



Meta's Submission on the *Scams Prevention Framework Bill 2024*

4 October 2024

Executive Summary

Meta shares the Australian Government's intent to prevent scams and disrupt scam networks and we are committed to playing our part to protect Australian consumers from these crimes. The importance of our services to Australian consumers - including through providing a place for people to connect with like communities; share and engage with content and information that they are interested in; access mental health resources and support; or build and grow their business - means that we have a responsibility to protect our users from bad actors and online harms, including the devastating impact caused by scammers.

Meta's approach to combating scams

At Meta, we have every incentive to combat scams. They cause potential harm to our users, can lead to loss of trust in our services and involve abuse of our advertising systems in ways that can undermine our business. This is why - globally and here in Australia - Meta continues to uplift our efforts to combat scams targeting Australians, including most recently through:

- **New National Anti-Scam Centre reporting channels:** This year, we expanded our existing reporting and information sharing partnership with the National Anti-Scam Centre. The early results are promising; for example, between July and August 2024, from 18 pieces of content reported to Meta by the NASC, we were able to widen our search and identify and delete an additional 2,600+ pieces of content that were similar to those originally reported.
- **New intelligence sharing partnership with the banking sector:** We also commenced a new intelligence sharing initiative with the banking industry through the Fraud Intelligence Reciprocal Exchange (FIRE).¹ Of the 102 reports provided via the Australian Financial Crimes Exchange during the three-month pilot phase, Meta was able to conduct a wider investigation and identify and remove over 9,000 Pages and over 8,000 AI-generated celeb-bait scams across Facebook and Instagram.

¹ Meta (October 2024), Meta partners with the Australian Financial Crimes Exchange (AFCX) and Australian banking sector to combat scams
<https://medium.com/meta-australia-policy-blog/meta-partners-with-the-australian-financial-crimes-exchange-afcx-and-australian-banking-sector-to-7b7b26227360>

- **Advertiser verification:** In June 2024, Meta commenced the rollout of phone verification for new advertisers globally and launched SMS verification for higher-risk sellers on Facebook Marketplace in Australia in August 2024.²
- **Strategic network disruption:** In line with our work on countering other adversarial threats, like Influence Operations, Espionage actors etc we have teams that are dedicated and are actively working to disrupt large criminal networks that have been conducting cross-border and cross-industry cybercrimes, including those targeting Australian consumers.
- **Stronger enforcement policies and processes:** Over the past six months, we have further strengthened our policies to enable us to enforce more strictly on scam content on our services. In July 2024, we conducted a targeted search that led to the identification and removal of nearly 20,000 investment scam ads. To build on this investigation and prevent similar ads from running on our services, we then launched an auto-enforcement pipeline on July 15 2024. By August 4, this pipeline had taken down over 21,000 additional ads. Beyond enforcing on specific content and users that violate our policies, Meta has also brought legal action against individuals and entities who have used our platforms to scam people. Examples of this are shared below.
- **Awareness raising to the public:** We continue to run proactive scam awareness and education campaigns targeting Australian consumers, including a new campaign focused on combating scams on WhatsApp. Further details on our consumer education work are outlined below.
- **Local and regional partnerships:** We have continued to advance our anti-scam partnerships with key organisations, not only in Australia, but across the broader Oceania region, including with IDCARE, the Council of Small Business Organisations Australia, Netsafe New Zealand and the Global Anti-Scams Alliance.

To provide greater transparency and accountability for Meta and the broader digital industry's work to combat scams, we were also a founding signatory of the DIGI Australian Online Scams Code of Practice (AOSC), which launched in July 2024.³ The AOSC comprises a holistic range of commitments aimed at combating scams in Australia, traversing blocking and takedown, advertiser verification measures and increased collaboration with the NASC. One of these commitments includes introducing reasonable

² Meta, Business Help Centre, 'About phone verification for new advertisers.'

<https://en-gb.facebook.com/business/help/1064155054687612>

³ DIGI (July 2024), Australian Online Scams Code of Practice. <https://digi.org.au/scams/>

measures to confirm that an advertiser holds the necessary financial services licence to advertise a regulated financial service, which we are working towards launching in Australia in the coming months.

Earlier this year, we also launched the new Anti-Scam Hub in Australia, which is a dedicated website intended to provide a single place for consumers to access information on Meta's anti-scam policies, tools, enforcement and resources.⁴

Comments on the Government's legislative proposals

We have some significant concerns about the workability and likely consequences of the *Scams Prevention Framework Bill 2024* (SPF). Some of our concerns repeat the feedback we provided to the government's initial consultation at the start of 2024. The draft legislation is not evidence based; it may disincentivise continuing industry investment and collaboration in scam prevention; and it risks increasing the attractiveness of Australia for scammers, because of reduced user vigilance.

