. For example, we see cases in our frontlines of scammers coaching vulnerable consumers to open accounts with digital banks as there is no human interaction which may otherwise identify that the consumer may be more at risk of being scammed, whether due to low digital literacy, language barriers or disability.

Where a bank has this knowledge, it is better placed to proactively intervene and make meaningful inquiries of transactions. We see other cases of scammers coaching consumers to open an account with a bank that has minimal or no restrictions on payments to crypto platforms, a known scam vector[27]. Scammers are aware of, and weaponise, protection gaps. We need to remove these gaps and establish a consistent baseline of protections across all banks as a matter of urgency.

Case Study

Alex lives with her family and experiences developmental delay, learning disabilities, and autism spectrum disorder. She requires support to navigate complex systems and has limited experience with financial products beyond basic banking.*

Alex was experiencing social isolation and using online platforms to seek connection and companionship. She met a man through a dating application who encouraged her to move the conversation to another messaging platform.

The scammer communicated frequently with Alex and shared personal stories about his work overseas and plans to move to Australia once his contract finished.

[25] Treasury, *Competition and Consumer (Scams Prevention Framework—SPF Codes) Instrument 2026*, Exposure Draft, ss 3-4, 3-6 and 3-7.
[26] Australian Banking Association, *Keeping Australia Scam Safe,* (Webpage, undated).
[27] Australian Financial Crimes Exchange, *Half of all scam funds flow to cryptocurrency* (Webpage, dated 14 August 2023).

Once Alex began to trust the scammer, he convinced her to open a bank account online and accounts with multiple cryptocurrency exchanges despite her having no experience with it.

The scammer told Alex he needed to borrow approximately $600,000 for work and promised to pay the money back with 50% interest. Over a two month period, Allison made 41 separate transfers to the bank account and then sent money to the crypto accounts.

When Alex said she had no money left, he put more pressure on Alex and claimed he was being sentenced to jail by his company. Alex believed she was helping someone she trusted and took out a $50,000 loan from another bank which was transferred to the scammer.

Soon after, contact stopped and Alex realised she was a victim of a scam. Alex reported the scam to the banks and crypto platforms but none of the money could be recovered. Alex lost her entire life savings.

Alex made a complaint to AFCA, but they found in favour of the bank. AFCA concluded the bank was not on notice of Alex's vulnerability (despite the bank not having anywhere for Alex to disclose her vulnerabilities at time of sign-up), the transactions were processed in accordance with legal obligations, the bank's monitoring systems were not triggered by the transactions, and reasonable attempts were made to recover funds once the scam was reported.

The bank offered Alex a $2,000 goodwill payment, but this did not address her devasting financial loss. The scam, the bank's response, and AFCA's decision have had a significant and lasting impact on her mental health and wellbeing.

**Name changed*

Based on insights and data from our frontlines, we recommend that the SPF banking code include the following prescriptive baseline standards.

5.1 High-risk activity should trigger enhanced scrutiny and intervention

Provision 3–4 requires banks to maintain "reasonable systems" to identify high-risk activity but provide limited guidance on what should trigger scrutiny or intervention.

The SPF banking code should include a non-exhaustive list of factors giving rise to a presumption that a transaction is high-risk. These should include but not limited to:

- new or unusual payees;
- high-value or high-velocity payments;

- behaviour inconsistent with a consumer's usual patterns (including behavioural biometrics such as irregular mouse or device use);
- unusual destinations, particularly overseas accounts;
- indicators of account compromise such as multiple logins or atypical IP addresses;
- payments to cryptocurrency platforms (see further below); and
- indicators of consumer vulnerability.

Receiving banks should be expressly required to disrupt scams such as business email compromise by monitoring for anomalous inbound transactions (for example, rapid, large deposits into personal accounts) and freezing funds pending investigation. Mandatory delay settings should also apply to receiving banks: a one business day hold on large deposits, and three business days for deposits into new accounts unless the purpose has been verified in advance.

Effective intervention depends not only on detection but on the quality of the bank's response. Generic warnings or passive acknowledgements are insufficient where credible scam indicators exist. Banks should be required to provide clear, tailored engagement explaining why a transaction has been identified as high-risk, enabling the consumer to make an informed decision. Where appropriate, banks should delay, pause or block transactions and undertake further verification before processing. Records of warnings and interventions (including in-app alerts, SMS, email, websites and IVR messages) should be retained and made available to consumers, including as evidence for any Statement of Compliance.

Stronger prevention controls should also be mandated. These include (but are not limited to):

- comprehensive staff training on scam typologies, vulnerability indicators and signs of customer coaching;
- prescribed enquiry protocols for high-risk transactions (covering the purpose of the payment, how it arose and whether it has been independently verified);
- strengthened onboarding controls with mandatory multi-factor authentication (**MFA**), including at least one biometric factor, and MFA for high-risk account changes such as adding new devices, payees or increasing limits[28];
- restrictions on the number of devices linked to an account unless verified; and

[28] Note: strengthened authentication requirements should not exacerbate financial exclusion. Banks must continue to accept alternative forms of identification in line with AUSTRAC's Alternative Identification guidance to help prevent financial exclusion among people already experiencing vulnerable circumstances.

- deliver one-time passcodes only through secure in-app channels and provide in-app confirmation that customers are communicating with the bank.

The SPF banking code should recommend as good industry practice the use of behavioural biometrics and device intelligence to detect anomalous activity, suspicious devices and unusual access patterns.

Case Study

Julie is an older person who received what appeared to be a fraud alert from her bank regarding suspicious transactions. After calling the number provided, she spoke with a person she believed was a bank representative, who instructed her to log into her banking app that she hadn't used in a few years and to enter her pin to reverse several transactions.*

The following day, Julie attended a bank branch and discovered that approximately $35,000 had been withdrawn through 17 separate transactions, leaving less than around $60 in her account.

The bank recovered around $15,000. Julie tells us the bank advised her that the transactions had not been flagged because the individual payments were relatively small and the correct PIN had been used. Despite 17 transactions occurring in less than a day and almost completely emptying the account, no intervention occurred before most of the funds were lost.

The bank offered $5,000 to resolve the complaint, an offer that would leave Julie to bear a significant unrecovered loss.

**Name changed*

5.2 There should be prescribed timeframes for recall requests

The requirement on a bank to make recall requests "as soon as reasonably practicable" lacks urgency and fails to provide certainty to consumers regarding timeframes.

Scammers act quickly to move funds. Payment recall requests should be subject to clearly defined, short timeframes to maximise the likelihood of recovering funds. Unless exceptional circumstances apply, sending banks should request the return of funds within one hour of identifying the scam or being asked to do so by the consumer, and a receiving bank should return funds within 24 hours of such notification if the funds are available.

This obligation could be framed as "as soon as practicable *but no later* than 1 hour." This would ensure the obligation sets a minimum compliance expectation without putting a ceiling on compliance where it can be proved a bank could be reasonably expected to

act more quickly. This construction could be used throughout the codes when adding specificity to ensure a compliance floor is set without inadvertently creating a ceiling.

5.3 Cryptocurrency should be explicitly included as a high-risk category

The draft SPF banking code does not expressly recognise cryptocurrency-related transactions as a high-risk category despite clear evidence that cryptocurrency transactions present elevated scam risk.[29] We regard this as a fundamental gap: payments to these channels must be managed safely to address known risk.

While cryptocurrency transactions may be captured by broader high-risk provisions, reliance on implicit coverage creates uncertainty and may lead to inconsistent treatment across institutions. Cryptocurrency transactions are favoured by scammers because funds can be transferred rapidly, moved across jurisdictions and, once transferred, are difficult to recover.

The *Scam Safe Accord* described crypto platforms as "high-risk getaway vehicles used by scammers to move money out of Australia".[30] These characteristics reduce opportunities for intervention and recovery. Without clearer expectations, consumer protections may vary between institutions and limit the effectiveness of scam prevention measures.

At a minimum, the SPF banking code should require banks to block transfers to known scam-linked exchanges and impose appropriate delays or limits (we suggest a minimum of one business day) to other crypto platforms.

5.4 Risk assessments should support, not delay, intervention

Provision 2-15 requires banks to undertake a risk assessment and disruption action that is proportionate to the identified risk. While risk assessments are appropriate, the SPF banking code should make clear that they are not intended to delay intervention where credible scam indicators are present.

The recent Federal Court proceedings in *ASIC v HSBC* highlights the importance of this approach. HSBC admitted in Federal Court proceedings that it failed to maintain adequate controls despite increasing impersonation scam risks, demonstrating that

[29] Australian Competition and Consumer Commission, *Targeting Scams: Report of the National Anti-Scam Centre on Scams Data and Activity 2025* (March 2026) p36. The highest overall losses in 2025 were made by cryptocurrency/Digital Currency Exchange (3,993 transactions) which accounted for 36.2% of overall losses with $121.3 million reported lost. This has been a significant shift from bank transfers in 2024.

[30] Australian Banking Association, *Banks Unite to Declare War on Scammers* (Media Release, 24 November 2023).

identifying scam risks without taking effective action can still result in substantial consumer harm.[31]

Similarly, the obligation to take "proportionate" action would benefit from greater clarity. Where a bank has identified strong indicators of scam activity, the SPF banking code should clearly set out the circumstances in which protective action, including pausing, delaying or blocking a transaction, is expected.

Recommendations

13. Require banks to identify high-risk activity using prescribed minimum indicators and take effective action, including tailored warnings, direct notification, transaction delays or blocks and receiving-bank disruption.

14. Require stronger security controls, including MFA, secure one-time passcodes, staff training and fraud-detection tools.

15. Require sending banks to initiate recall requests within one hour and receiving banks to return available funds within 24 hours, unless exceptional circumstances apply.

16. Expressly treat cryptocurrency-related transactions as high-risk and require controls such as delays, monitoring, verification and blocking transfers to known scam-linked exchanges.

17. Make clear that risk assessments must not delay intervention where credible scam indicators are present.

[31] Michael Atkin, '*HSBC agrees to pay $35 million penalty after widespread scam failures*', ABC News, 18 June 2026.

6 SPF digital platform code

Key points

- The draft digital platform code risks becoming a tick-box compliance regime, allowing platforms to point to verification, monitoring and review processes without showing they reduce scam activity or consumer harm.
- Verification obligations are too weak and narrow, relying on "reasonableness" and focusing on new users and paid ads, while failing to adequately address existing scam accounts, repeat offenders and commercial activity occurring outside paid ads.
- Stronger disruption obligations are needed, including mandatory response and takedown timeframes, precautionary action where credible scam indicators exist, and direct notification of users where they can be identified.
- The framework does not reflect how scams operate across platform ecosystems or keep pace with emerging threats, including AI-enabled scams. It should require platform-wide monitoring, updates to detection systems over time, and searchable ad libraries for scrutiny.

6.1 The code obligations are a tick-box approach

The proposed obligations in the draft SPF digital platform code emphasise preventative measures such as user verification, advertiser verification, advertisement review and targeted warnings. While these obligations may appear substantial, many simply reflect practices that major digital platforms already purport to be undertaking. As a result, platforms may be able to demonstrate compliance while scam accounts, scam advertisements and scam content continue reaching consumers at scale. The preventative obligations do little beyond codifying some of the lowest hanging fruit. This is a long way from the Government's initial goal to create the "world's toughest anti-scam laws."[32]

Internal Meta documents from late 2024 projected that the company would earn around 10 per cent of that year's total revenue – around USD$16 billion – from hosting advertising for scams and banned goods.[33] Digital platforms have a perverse incentive to find a home for scam content somewhere on their platforms, and these obligations do very little to

[32] Stephen Jones and Michelle Rowland, *Parliament Passes World-Leading Scams Prevention Framework* (Joint Media Release, 13 February 2025).
[33] Reuters, '*Internal Documents Show Meta Is Earning Billions of Dollars from a Deluge of Fraudulent Ads*', *ABC News* (dated 7 November 2025).

counter that. Actively profiting off scam victims should be illegal and subject to strong penalties, but the draft SPF digital platform code does not make this so.

6.2 Verification obligations don't go far enough

Individual user and advertiser verification are presented as some of the strongest preventative obligations in the draft SPF digital platforms code. However, the obligations are significantly undermined by the absence of minimum standards, and the reliance on a flat "reasonableness" test. This must be replaced with "effective".

The code requires platforms to verify users and advertisers but provides little clarity regarding what minimum verification must actually involve. This creates a situation where vastly different verification approaches may all be treated as compliant. A platform relying primarily on self-declared information and automated screening may be just as compliant as a platform conducting rigorous identity and business credential checks. It is not at all clear where the line will be drawn.

The focus on new accounts only also allows existing scam accounts to continue to operate unverified.

This is particularly concerning given that many major platforms claim to be already conducting advertiser verification, business verification and account reviews. Yet, clear scam ads continue to be shockingly easy to find across major digital platforms. The code risks simply formalising and endorsing existing practices, rather than requiring platforms to ensure their scam prevention measures are actually effective.

A consumer's relationship with a digital platform is fundamentally different to their relationship with a bank or a telecommunications provider, and this should be reflected in the privacy considerations which apply to the different services. For a variety of reasons, including privacy and data security, it would be highly inappropriate for individual users to be forced to upload sensitive personal documents to, for example, Facebook or WeChat in order to prove their identity, even though these practices are commonplace when setting up an account with a bank or a telco. Accordingly, specific minimum requirements, such as the use of certain identity documents for verification purposes, are less appropriate for digital platforms than for banks and telecommunications.

To resolve this issue, we encourage the Government to frame the verification requirements for digital platforms around an outcomes-based effectiveness test, and set out clear and specific ways that this effectiveness can be assessed. The SPF digital platforms code should set out that, for the purposes of determining whether a digital platform has effective verification processes in place, the following factors may be considered:

- The number of verification failures (i.e. accounts that are verified by the platform but then engage in scam activity)
- The number of scam accounts identified during or following verification.
- The number of repeat-offenders detected by the platform.
- The number of accounts suspended or removed due to verification failures.
- The number of previously removed scam actors prevented from creating new accounts.
- The effectiveness of verification controls in reducing scam activity and consumer exposure to scams.

In order to drive accountability and transparency, these factors should also be the subject of periodic mandatory public reporting.

Recommendations:

18. Verification requirements should apply to both new and existing accounts.

19. The Government should frame the general verification requirements for digital platforms around an outcomes-based effectiveness test, and the code should set out that, for the purposes of determining whether a digital platform has effective verification processes in place, the following factors may be considered:
    - The number of verification failures (i.e. accounts that are verified by the platform but then engage in scam activity).
    - The number of scam accounts identified during or following verification.
    - The number of repeat-offenders detected by the platform.
    - The number of accounts suspended or removed due to verification failures.
    - The number of previously removed scam actors prevented from creating new accounts.
    - The effectiveness of verification controls in reducing scam activity and consumer exposure to scams.

20. The above factors should also be the subject of periodic mandatory public reporting.

21. Advertiser verification requirements should require a check of government-issued identification.

6.3 The obligations focus on account types rather than scam risk

The verification obligations in the SPF digital platforms code focuses heavily on new users and paid advertisers, while providing limited coverage of other high-risk commercial activity occurring on digital platforms.

Scammers do not confine themselves to paid advertising channels. They frequently operate through business accounts, marketplace activity, and influencer-style promotion, as well as groups, pages and accounts that transition from personal to commercial use over time.

The current focus on specific account categories rather than the underlying scam risks has the potential to create a two-tiered system, with scammers easily able to pivot their activities to the types of accounts that are subject to less rigorous verification requirements.

Digital platforms should be required to detect potential commercial activity outside of paid advertisements, triggering advertiser verification requirements.

Recommendation:

22. Potential commercial activity outside of paid advertisements should trigger advertiser verification requirements.

6.4 Licence verification should extend beyond financial services

Scam activity is not confined to financial services. Accordingly, we support a broad principle that where an advertiser is offering a product or service that requires a licence, registration or authorisation to operate legally in Australia, digital platforms must verify that authorisation before permitting the advertisement to be displayed.

The EU Digital Services Act provides a useful precedent through its "traceability of traders" obligations, which require online platforms to collect and assess information about business users (such as identity, payment and registration information) before they can offer goods or services to consumers.[34] This supports a broader verification model that is not confined to financial services and better reflects scam risks across regulated activities.

Consumers are routinely targeted through advertisements relating to housing, migration, employment, health services, charitable donations and other regulated activities. Restricting licence verification to some industries but not others would create incentives for scammers to shift into other sectors where consumers face substantial financial, safety and wellbeing risks.

[34] Article 30, the Digital Services Act (DSA).

Examples of licences, registrations and authorisations that should be captured include:

- Australian Financial Services Licences (AFSLs);
- Australian Credit Licences (ACLs);
- Authorised Deposit-taking Institution (ADI) licences;
- Australian Business Number (ABN)
- Migration agent registration;
- Real estate agent licences;
- Health practitioner registration;
- Building and trade licences;
- Gambling and wagering licences; and
- Motor vehicle dealer licences.

A principles-based approach is preferable to maintaining a fixed list in the code, however we encourage the Government to consider listing some further examples from other industries in the Explanatory Memorandum, to make it clear that this obligation does not only apply where the advertiser is a financial services business. Scam risks evolve rapidly and new high-risk sectors may emerge over time, and so the framework should be capable of capturing any activity that requires a licence, registration or authorisation under Australian law.

We also strongly support the requirement for platforms to verify an advertiser's purported registered charity status, through the Australian Charities and Not-for-Profits register.

Recommendation:

23. Government should make it expressly clear through the Explanatory Memorandum that licence verification requirements apply to all regulated activities requiring legal authorisation, not just those in the financial services sector.

6.5 Warnings should not become a substitute for intervention

The draft SPF digital platforms code places considerable emphasis on targeted warnings for consumers who are at a higher risk of exposure to scams.

While warnings may have some value, they are among the weakest interventions available to platforms. Research shows that once a scammer has established trust and

created a sense of urgency, victims often proceed despite warnings or questioning from banks and other third parties.[35]

There is a risk that the framework encourages platforms to rely on warnings as a compliance mechanism rather than taking stronger preventative action.

Recommendation:

24. Government should make clear that warnings are supplementary measures along with interventions such as content restriction, account limitations or removal.

6.6 Disruption obligations are weak

The disruption provisions in the SPF digital platforms code are intended to ensure digital platforms act to prevent consumer harm once scam activity has been identified.

In practice, the disruption framework is heavily focused on investigations, assessments and procedural requirements, while imposing very limited expectations regarding how quickly platforms must intervene.

This reflects a broader issue throughout the SPF. The Government has developed a framework that may prove effective at requiring platforms to identify scams, investigate scams and document scams. However, it is not clear that it will be effective at requiring platforms to stop scams.

6.7 The code contains no meaningful expectations regarding speed

One of the most significant weaknesses of the disruption framework is the lack of clear response and takedown timeframes. Requiring action "as soon as practicable" provides little practical guidance, giving platforms broad discretion and leaving consumers with no certainty.

Speed is critical: rapid intervention can limit harm, particularly for high-risk content like scam ads, fake investments and impersonation campaigns. Under the current drafting, removing a scam within an hour or after several weeks may both meet the same obligation. This risks incentivising technical compliance over effective disruption. Without mandatory response standards, the code may produce inconsistent outcomes across platforms and undermine its core objective of preventing and limiting scam-related harm.

[35] Which?, *The Psychology of Scams: Understanding Why Consumers Fall for APP Scams* (December 2022) p 25–26. The report found that victims frequently continued with transactions despite warnings or questioning because they had already accepted the scammer's narrative and trusted the scammer.

Recommendation:

25. Government should establish clearer, mandatory response and takedown timeframes for scam advertisements, impersonation content and other high-risk scam activity.

6.8 The framework assumes disruption should occur only after certainty exists

The draft SPF digital platforms code provides limited clarity regarding what action should be taken where scam indicators have been identified but an investigation has not been completed.

This creates a potentially significant gap in consumer protection. Where a platform identifies credible indicators of scam activity, there may be a substantial period between initial detection and a final determination that the content constitutes a scam. During this period, potentially harmful content may remain visible to consumers and continue causing harm.

The draft SPF digital platforms code should adopt a stronger disruption approach. Where credible indicators of scam activity exist, the default response should be to reduce consumer exposure to the risk while investigations are undertaken. If subsequent investigations determine that the activity is legitimate, those measures can be reversed.

Recommendation:

26. Government should require platforms to take precautionary disruption measures immediately by blocking suspected scam content and suspending associated accounts, and reverse those measures later if the activity is ultimately found to be legitimate.

6.9 The framework does not reflect how scams operate in practice

The draft SPF digital platforms code contains a long list of obligations relating to verification, monitoring, investigation and disruption. However, many of these obligations appear to have been designed around regulatory categories rather than the realities of modern scam activity.

Scams do not respect service boundaries or operate within neatly defined product categories. Simultaneously, consumers do not distinguish between separate services operated by the same platform.

Yet the framework repeatedly approaches scam prevention as though these distinctions matter. The result is a framework that risks addressing scams as the Government categorises them rather than as consumers experience them – this is a further example of a design that is not consumer-centred.

6.10 The framework regulates platform services separately, but this does not reflect the way that scammers and consumers use these platforms

One of the main gaps of the draft framework is its continued reliance on service-by-service regulation.

Consumers experience services such as Facebook, Facebook Messenger and Facebook Marketplace as parts of a single platform ecosystem. Scammers exploit them the same way as well. A scam may begin through a recommendation algorithm, move into private messages, direct consumers to a marketplace listing and ultimately redirect victims to an external website.

From the consumer's perspective, this is a single scam occurring within a single platform environment, but the framework treats it as a series of separate services with separate obligations. The practical consequence is that platforms may be able to satisfy obligations within one or more individual services while failing to address scam risks emerging across their broader ecosystem.

The combination of patchy designation coverage and patchy obligations in the SPF digital platforms code as currently drafted will create needless imbalances in the protections in place for consumers. Page 51 of the Explanatory Memorandum notes that "if suspicious activity is flagged in a user's social media post, the entity's processes may require an investigation of that user's instant messaging activity for the purposes of determining whether the activity is or may be a scam." But it fails to acknowledge that the same requirement does not appear to apply to a scam that originates in a Facebook Marketplace ad, even though both may then progress to Messenger.

Consumers should not receive weaker protection because a scam moved between products owned and operated by the same company – one of the most well-resourced and technologically capable in the world. If the Government is not willing to designate services such as email and Facebook Marketplace, then it should at the very least require platforms to include such services in their detection activities where they also operate them.

Recommendation:

27. Government should require genuinely platform-wide monitoring, intelligence sharing, risk assessment and disruption obligations across interconnected services operated by the same platform group or company.

6.11 The framework is already struggling to keep pace with emerging scam threats

The code's treatment of AI-enabled scams is surprisingly limited. It understates the extent to which these technologies are already being used by scammers. Deepfake videos, synthetic voice cloning, AI-generated websites and AI-generated scam advertisements are no longer theoretical concerns. They are already being deployed to increase the scale, sophistication and credibility of scam campaigns.

Recent events demonstrate how quickly scam techniques are evolving beyond the assumptions underpinning the framework.

In June 2026, ABC News uncovered a sophisticated investment scam that used AI-generated images of journalists, politicians and public figures, alongside a near-perfect clone of the ABC News website, to promote a fraudulent investment platform. The operation used paid social media advertisements, fabricated news stories and AI-generated imagery to create the appearance of legitimacy. The scam is estimated to have stolen at least $350 million globally, with one Australian victim reportedly losing more than $500,000. Despite complaints from ABC and repeated reports identifying the scam, the advertisements continued to appear on Meta's platforms.[36]

This illustrates both the growing sophistication of AI-enabled scams and the limitations of existing platform detection and enforcement systems.

Yet the framework remains largely focused on current systems and processes rather than ensuring platforms continuously adapt to evolving threats. This is reflected in the code's treatment of AI-enabled scams. The Explanatory Statement refers to "deepfake" and "AI-generated" imagery only as examples of suspicious content that platforms may scan for when monitoring advertisements. The framework contains no dedicated obligations, minimum standards or performance expectations relating to AI-enabled scam activity.

[36] Fell, J., & Fankhauser, J. *The fake ABC News articles trying to sell you a scam*, ABC News, online, 23 June 2026. ABC reported that the scam used AI-generated images, cloned ABC News webpages, paid social media advertisements and a fake investment platform, with estimated global losses of at least $350 million and individual Australian losses exceeding $500,000.

A static compliance framework is unlikely to remain effective in an environment where scam methodologies change rapidly and increasingly rely on technologies that reduce the cost and effort required to deceive consumers.

The framework risks becoming outdated before it is implemented.

Recommendations:

28. Government should require ongoing testing, review and updating of scam detection and disruption capabilities to ensure platforms remain capable of responding to evolving scam threats.

29. Government should require digital platforms that run advertisements to maintain accessible and searchable ad libraries for users and regulators to cross-check ads.

7 SPF telecommunications code

Key points

- Telecommunications are a core scam pathway, with scammers using calls and messages to reach consumers. Given telco services underpin access to banking, healthcare, government and emergency services, stronger scam protections are essential.
- The SPF telco code needs clearer, more prescriptive identity verification, including stronger Know Your Customer (**KYC**) obligations, rights of use checks, business verification, and alternative identity pathways to prevent digital exclusion.
- Sector-wide controls are needed for high-risk services, such as prepaid SMS limits, SIM registration caps and future-proofed actionable scam intelligence obligations.
- Providers must be responsible for protecting consumers, including proactive support for vulnerable consumers, blocking known scam numbers, trust marking, and a centralised Australian Communications and Media Authority (**ACMA**) managed Do Not Originate list.
- Actionable scam intelligence rules are too narrow and risk becoming outdated. They must be broadened to cover all relevant actionable scam intelligence, not just linked to phone numbers so obligations keep pace with evolving scam tactics.

7.1 Telecommunications are a frontline scam pathway

The telecommunications sector plays a critical role in the scam ecosystem, serving as a primary pathway through which scammers reach their victims. Whether through voice calls or messages, telecommunications networks are, alongside digital platforms, the key infrastructure that connects fraudulent actors to consumers.

According to the National Anti-Scam Centre's 2025 Targeting Scams Report, phone scams tend to generate higher individual losses than other contact methods, with a median loss of $3,800 per victim, while losses from text message scams rose from $14.0 million in 2024 to $17.9 million in 2025, reflecting the growing scale and sophistication of telecommunications scams.[37]

Telecommunications is an essential service that underpins access to other essential services, including banking, healthcare, government services, and emergency support.

[37] National Anti-Scam Centre, *Targeting Scams: Report of the National Anti-Scam Centre on Scams Data and Activity 2025* (Report, Australian Competition and Consumer Commission, 30 March 2026), p 35.

As consumers increasingly rely on mobile connectivity to manage daily life, telecommunications have become an attractive and high-value vector for scammers and fraudsters seeking to exploit that trust. Protecting consumers from telecommunications scams is therefore fundamental to keeping essential services safe and accessible for all Australians.

7.2 The SPF telecommunications code should strengthen Know Your Customer requirements

Prescriptive obligations should be introduced to strengthen KYC requirements. While we appreciate that the SPF telco code seeks to provide flexibility for regulated entities to determine identity verification methods and processes, the lack of any prescriptive obligations in the code affords considerable discretion to telecommunications providers regarding the adequacy of such measures.

It is anticipated that telecommunication providers may comply with the SPF telco code obligations through compliance with other regulatory instruments, including the Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017, the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 and the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022.

While we support this, we understand that there are instances of identity verification that fall outside these instruments (such as where an entity registers a postpaid service to a new customer). These instances are left without meaningful prescriptive steps or guardrails that set expectations for the standard of identity verification.

The Explanatory Material expects that regulated entities may meet the requirement by "sighting of multiple points of reliable identity documents that are independent of each other, or the use of an identity verification service as defined by the Identity Verification Services Act 2023 or use of the Digital ID System".[38] We consider such expectations should be elevated to requirements in the SPF telco code itself to ensure appropriate and consistent standards of identity verification. At minimum, the SPF telco code should specify that multiple forms of independent, reliable identity documents are required to verify the consumer's identity.

In addition, we recommend the SPF telco code place an active requirement on telecommunications providers to conduct rights of use (**ROU**) checks for customers of all telecommunications services before entering a contract. While clause 7 of the draft SPF telco code requires providers to prevent the carriage of calls or messages where the party does not hold ROU to the number, the SPF telco code does not place a positive

[38] Explanatory Material, *Competition and Consumer Amendment (Scams Prevention Framework—Telecommunications Code) Instrument 2026*, p2.

obligation on providers to conduct ROU checks, except in limited circumstances. We consider ROU checks are not an onerous requirement. As the Explanatory Statement asserts, originating carriage service providers should have reason to believe a customer has ROU to a number. Inserting a positive obligation for originating carriage service providers to conduct ROU checks would ensure stronger customer verification and enable trust marking to be broadly applied to telecommunications traffic, enabling greater protections for consumers.

7.3 Identity verification requirements must balance robustness and flexibility

Identity verification requirements are an important measure to combat scams and fraud, but in some cases, they have exacerbated digital exclusion among vulnerable consumer cohorts. Consumer reports from First Nations communities have raised concerns about identity verification requirements that bar consumers from activating prepaid services because of difficulties in sourcing sufficient identity documents.

Similarly, disability advocates have raised concerns regarding inaccessible identity verification requirements that prevent people with disabilities from accessing communications services. Therefore, it is critical that stronger KYC requirements are carefully designed to balance the need for effective scam prevention measures with the promotion of equitable access to communications services for all consumers, whilst also ensuring that those same consumers are not exposed to greater risk of scams and fraud. Financial service providers already accept alternative forms of identification in line with AUSTRAC's Alternative Identification guidance to help prevent financial exclusion among people already experiencing vulnerable circumstances.[39]

7.4 There should be greater requirements to verify business customers

Where a customer is or represents to be a business customer, additional identity verification steps should be taken to confirm the business is legitimate and the person has the authority to act as its representative. To verify business customers, requirements in the SPF telco code should mirror those in the *Telecommunications (SMS Sender ID Register) Industry Standard 2025* and the *SMS Sender ID Register (Application, Access and Administration) Determination 2025*. The instruments set out requirements for verifying ABN and non-ABN entities and an entity's authorised representatives.

Including comparable requirements in the SPF telco code would ensure consistent standards of identity verification between the SPF and SMS Sender ID Register, while not imposing greater regulatory burden on regulated entities. To ensure strong protections,

[39] AUSTRAC, '*Identifying Individuals Who Don't Have Standard ID*' (Webpage, last updated 27 Mar 2026).

the strengthened identity verification requirements we have proposed should be applied throughout the SPF telco code for customers of all telecommunications services, including high-risk telecommunication services.

Recommendations:

30. Strengthen identity verification requirements to explicitly require regulated entities to use multiple forms of independent identity documents to verify customer identity.

31. Require telecommunication providers implement rights of use checks for customers of all telecommunications services prior to entering a contract.

32. Ensure identity verification requirements enable the use of alternative identity verification methods to promote safe and equitable access to communications services for all consumers

33. Include additional requirements to verify business customers, including the legitimacy of the business, the authority of the contact to act on behalf of the business, and the legitimate use case for the telecommunications service.

7.5 Prepaid limits should be consistent across the sector

A prescribed limit on high-volume pre-paid SMS traffic is needed

The SPF telco code affords discretion to telecommunications providers to set appropriate prepaid message volume limits. It is our understanding that businesses do not typically use prepaid services to send high volumes of SMS traffic and therefore, we consider there are little grounds for varying discretionary prepaid message limits across the telecommunications sector. Rather, we recommend the SPF telco code set an overarching, consistent and appropriate limit for the acceptable volume of prepaid messages within a set period.

In this setting, if necessary, provisions could be made to allow businesses to apply to their telecommunications provider by exception to increase the prepaid message limit if the customer's identity, business, and authorisation is verified and the business can establish a legitimate use case. When considering applications to raise prepaid message limits, providers should be obligated to consider the matters set out at clause 16 of the SPF telco code.

A limit on the number of prepaid SIM cards available to purchase and register per customer is needed

While we welcome the proposal to limit prepaid message volumes (albeit at the discretion of providers), the SPF telco code should also set a prescribed, sector-wide limit on the number of prepaid SIM cards a customer can purchase and be registered to. Currently, there are no regulatory requirements in Australia that govern prepaid SIM card limits. Yet prepaid SIM cards are widely used and at scale to perpetrate scams due to their low-cost and weaker registration requirements.

In practice, carriage service providers may set internal customer limits on the number of prepaid SIM cards that can be registered to a customer. For example, Telstra currently restricts customers to having a maximum of 35 prepaid services registered to their name, regardless of how many accounts the customer holds.[40] However, stronger regulatory standards are in place in Singapore that only allow consumers to purchase 3 prepaid and 10 postpaid SIM cards.[41] This limit is imposed alongside identity checks for prepaid consumers.

To strengthen consumer protections, we recommend the SPF telco code explicitly set a sector-wide limit on how many prepaid SIM cards can be registered to one user, and a limit for how many prepaid SIM cards can be purchased in one transaction.

Determining an appropriate sector-wide limit would require meaningful consideration of consumers' use of prepaid services. It is critical prepaid limits do not restrict consumers' legitimate use of prepaid services. Prepaid services are disproportionately relied upon by First Nations and low-income consumers.[42]

Should a prepaid limit be set too low, it would risk exacerbating the digital exclusion of consumer cohorts who already experience a disproportionate level of digital exclusion. Therefore, appropriate prepaid limits must be balanced between the objectives of robust scam protection and ensuring equitable access to communications services. To ensure an appropriate balance, we recommend the regulator conduct further consultation with representative consumer groups.

Some anti-scam controls should not be publicised

Some telecommunications anti-scam controls should not be publicly disclosed to safeguard against scam actors accessing information to help circumvent the controls. For example, where an anti-scam control contains a specific limit or volume, and this is prescribed in a public instrument, this might enable scammers to simply issue

[40] Telstra, *Customer terms update*.
[41] Infocomm Media Development Authority, *Anti-Scam Measures*, updated 30 June 2026.
[42] Daniel Featherstone et al, *Mapping the Digital Gap: 2025 Outcomes Report*. Report, ARC Centre of Excellence for Automated Decision-Making and Society, 3 December 2025.

communications just under the prescribed limit or volume and thus still reach consumers.

This concern could apply to specific prescribed limits for high-volume prepaid SMS traffic and may extend to other prescriptive measures in the SPF telco code. Where anti-scam measures are subject to such restrictions and may need to be communicated less publicly between Government and regulated entities, we consider the regulator should conduct targeted, closed consultation with industry and consumer stakeholders and provide closed guidance to industry participants.

Recommendations

34. Set an explicit sector-wide limit for the acceptable volume of prepaid messages within a set period.

35. Set an explicit sector-wide limit for the maximum number of prepaid SIM cards that can be registered to a consumer, and the maximum number of prepaid SIM cards that can be purchased in a single transaction.

7.6 The onus to protect consumers must be on providers

Stronger requirements are needed to support consumers at higher risk to scams

The SPF telco code fails to oblige telecommunications providers to proactively identify and support consumers, including consumers who may be at higher risk to scams. The drafting does not meet the policy intent of the SPF and further places the burden on consumers to protect themselves from scams.

Clause 17 narrowly places a passive obligation on providers to assist an SPF consumer where the consumer *requests* assistance. We note that obligations in the common code require systems and policies to have regard to types of SPF consumers and staff training to support staff to identify SPF consumers (including those at higher risk). However, these obligations are limited and do not require regulated entities to meaningfully or proactively support vulnerable SPF consumers.

As noted in section 4.2 above, vulnerability should be addressed as a cross-sector obligation across all SPF codes. In the telecommunication context, this is particularly important because telecommunications services are essential services and are frequently used by scammers to reach consumers. The SPF telecommunications code should therefore include clear proactive obligations to identify and support consumers at higher risk of scams, consistent with existing telecommunications standards on financial hardship and domestic, family and sexual violence.

Stronger obligations to protect consumers from known scam numbers are needed

We are also concerned that obligations at clause 25 do not sufficiently place the onus on providers to protect consumers from scams.

Clause 25(2) places a broad obligation on telecommunications providers to take reasonable steps to interrupt a voice call or message where the entity has investigated the activity and determined it is a scam. We consider the drafting of this clause is not sufficiently robust and provides undue flexibility to telecommunications providers that limits their liability to disrupt known scam activities. Instead, the SPF telco code should include a clear presumption that the telecommunications provider is liable if it has failed to block identified scam calls or messages on its network.

In addition, where a consumer contacts a known scam number, telecommunications providers must take reasonable steps to warn the consumer. This obligation is subject to a broad reasonableness test that significantly weakens its operation and therefore, consumer protection.

It is critical that where a telecommunications provider is aware that a number is a known scam number, it is obligated to block all outbound traffic to that number. This provision would reflect the capacity and responsibility of telecommunications providers to protect consumers from scams and strengthen the SPF telco code to provide appropriate consumer protections.

Recommendations

36. Require telecommunications providers to proactively identify vulnerable consumers, in line with clear criteria and obligations.

37. Include a presumption of liability where a telecommunications provider fails to block identified scam calls and messages on its network.

38. Require telecommunications providers to block all outbound traffic to known scam numbers.

7.7 Trust marking is essential and should be mandated

Currently, trust marking in the telecommunications industry is a commercial decision and inconsistently applied across the sector. The SPF telco code requires telecommunications providers to apply network trust information but fails to mandate consumer-facing trust marking of voice calls and messages. The justification and rationale for such discrepancy are not made clear in the Explanatory Statement or consultation materials. We consider it appropriate that where a telecommunications

provider is aware that traffic is legitimate, it should be required to apply consumer-facing trust marking.

Requirements on trust marking should mandate the form and content of trust marks and specify that transiting and terminating providers must carry trust marking to the receiving party unless the entity has reasonable grounds to believe the trust marking has been applied incorrectly. Where trust marking is terminated to the receiving party and later the number is found to be a scam, clear liability should be apportioned to telecommunications providers and compensation paid to scam victims.

Consumer-facing trust marking is essential to ensure consumers can engage in the digital economy with confidence. Consumers frequently screen calls and messages due to scam and spam risks, and scam victims may withdraw from the digital economy due to lost confidence. While the SMS Sender ID Register is a positive step to increase confidence in the legitimacy of SMS sender ID messages, it does not apply to voice calls or non-sender ID message traffic. We therefore recommend the SPF telco code mandate reliable and consistent trust marking in the telecommunications sector to empower consumers to engage in the digital economy and minimise the costs of withdrawal on economic productivity.

Recommendation

39. Mandate consistent industry-wide consumer-facing trust marking.

7.8 Unverified overseas calls should be over stamped to warn consumers

Clause 9 of the SPF telco code requires telecommunications providers to either block or over-stamp the calling line identification (**CLI**) of international calls where the provider is unsure if the traffic is legitimate. However, blocking the CLI of a call may result in the call displaying as "No Caller ID", "Unknown", or similar label to the receiving party. Blocking CLI shares characteristics with legitimate traffic, such as that from government agencies who frequently use "No Caller ID" to contact consumers. In addition, blocking CLI does not provide the consumer with information about the legitimacy of the traffic or sufficiently put the consumer on notice to treat the contact with caution.

We understand that some telecommunications providers already undertake over-stamping of international calls, however current industry practice is inconsistent and subject to commercial decisions.[43] Therefore, to uplift industry practice, we recommend

[43] Telstra Limited, '*Protect Yourself from Scam Calls*'; Alice Chambers, '*Vodafone Uses Network AI to Stop Scam Calls Before They Ring*' (19 April 2026).

that the SPF telco code explicitly require over-stamping international calls with a consistent warning (such as unverified) where the telecommunications provider is unable to determine the legitimacy of the contact to ensure consumers are appropriately warned about the nature of the communication. We also support this obligation being applied to warnings delivered to consumers under clause 24.

Recommendation

40. Require telecommunications providers to over-stamp international calls where the legitimacy of the call is unable to be determined.

7.9 The ACMA should be responsible for a centralised Do Not Originate list

The SPF telco code requires providers to host individual Do Not Originate lists and share the list with other regulated entities. We consider the ACMA should be responsible for hosting a centralised Do Not Originate list for the telecommunications sector. This is commensurate with the ACMA's role in the SMS Sender ID Register and would provide the ACMA with greater regulatory oversight of the operation of the code obligation. This approach also reflects international approaches to the management of Do Not Originate lists.[44]

Recommendations

41. Ensure the ACMA is responsible for managing a centralised Do Not Originate list.

7.10 The enforceability of the telecommunications code must be unambiguous

Unlike the banking, digital platforms, and common codes, the telecommunications code does not specify which, if any, of its provisions are civil penalty provisions. This omission creates significant ambiguity regarding the enforceability of the code.

Without clearly designated civil penalty provisions, regulators may face confusion and difficulty enforcing the telecommunications code with the same rigour applied under the banking and digital platforms codes. Telecommunications providers could therefore be subject to a weaker enforcement regime than their counterparts in other sectors – an

[44] See Ofcom, '*The Do Not Originate (DNO) List'* (23 February 2022); Commission for Communications Regulation, '*Do Not Originate List*' (19 October 2022).

outcome that would be inconsistent with the intent of the SPF and risks undermining its effective and uniform operation across regulated entities.

To ensure consistency and coherence across the SPF framework, the telecommunications code should be amended to expressly identify which of its provisions are civil penalty provisions. We note at least one civil penalty provision applies to nearly all sections of the banking, digital platforms, and common codes. We support adopting a similar approach for the telecommunications code to ensure comparable enforceability.

Recommendations

42. Amend the telecommunications code to explicitly identify which provisions are subject to civil penalties.

43. Include numeric sender IDs under the definition of high-risk telecommunications services.

44. Include specific SPF telco code obligations regarding appropriate actions and assistance a telecommunications provider must provide where disruptive action has been taken in error.

45. Require telecommunications providers to record how it established a legitimate use case under clause 6 and the evidence relied upon.

46. Apply clause 8(3), clause 9 and clause 10 to overseas messages using Australian numbers to future proof the telecommunications code.

47. Require disruption disputes to be escalated to the ACMA and SPF regulator.

8 Dispute resolution

Key points

- The SPF must create a single, coordinated multi-party IDR system where all regulated entities involved in a scam participate from the outset, rather than leaving consumers to coordinate disputes across banks, telcos and digital platforms.
- Consumers should have one entry point and one consolidated outcome, with transparent decision-making, clear governance, enforceable cooperation obligations and proper record-keeping.
- Automatic compensation should be set at a meaningful level, with the threshold increased to $10,000, so lower-value claims are resolved quickly and do not unnecessarily burden EDR.
- Consumers must not face reduced rights, fees, excesses, non-disclosure agreements or limits on AFCA's fairness jurisdiction. The dispute resolution system must remain free, accessible, transparent and capable of delivering fair outcomes.

8.1 Multiparty system for IDR – a vision of the SPF with consumers at the heart

As set out in **Appendix C** of this submission, and consistent with our previous submission of 24 December 2025, a multiparty IDR system will only work for consumers if it includes the following.

A single system where everyone is involved

The SPF must establish a truly unified IDR system where all regulated entities involved in a scam are brought within a single, coordinated IDR process. Scams span multiple sectors and a fragmented system will not deliver fair or timely outcomes.

Responsibility for coordination must sit within the system, not the consumer, with all relevant entities required to participate from the outset. This requires a single designated IDR body capable of managing multiparty disputes across sectors.

One entry point, one coordinated outcome

Consumers should only have to report once to enter the IDR system (i.e. no wrong door, but single entry) and must receive a single, consolidated outcome. The current model risks retaining a siloed approach to dispute resolution, where each entity investigates and reaches decisions independently, forcing consumers to navigate multiple pathways.

In practice, this will require consumers to repeatedly recount their experiences, gather evidence across entities and pursue each organisation separately, effectively acting as "debt collectors" to secure a full remedy. A functional system must instead deliver a streamlined, end-to-end process with shared responsibility and a unified resolution.

Transparent processes and decision-making

Transparency must be embedded across the IDR framework to address existing information asymmetries between consumers and regulated entities. This includes making actionable scam intelligence accessible to AFCA and the Australian Competition and Consumer Commission and being required to publicly report IDR outcomes and performance.

Current IDR processes are opaque and produce different outcomes compared to EDR. This undermines trust. Streamlined or automated processes can be appropriate for low value claims, but this must not come at the expense of transparency in decision-making or outcomes.

Clear governance and an accountability framework

The multi-party IDR system must be supported by clear governance arrangements and strong accountability mechanisms to ensure it functions effectively in practice. This includes clearly defined roles, enforceable cooperation obligations, and requirements for entities to maintain comprehensive records of IDR processes and decisions, enabling regulators to monitor compliance and request information at any time.

Without these foundational elements, there is a risk that coordination remains high-level and unenforceable, leading to fragmented outcomes and limited oversight. A robust governance framework is essential to ensure consistency, transparency and meaningful accountability across all regulated entities.

A prohibition on non-disclosure agreements in scam disputes

Non-disclosure agreements must be prohibited under the SPF.

They undermine transparency and accountability by concealing systemic failures and limiting scrutiny on industry practices, especially in the context of a framework that relies heavily on Statements of Compliance generated by the entities themselves.

Non-disclosure agreements also risk reinforcing information and power imbalances, especially where consumers are pressured to accept low-value settlements without understanding whether a regulated entity met their obligations. A consumer-centered framework must prioritise openness and ensure that settlement outcomes contribute to systemic learning and improved scam prevention.

Recommendations

48. Define enforceable cooperation obligations for regulated entities involved in multi-party scam complaints.

49. Mandate all regulated entities involvement in single multi-party IDR body.

50. Require complaint assessment processes to include human review and consideration of individual scam circumstances, vulnerability and relevant SPF obligations.

51. Support the multi-party IDR system with clear governance arrangements and strong accountability mechanisms to ensure it functions effectively in practice.

52. Ensure IDR rules prohibit the use of non-disclosure agreements or confidentiality clauses in SPF scam settlements.

53. Prohibit any settlement terms that restrict consumers from discussing their scam experience, complaint process or settlement outcome with regulators, dispute resolution bodies, consumer advocates, financial advisors/accountants, or medical practitioners.

54. Ensure settlement processes remain transparent and do not discourage scrutiny of systemic scam prevention failures or industry practices.

8.2 Automatic compensation must be higher to support functional dispute resolution system

We strongly support the introduction of automatic compensation for low-value claims as a means of improving efficiency and accessibility within the dispute resolution system.

However, the proposed threshold of $3,000 is too low to comprehensively achieve this objective and risks limiting the effectiveness of the reform. At this level, a significant portion of scam victims will fall outside the automatic reimbursement process and be pushed into the more complex and resource-intensive pathways, such as EDR. This creates barriers to access, particularly for vulnerable consumers and undermines the goal of delivering timely and accessible redress.

A higher threshold supports the efficiency of the dispute resolution system by reducing the volume of low-value matters progressing to EDR and allowing resources to focus on

more complex cases, particularly where there has been clear breach, so insights can inform improved policies, processes and system design to avoid repeat consumer harm. There are also clear and compelling commercial incentives for businesses to resolve disputes early and quickly.

We are concerned that some regulated entities are fixated on "moral hazard" arguments around mandatory reimbursement which perpetuates victim blaming and fails to acknowledge both the commercial overhead of processing large volumes of scam complaints and the fact that there is no substance to claims that consumers are likely to defraud the system.

A $10,000 threshold would capture a broader proportion of scam losses and reduce reliance on more resource and time-intensive processes. It also recognises that lower-value losses can still cause significant financial harm and improves access to more meaningful and consistent redress.

If regulated entities do not volunteer to adopt this automatic reimbursement model, we consider SPF decision makers should use all available levers to encourage or compel automatic reimbursement. One option available to discourage unnecessary use of AFCA's resources on small value complaints is to build into AFCA's fee mechanism a premium which, in effect, penalises entities that choose not to automatically reimburse complaints of less than $10,000. Another option is for Government to impose a levy on regulated entities that would fund auto compensation.

Recommendations:

55. Increase the automatic reimbursement threshold to $10,000, which would better reflect the scale of scam losses, while remaining cost-effective compared to the expense of the full dispute resolution process. We support the policy direction and encourage Government to strengthen it to ensure the system delivers practical benefits.

56. AFCA should use its fee structure to incentivise full and automatic reimbursement of complaints under $10,000.

8.3 Subset of scam victims must not have their rights limited

Low-value scams should not receive reduced protections under the SPF.

The proposed approach risks creating a two-tier system where complaints are assessed based on the value of the loss rather than the seriousness of harm caused.

Lower value matters are still often complex, involve multiple entities and vulnerable consumers and can cause significant financial hardship. Reduced obligations should only apply if consumers are automatically compensated and made whole again. Otherwise, full SPF obligations must apply. As noted elsewhere in this submission, increasing the automatic compensation threshold to $10,000 would reduce reliance on simplified processes and better support fair, consistent outcomes.

Recommendations:

57. Apply equivalent consumer protections, liability standards and dispute resolution rights to low-value scam complaints.

58. Ensure all complaints remain subject to the full suite of SPF obligations unless consumers receive automatic compensation.

8.4 Liability apportionment

We support the default position of equal apportionment of liability, as it provides a simple and efficient starting point.

However, giving entities the ability to vary apportionment by agreement will create significant risks, as there is little incentive for entities to accept a higher share of liability, especially where large amounts are involved. This will result in disputes, delays and more complaints escalating to EDR.

As noted in our joint submission in the SPF draft law package and position paper of 24 December 2025, we reiterate that consumers should receive compensation upfront based on the default apportionment, with any reallocation resolved between entities later. Otherwise, consumers will face delays and be forced into unnecessary dispute resolution processes, only to then receive compensation which they were originally owed, after an unnecessarily drawn-out process.

Recommendations:

59. The framework should ensure that consumers are compensated quickly based on the default apportionment, with any variations to liability determined between businesses after compensation has been paid. The primary objective should be to ensure that liability allocation does not delay or reduce compensation to consumers.

8.5 Consumers must not pay to access dispute resolution

Dispute resolution under the SPF must remain free, accessible and independent for consumers. This is the cornerstone of dispute resolution in Australia. The SPF is already stacked significantly in regulated entities' favour through legal, power and information imbalances. We can't also trade away fairness and access to the system.

Scam victims are often experiencing financial stress, vulnerability and significant emotional harm when seeking assistance. Any requirement for consumers to contribute to the costs of pursuing a complaint, including through fees, excess payments or other cost-sharing arrangements, would create a substantial barrier to justice and undermine confidence in the framework.

This is particularly important given SPF complaints may involve multiple regulated entities, complex scam pathways and significant information asymmetries between consumers and industry participants. Consumers already face challenges accessing transaction records, internal intervention information and compliance material needed to assess whether SPF obligations have been met.

Consumer access to IDR and external dispute resolution must therefore remain available and meaningful across all scam complaint categories, including low-value complaints.

The Government should not be deterred by self-serving claims from some regulated entities that fees or excesses are necessary to address the so-called "moral hazard". In our extensive experience, consumers never set out to be scammed and evidence from comparable jurisdictions, including the UK, demonstrate that the incidence of fraudulent claims remains low even under more generous reimbursement models.[45] Regulated entities already manage fraud risk as part of their business-as-usual operations and can identify and respond to fraudulent actors. Introducing consumer costs in the name of moral hazard would impose unnecessary barriers without delivering meaningful risk mitigation.

The SPF should not create a system in which a consumer's ability to pursue a fair outcome depends on their financial capacity, vulnerability or ability to navigate complex dispute resolution processes.

There is zero trade off in the SPF for further winding back of consumer rights such as a consumer paying a fee to access dispute resolution. In the UK the fee is in the context of mandatory reimbursement of scam losses up to £85,000 per claim. In Australia, victims have to navigate complex dispute resolution and somehow prove their case against multiple entities who have breached their obligations. It is not a reasonable comparison.

[45] Payment Systems Regulator, *APP scams reimbursement dashboard for Q4 2025*, updated 11 June 2026.

Recommendations:

60. Do not introduce consumer fees, "excess" payments or any other cost-sharing requirements for SPF internal or external dispute resolution processes.

61. Require regulated entities to provide consumers, free of charge and within a prescribed timeframe, with relevant complaint and scam investigation information, including transaction records, intervention actions and fraud alerts.

8.6 Any restriction of AFCA fairness jurisdiction is unacceptable

AFCA's fairness jurisdiction is a critical consumer safeguard and must not be undermined by the SPF framework.

We are concerned by the implication created in the Internal Dispute Resolution position paper that SPF code obligations would displace both existing specific consumer protections and broader considerations of fairness in AFCA's consideration of scam complaints.[46]

AFCA must remain able to consider the full circumstances of a complaint, including fairness, vulnerability, industry practice and other guidance. The SPF should support, rather than constrain, AFCA's broader access to justice function. AFCA serves as a check and balance over IDR to ensure it remains on track and providing justice to victims.

Treasury's proposal asks Australians to accept a system where the odds are stacked against them, where it will take victims of crime great strength, resilience and possibly money to pay a lawyer, to pursue a compensation claim. We have a new multi-party IDR system being built without consumers being consulted at all. The only safeguard victims can hope for is the EDR oversight that was promised throughout development of the SPF.

The fairness jurisdiction is also critical to the SPF's ability to determine (many, even most) cases that don't fit squarely into a sector or category. For example:

- an investment scam where the scammer manipulated the victim into taking out a personal loan, and the bank failed to meet is responsible lending obligations.
- a new technology or scam type - there will always be a risk that new technologies and avoidance techniques will not be explicitly contemplated in legislation.

[46] Points contributing to this impression are in section 'Clear SPF obligations will support consistent and predictable AFCA outcomes' points 2 and 5.

The fairness jurisdiction allows AFCA some flexibility to reasonably adjust to a changing environment (noting that legislation reform is a slow process and would not be applied retrospectively), and where complex cases don't fit neatly into categories.

Recommendations:

62. Preserve AFCA's full fairness jurisdiction and ensure scam complaints continue to be determined based on what is fair in all the circumstances, rather than narrow assessments of SPF code compliance.

63. Maintain AFCA as an independent backstop capable of delivering fair, holistic and outcome-focused resolutions for scam victims.

8.7 The SPF can operate alongside the ePayments Code without conflict

The Internal Dispute Resolution position paper also states that the SPF will take "priority over other applicable frameworks (e.g. ePayments Code)". The introduction of the SPF should not impact or reduce existing protections available to consumers via the ePayments Code.

The SPF code and the ePayments Code operate in parallel and, in practice, address different aspects of scam transactions.

The key issues under the SPF are whether:

- the consumer "authorised" the transaction and,
- if so, whether the bank took appropriate steps to detect, prevent or respond to the scam.

The SPF is directed primarily to the second issue. It imposes obligations on regulated entities to implement scam prevention and response measures, including the use of scam intelligence, transaction monitoring and payment intervention tools.

By contrast, the ePayments Code is concerned with the operation of electronic payment systems and, critically, the allocation of liability for unauthorised transactions. It does not deal with scams as such. Its relevance in scam matters lies principally in determining whether a transaction was "authorised".

Where a transaction is not authorised, the consumer is generally not liable. In those circumstances, the question of whether additional scam prevention measures should have been taken does not arise in the same way.

A central issue in determining authorisation is whether the consumer "voluntarily disclosed" a passcode. AFCA has considered this issue, including in Determination 1016692,[47] confirming that disclosure will not be "voluntary" where a consumer's will is overborne by deception, pressure or threats. Conduct induced by fear of financial loss may therefore not constitute voluntary disclosure.

Against that background, there is a risk that a provision giving the SPF code priority over the ePayments Code could, in practice, undermine the operation of the ePayments Code, particularly the protections in Chapter C relating to unauthorised transactions and passcode disclosure.

If any inconsistencies between the two frameworks are said to arise, they should be clearly identified and subject to consultation. At present, no clear or material conflict has been identified.

More broadly, the two frameworks operate in distinct domains:

- the ePayments Code addresses authorisation and liability;
- the SPF code addresses scam prevention and response.

Importantly, this distinction means there is no policy basis to subordinate or amend the ePayments Code to accommodate the SPF. Each framework performs a different function and should operate without limiting the scope or effect of the other.

The only potential area of overlap is in relation to mistaken internet payments under clauses 26–36 of the ePayments Code, which may in some cases involve scam transactions. However, these provisions are narrowly confined to payment recall processes, and the corresponding SPF obligations are expressed at a high level. Any inconsistency is therefore limited.

[47] Australian Financial Complaints Authority, *Case No 12-00-1016692 (HSBC Bank Australia Limited)* (Determination, 22 August 2024).

Recommendation:

64. Chapter C of the ePayments Code, dealing with liability for unauthorised transactions, should be preserved in its current form;
    a. the SPF code and ePayments Code should operate concurrently, without modification to or limitation of either framework;
    b. there is no clear or substantial conflict between the two frameworks, other than limited overlap in relation to mistaken internet payments; and
    c. any proposal to give the SPF code priority should be supported by clearly identified and demonstrable inconsistencies.

65. Clarify that the SPF supplements, and does not diminish or displace, existing consumer protections under frameworks including the ePayments Code.

Appendix A: Consolidated list of recommendations

Section 2: The SPF remains partial, delayed and risks failing consumers

This SPF does not have consumers at the heart

1. Apply SPF obligations across all digital platform services, regardless of service type.

2. Remove the exemption for PPFs so SPF obligations apply consistently across regulated payment services that facilitate consumer fund transfers and present scam-related risk exposure.

3. Commit publicly to a clear timeline for expanding SPF designations to additional high-risk sectors (including non-bank payment platforms, dating apps and superannuation).

4. Consider alternative approaches to expanding the SPF to prevent ongoing significant delays.

Section 3: SPF rules

Proposed Statement of Compliance will not fulfil its intended purpose

5. To achieve Government's intended policy outcome, Statements of Compliance should require regulated entities to provide the consumer with case-specific evidence to assist them to understand and assess how the entity has met its obligation, including timelines, alerts, warnings, intervention steps, recall or disruption actions, and reasons for any decision not to compensate.

6. Confidentiality claims should not be used to withhold evidence consumers need to assess or challenge an outcome.

7. The use of a short Statement of Compliance should be limited to circumstances where the consumer is made whole through reimbursement and they have provided informed consent.

8. The use of non-disclosure agreements should be prohibited in all cases.

9. Regulated entities should be required to publicly report on the number of Statements of Compliance they issue, and the consumer outcome for each.

Definition of a scam

10. The definition of a scam should remain broad and flexible. No further exclusions should be introduced unless it can be demonstrated that they will not create gaps in SPF coverage or unintentionally exclude scam conduct from the framework.

Section 4: SPF codes

11. All regulated entities should be required to proactively identify and support vulnerable consumers, adopting a scams-specific understanding of vulnerability (further detail in section 4.2).

12. Measures used in the SPF to identify and respond to scams must also consider the special needs of First Nations consumers, especially in remote communities. This would include cultural awareness training from top to frontline staff and availability of specialised staff to receive First Nations complaints and respond accordingly.

Section 5: SPF banking code

13. Require banks to identify high-risk activity using prescribed minimum indicators and take effective action, including tailored warnings, direct notification, transaction delays or blocks and receiving-bank disruption.

14. Require stronger security controls, including MFA, secure one-time passcodes, staff training and fraud-detection tools.

15. Require sending banks to initiate recall requests within one hour and receiving banks to return available funds within 24 hours, unless exceptional circumstances apply.

16. Expressly treat cryptocurrency-related transactions as high-risk and require controls such as delays, monitoring, verification and blocking transfers to known scam-linked exchanges.

17. Make clear that risk assessments must not delay intervention where credible scam indicators are present.

Section 6: SPF digital platform code

The code obligations are a tick box approach

18. Verification requirements should apply to both new and existing accounts;

19. The Government should frame the general verification requirements for digital platforms around an outcomes-based effectiveness test, and the code should set out that, for the purposes of determining whether a digital platform has effective verification processes in place, the following factors may be considered:
    a. The number of verification failures, (i.e. accounts that are verified by the platform but then engage in scam activity).
    b. The number of scam accounts identified during or following verification.
    c. The number of repeat-offenders detected by the platform.
    d. The number of accounts suspended or removed due to verification failures.
    e. The number of previously removed scam actors prevented from creating new accounts.
    f. The effectiveness of verification controls in reducing scam activity and consumer exposure to scams.

20. The above factors should also be the subject of periodic mandatory public reporting.

21. Advertiser verification requirements should require a check of government-issued identification.

The obligations focus on account types rather than scam risk

22. Potential commercial activity outside of paid advertisements should trigger advertiser verification requirements

Licence verification should extend beyond financial services

23. Government should make it expressly clear through the Explanatory Memorandum that licence verification requirements apply to all regulated activities requiring legal authorisation, not just those in the financial services sector.

Warnings should not become substitution for intervention

24. Government should make clear that warnings are supplementary measures along with interventions such as content restriction, account limitations or removal.

The code contains no meaningful expectations regarding speed

25. Government should establish clearer, mandatory response and takedown timeframes for scam advertisements, impersonation content and other high-risk scam activity.

The framework assumes disruption should occur only after certainty exists

26. Government should require platforms to take precautionary disruption measures immediately by blocking suspected scam content and suspending associated accounts, and reverse those measures later if the activity is ultimately found to be legitimate.

The framework regulates platform services separately, but this does not reflect the way that scammers and consumers use these platforms

27. Government should require genuinely platform-wide monitoring, intelligence sharing, risk assessment and disruption obligations across interconnected services operated by the same platform group or company.

The framework is already struggling to keep pace with emerging scam threats

28. Government should require ongoing testing, review and updating of scam detection and disruption capabilities to ensure platforms remain capable of responding to evolving scam threats.

29. Government should require digital platforms that run advertisements to maintain accessible and searchable ad libraries for users and regulators to cross-check ads.

Section 7: SPF telecommunications code

Telecommunications are a frontline scam pathway

30. Strengthen identity verification requirements to explicitly require regulated entities to use multiple forms of independent identity documents to verify customer identity.

31. Require telecommunication providers implement rights of use checks for customers of all telecommunications services prior to entering a contract.

32. Ensure identity verification requirements enable the use of alternative identity verification methods to promote safe and equitable access to communications services for all consumers

33. Include additional requirements to verify business customers, including the legitimacy of the business, the authority of the contact to act on behalf of the business, and the legitimate use case for the telecommunications service.

Prepaid limits should be consistent across the sector

34. Set an explicit sector-wide limit for the acceptable volume of prepaid messages within a set period.

35. Set an explicit sector-wide limit for the maximum number of prepaid SIM cards that can be registered to a consumer, and the maximum number of prepaid SIM cards that can be purchased in a single transaction.

Stronger obligations to protect consumers from known scam numbers are needed

36. Require telecommunications providers to proactively identify vulnerable consumers, in line with clear criteria and obligations.

37. Include a presumption of liability where a telecommunications provider fails to block identified scam calls and messages on its network.

38. Require telecommunications providers to block all outbound traffic to known scam numbers.

Trust marking is essential and should be mandated

39. Mandate consistent industry-wide consumer-facing trust marking.

Unverified overseas calls should be over stamped to warn consumers

40. Require telecommunications providers to over-stamp international calls where the legitimacy of the call is unable to be determined.

The ACMA should be responsible for a centralised Do Not Originate list

41. Ensure the ACMA is responsible for managing a centralised Do Not Originate list.

The enforceability of the telecommunications code must be unambiguous

42. Amend the telecommunications code to explicitly identify which provisions are subject to civil penalties.

43. Include numeric sender IDs under the definition of high-risk telecommunications services.

44. Include specific SPF telco code obligations regarding appropriate actions and assistance a telecommunications provider must provide where disruptive action has been taken in error.

45. Require telecommunications providers to record how it established a legitimate use case under clause 6 and the evidence relied upon.

46. Apply clause 8(3), clause 9 and clause 10 to overseas messages using Australian numbers to future proof the telecommunications code.

47. Require disruption disputes to be escalated to the ACMA and SPF regulator.

Section 8: Dispute resolution

Multiparty system for IDR – a vision of the SPF with consumers at the heart

48. Define enforceable cooperation obligations for regulated entities involved in multi-party scam complaints.

49. Mandate all regulated entities involvement in single multi-party IDR body.

50. Require complaint assessment processes to include human review and consideration of individual scam circumstances, vulnerability and relevant SPF obligations.

51. Support the multi-party IDR system with clear governance arrangements and strong accountability mechanisms to ensure it functions effectively in practice.

52. Ensure IDR rules prohibit the use of non-disclosure agreements or confidentiality clauses in SPF scam settlements.

53. Prohibit any settlement terms that restrict consumers from discussing their scam experience, complaint process or settlement outcome with regulators, dispute resolution bodies, consumer advocates, financial advisors/accountants, or medical practitioners.

54. Ensure settlement processes remain transparent and do not discourage scrutiny of systemic scam prevention failures or industry practices.

Automatic compensation must be higher to support functional dispute resolution system

55. Increasing the automatic reimbursement threshold to $10,000, which would better reflect the scale of scam losses, while remaining cost-effective compared to the expense of the full dispute resolution process. We support the policy direction and encourage Government to strengthen it to ensure the system delivers practical benefits.

56. AFCA should use its fee structure to incentivise full and automatic reimbursement of complaints under $10,000.

A subset of scam victims must not have their rights limited

57. Apply equivalent consumer protections, liability standards and dispute resolution rights to low-value scam complaints.

58. Ensure all complaints remain subject to the full suite of SPF obligations unless consumers receive automatic compensation.

Liability apportionment

59. The framework should ensure that consumers are compensated quickly based on the default apportionment, with any variations to liability determined between businesses after compensation has been paid. The primary objective should be to ensure that liability allocation does not delay or reduce compensation to consumers.

Consumers must not pay to access dispute resolution

60. Do not introduce consumer fees, "excess" payments or any other cost-sharing requirements for SPF internal or external dispute resolution processes.

61. Require regulated entities to promptly provide consumers, free of charge, with relevant complaint and scam investigation information, including transaction records, intervention actions and fraud alerts.

Any restriction of AFCA fairness jurisdiction is unacceptable

62. Preserve AFCA's full fairness jurisdiction and ensure scam complaints continue to be determined based on what is fair in all the circumstances, rather than narrow assessments of SPF code compliance.

63. Maintain AFCA as an independent backstop capable of delivering fair, holistic and outcome-focused resolutions for scam victims.

The SPF can operate alongside the ePayments Code without conflict

64. Chapter C of the ePayments Code, dealing with liability for unauthorised transactions, should be preserved in its current form;
    a. the SPF code and ePayments Code should operate concurrently, without modification to or limitation of either framework;
    b. there is no clear or substantial conflict between the two frameworks, other than limited overlap in relation to mistaken internet payments; and
    c. any proposal to give the SPF code priority should be supported by clearly identified and demonstrable inconsistencies.

65. Clarify that the SPF supplements, and does not diminish or displace, existing consumer protections under frameworks including the ePayments Code.

Appendix B: Responses to consultation questions

General questions
1. Do any of the proposed provisions create conflicting requirements with other elements of the SPF or with other regulations? Yes. Some proposed provisions create tension with existing SPF objectives and other consumer protection frameworks. In particular, the proposed Statement of Compliance rules risk undermining the SPF's intended purpose of reducing information asymmetry, while aspects of the banking code may set a lower practical standard than existing obligations under financial services law and established fraud principles. The SPF should also be clarified so that it supplements, and does not diminish or displace, existing protections under frameworks such as the ePayments Code.
2. Are there any transition arrangements required to support industry compliance? Further transition arrangements should not be used to delay commencement of enforceable obligations. The SPF has already been delayed until 31 March 2027, leaving consumers exposed to ongoing scam harm. To the extent transition arrangements are required, they should be limited, time-bound and directed towards implementation of stronger obligations, not weakening or postponing them. For future sectors, Government should consider faster mechanisms for designation, including bringing sectors within the SPF principles before detailed codes are finalised.
3. Do the draft rules and codes strike the appropriate balance between effective regulation and personal privacy? If not, what changes would you suggest? Not yet. The draft framework does not strike the right balance because it sometimes relies on privacy concerns to justify insufficient transparency, while elsewhere it lacks clear safeguards for identity verification and vulnerable consumers. The SPF should require meaningful disclosure to consumers, AFCA and regulators while protecting genuinely sensitive information and information that could help scammers circumvent controls. Verification obligations should be robust but proportionate, with different expectations for banks, telecommunications providers and digital platforms, and should include alternative pathways so privacy and identity requirements do not worsen digital exclusion.
SPF rules - digital platforms designation exceptions
4. It is intended that the active Australian user test captures users that accessed the service from within Australia at least once during the relevant month. Does the proposed provision achieve this and does the definition of an 'active Australian user' provide sufficient clarity for stakeholders to assess whether a platform meets the 200,000 monthly average Australian user threshold? The proposed active Australian user test may provide some clarity, but we remain concerned that the 200,000 monthly Australian user threshold narrows the framework in a way that is not sufficiently risk-based. Smaller, niche or emerging platforms may still present significant scam risk, particularly where they enable user-to-user contact or

commercial activity. Government should publish information about which platforms would be captured under the proposed test and consider applying baseline SPF obligations to digital platform services based on scam risk, not size alone.

5. Does the proposed revenue test clearly indicate it is intended to apply on a global basis, including to entities that are part of a multinational group with global revenue over $1 billion?

No substantive comment

6. Given that financial reporting periods do not always align with the calendar year, are there any practical challenges with assessing both the active Australian user test and revenue test as at 1 January each year?

No substantive comment

SPF rules - banking designation exceptions

7. Does the proposed definition of an SPF consumer for a covered banking service effectively carve out business-to-business banking services that do not have a direct relationship with SPF consumers?

The proposed definition appears to appropriately seek to exclude back-end business-to-business banking services where there is no direct relationship with an SPF consumer. However, the drafting may create uncertainty in more complex payment chains where a consumer is affected by a banking service but does not have a direct contractual relationship with the relevant entity.

Scams often involve multiple intermediaries, payment processors and banking infrastructure, and the framework should ensure accountability does not fall away simply because the consumer relationship is indirect. The rules should clarify that business-to-business services are excluded only where they do not materially contribute to consumer scam risk, and should explain how responsibility is allocated where a consumer is affected by an indirect or intermediated banking service.

8. Does the proposed exception of providers of PPFs appropriately capture standalone PPF providers? Are there any inadvertent consequences of this exception?

Please refer to 'Specific proposed exemption for purchased payment facilities' under section 2.3.

SPF rules - Statement of Compliance

9. How can the statement of compliance requirements in the SPF rules support the efficient and early resolution of complaints where a complaint is resolved quickly to a consumer's satisfaction?

Please refer to section 3.1, 'Proposed Statement of Compliance will not fulfil its intended purpose'.

Definition of scam
10. What other conduct, if any, should be excluded from the definition of a scam? Please refer to section 3.2, 'Definition of a scam'.
Dispute resolution
11. Should the internal dispute resolution guidance in the SPF rules enable regulated entities to apply a consumer contribution or excess to scam reimbursements? Please refer to section 8.1, 'Multiparty system for IDR - a vision of the SPF with consumers at the heart'.
12. Does an automatic compensation approach for losses under $3,000, as set out in the Internal Dispute Resolution under the Scams Prevention Framework position paper, provide a sensible approach to handling low-value scam complaints in an efficient and proportionate manner? If not, how else can low-value scam complaints be handled efficiently and proportionately? Please refer to section 8.2, 'Automatic compensation must be higher to support functional dispute resolution'.
SPF sector codes - common provisions
13. The draft common code provisions are intended to require regulated entities to work together effectively to resolve multi-party scam complaints through internal dispute resolution (section 2.26). This reflects that a single scam event will often involve several entities. Does the draft code effectively require cooperation between entities during internal dispute resolution to support consumers making complaints involving more than one entity? Please refer to section 8.1, 'Multiparty system for IDR - a vision of the SPF with consumers at the heart'.
SPF sector codes - banking provisions
14. The draft code requires banks to verify the identity of consumers of their services, to prevent any misuse or manipulation by scammers (section 3-3). Is it clear how banks would implement these verification requirements? What further specific actions are appropriate for verification? **For example, how should this obligation interact with existing Know-Your-Customer obligations under Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) law? Should this interaction be made explicit in the legislation?** Please refer to section 5.1 in relation to strengthening account opening protocols through multi factor authentication, including at least one biometric check. Please refer to 'The SPF telecommunications code should strengthen Know Your Customer requirements' under section 7.4.

15. The draft code requires banks to identify transactions or activities that are a high-risk of being used to facilitate scams and take proportionate preventative action to limit scam losses before funds leave the system and it is impossible to recover them (sections 3-4 to 3-7). Is it clear what is meant by transactions and activities that 'have a high risk of being, or facilitating, a scam' (section 3-4)?

Please refer to 'High-risk activity should trigger enhanced scrutiny and intervention' under section 5.2.

16. Does the draft code make it sufficiently clear what steps are expected of banks who identify the transactions or activities referred to in section 3-4?

Please refer to 'High-risk activity should trigger enhanced scrutiny and intervention' and 'Risk assessments should support, not delay, intervention' under section 5.2.

17. Does the draft code include sufficient obligations on sending banks to disrupt scam activity (division 4), and is it clear that the disrupt obligations extend to both sending and receiving banks?

Please refer to 'High-risk activity should trigger enhanced scrutiny and intervention' and 'Risk assessments should support, not delay, intervention' under section 5.2.

18. Do the payment recall request obligations accurately reflect industry practice around payment recalls (section 3-11)? Is there a more appropriate way to frame this obligation?

Please refer to section 5.2, 'SPF banking code'.

Digital platform provisions

19. The draft code provisions for digital platforms are intended to be scalable and workable across different types and sizes of platforms. Do the proposed provisions appropriately address scams across all digital platforms? Do the provisions provide sufficient flexibility to support

compliance by smaller digital platforms?

Please refer to 'Digital platform coverage should be expanded' under section 2.3 and 'The obligations focus on account types rather than scam risk' under section 6.3.

20. The draft code requires digital platforms to verify the details of new users and advertisers (sections 5-3 and 5-4). Is it clear how digital platforms would implement these verification requirements? What further specific actions are appropriate for verification?

Please refer to 'Verification obligations don't go far enough' under section 6.2.

21. It is intended that digital platforms undertake ongoing re-verification of users and advertisers where the platform detects a change in the identity and/or contact information of the account holder to address potential account takeover (sections 5-3 and 5-4). Does the draft code achieve this objective?

Please refer to 'Verification obligations don't go far enough' under section 6.2.

22. Should verification of an advertiser's licence be confined to verification of an applicable Australian Financial Services Licence, Australian Credit Licence and Australian Deposit-taking Institution (ADI) Licence (section 5-4)? What other Australian licences, if any, should be captured?

Please refer to 'Licence verification should extend beyond financial services' under section 6.4.

23. The draft code requires digital platforms to check advertisements before they are published and engage in ongoing monitoring of advertisements (section 5-5). How could the provisions minimise any unintended consequences, particularly for small businesses?

No substantive comment.

24. It is intended that a digital platform operating multiple regulated services be required to have collective processes for monitoring and detecting scam risks across its multiple services (section 5-7). Do the proposed obligations achieve this objective?

Please refer to 'The framework regulates platform services separately, but this does not reflect the way that scammers and consumers use these platforms' under section 6.10.

25. Do the draft code provisions to disrupt suspected and confirmed scam content and advertising (section 5-9 and section 5-11) strike the right balance of proportionate action while minimising unintended consequences?

Please refer to 'Disruption obligations are weak', 'The code contains no meaningful expectations regarding speed' and 'The framework assumes disruption should occur only after certainty exists' under section 6.

26. Are additional safeguards needed to limit potential negative impacts on small businesses who rely on digital platforms for advertising and communication to customers?

No substantive comment.

Competition and Consumer Amendment (Scams Prevention Framework – Telecommunications Code) Instrument 2026 – consultation questions

27. Do the definitions in the draft code correctly reflect the sector and the positions of telecommunications services?

We consider the definitions of the telecommunications code appropriately reflect the position and capacity of telecommunications providers' role in the scams ecosystem.

28. Do the obligations match the role of the entity in the telecommunications ecosystem?

We support the code applying obligations to all regulated entities where possible to ensure it is future proofed against emerging scam harms and trends.

In many cases, originating carriers and originating carriage service providers will have the most visibility and capacity to undertake scam prevention measures. However, transiting and terminating providers should not simply rely on trust that originating providers have complied with SPF obligations or had complete information. Therefore, for a whole of ecosystem approach to the SPF to be effective, transiting and terminating providers must accept responsibility for their role, and be obligated to appropriately verify, monitor, detect, and disrupt traffic where there is a scam risk.

29. The draft provisions consider high-risk services as using Australian numbers from overseas, multiple service practice and sending of bulk SMS, as these services can obscure scam traffic. Are there any other services which should be considered high-risk in the context of scams?

High-risk services should include services using numeric sender IDs (short codes), particularly traffic arriving to Australia via international gateways as these services are excluded from the SMS Sender ID Register.

30. Could any of the obligations impede a telecommunications providers' ability to deliver legitimate, including critical, traffic?

Any obligations on telecommunications providers to disrupt traffic holds some risk of impeding legitimate traffic. However, this risk must be considered against the risk of scam harm to SPF consumers. There are demonstrable scam harms that arise from the misuse of telecommunications channels, and the risk of interrupting or delaying legitimate traffic is outweighed by the risk of scam harm. This principle has already been demonstrated in Government policy making through the establishment of the SMS Sender ID Register – which is a clear indication that the risk of scams outweighs the risk of labelling potentially legitimate traffic as "unverified".

We support greater consideration and specific code obligations regarding appropriate actions and assistance a telecommunications provider must provide where disruptive action has been taken in error. We recommend telecommunications providers are obligated to support SPF consumers following disruptive action in error to restore the consumer to the position they were in prior to the action, particularly where reversal of disruptive action is not practicable (for example, if account recovery is not possible, by supporting the customer as a priority to set up a new account).

31. Are there additional checks that should be undertaken before providing higher risk services, such as the overseas use of numbers or sending of bulk messages?

As outlined in the section above regarding identity verification, we consider that where a customer is or represents to be a business customer, additional identity verification steps should be taken to confirm the business is legitimate and the person has the authority to act as its representative.

These requirements should apply to contracting of all telecommunications services and high-risk telecommunications services. Such requirements should align with the SMS Sender ID Register regulations. We also recommend that regulated entities be required

to record how they established a legitimate use case under clause 6, and what evidence they relied upon.

32. Are there any other scam related reasons a regulated entity should not carry a call or message that should be added to clause 8?

We consider clause 8 appropriately captures high-risk traffic that is likely to be scam activity and should not be carried by telecommunications providers.

33. Are overseas messages using Australian numbers common? Should clause 8(3), clause 9 and clause 10 apply to messages using Australian numbers?

We consider clause 8(3), clause 9 and clause 10 should apply to overseas messages using Australian numbers to future proof the telecommunications code. While there are legitimate use cases of overseas messages using Australian numbers, including international roaming, the prevalence of bulk SMS as a common scam method warrants the inclusion of messages. Applying the clauses to messages would also ensure consistent protection across different covered telecommunications services regulated by the SPF.

34. In your experience with identifying scams, are there any additional scam indicators commonly found in the content of messages that would help with detection?

We support the provisions in clause 20 regarding automated filtering of messages for scam material, including in particular messages that contain a number, email address, URL, or hyperlink.

35. Are there other ways telecommunications services can quickly share scam information on calls and messages they have detected and if so, what regulatory arrangements are needed to support them?

We consider this is a matter for industry and the SPF regulator to resolve through engagement and the National Anti-Scam Centre's consultation on ASI and ASI sharing.

Overarchingly, we support real-time information sharing between telecommunications providers to ensure the effective operation of the SPF.

36. Are the proposed requirements sufficient to assist in resolving disputes where traffic is being disrupted?

The proposed requirements do not appropriately outline how traffic disputes will be resolved under the telecommunications code.

We consider that if a dispute remains once the steps at clause 29 are completed, the dispute should be escalated to the ACMA and the SPF regulator to determine the resolution. The ACMA and the SPF regulator should be obligated to respond to and resolve the dispute within a reasonable timeframe.

Appendix C: A vision of the SPF with consumers at the heart