In addition, the focus of the SPF on regulating industry's approach to combating scams needs to be complemented by commitments from the Government and relevant agencies to play their part in this complex, combative space. We stand ready to assist in sharing our understanding and intelligence about the pernicious and lucrative transnational and organised crime networks that are a significant source of the great majority of scams. With the insights on these underlying trends, it is clear that an effective response requires a wide range of industry players and government to work together with an ecosystem-wide, regional and international response.

Meta hopes that the Government will consider our concerns and proposals in the constructive spirit that we bring to this work and this consultation. We are firmly committed to playing our role in combating scammers to protect Australian consumers, as well as other users of our services across the globe. In this submission, we first provide further details on the key new initiatives that we have undertaken in 2024 to respond to the Australian Government's call for industry to step up their scam prevention efforts, before providing our feedback on specific provisions.

We look forward to improving how we work with the Australian Government and law enforcement, and across the industry eco-system towards delivering strong and meaningful protections for Australian consumers from scams.

⁴ Meta, Australia Anti-Scam Hub. <https://about.meta.com/actions/safety/anti-scam>

Table of Contents

[Executive Summary](#)

[Table of Contents](#)

[Overview of new Meta initiatives](#)

[Reporting channels and intelligence sharing](#)

[National Anti-Scams Centre \(NASC\)](#)

[The Fraud Intelligence Reciprocal Exchange Channel \(FIRE\)](#)

[Advertiser and Marketplace seller verification](#)

[Proactive detection and enforcement](#)

[Strategic network disruption](#)

[Improving our policies and enforcement relating to scam content](#)

[Consumer awareness raising](#)

[Local and regional partnerships](#)

[Comments on the Exposure Draft Legislation](#)

[Core Concerns](#)

[Feedback on specific provisions of the Exposure Draft](#)

[Reporting and notification requirements may overwhelm or desensitise consumers and detract focus away from high-risk scams](#)

[Consumers may be inundated by potential scam notifications, risking desensitisation and inaction](#)

[Compensation framework requires careful consideration](#)

[Duplicative and uncertain obligations under legislation and codes](#)

[Governance](#)

[Safe harbour protection](#)

[Absence of any transition period](#)

Overview of new Meta initiatives

Meta has heavily invested in tackling scams on our platform and takes a four-pronged approach to this work, comprising: (1) policies that prohibit scams and related behaviour; (2) enforcement both on and off-platform; (3) tools to allow people to block and report scams, but also warn people about potentially suspicious activity; and (4) consumer education initiatives and partnerships.

We know there is always more to do. Scams are a highly adversarial space and scammers have become increasingly sophisticated and able to rapidly adapt their techniques to avoid detection. Since our January 2024 submission in response to the Australian Treasury's 'Scams – Mandatory Industry Codes Consultation Paper', we are pleased to share the following updates to demonstrate the impact of our ongoing scam prevention efforts in Australia.⁵

Reporting channels and intelligence sharing

Scams typically cut across multiple sectors and are carried out using multiple tools and platforms, meaning that each company is only able to detect and counter a narrow part of a broader scam campaign. All sectors of the scam ecosystem need to work together in protecting Australian consumers and this is why we have actively stepped up our collaboration with government and industry to better connect the pieces. This is already enabling us to increase enforcement on scam content on our services. We also have dedicated teams who engage regularly with the Australian Federal Police Joint Policing Cybercrime Coordination Centres (JPC3), including on disrupting scam networks.

National Anti-Scams Centre (NASC)

In April 2024, we onboarded the NASC to two new direct scam reporting channels, enabling them to promptly share: 1) suspected scam content on Facebook and Instagram, and 2) WhatsApp numbers suspected as being used to spread scams that have been reported by Australian consumers (note that this is in addition to our in-app reporting tools that consumers can use directly). We are working closely with the NASC to ensure the efficacy of these new channels, but early results have been promising. For example, between July and August 2024, we deleted 18 pieces of content reported by the NASC.

⁵ Meta (January 2024), 'Meta's submission on the Scams - Mandatory Industry Codes Consultation Paper'.

[https://treasury.gov.au/consultation/c2023-464732#:~:text=NON%2DCONFIDENTIAL%20SUBMISSIONS%20\(D%2DM\)](https://treasury.gov.au/consultation/c2023-464732#:~:text=NON%2DCONFIDENTIAL%20SUBMISSIONS%20(D%2DM))

These reports enabled us to widen our search and identify and delete an additional 2,600+ pieces of content that were similar to those the NASC originally reported.

Beyond these formal reporting channels that we have established with the NASC, Meta also actively participates in the NASC's Fusion Cell taskforces, which aim to bring together industry and government actors to accelerate disruption activities focused on a specific scam problem. We were pleased to be represented on the inaugural Fusion Cell focused on investment scams and are again participating in the next group focused on job scams. We also participate in the NASC's ongoing working groups, covering: Data Integration and Technology, Communication and Awareness and Emerging Trends and Responses.

The Fraud Intelligence Reciprocal Exchange Channel (FIRE)

At the start of October 2024, Meta and the Australian Financial Crimes Exchange (AFCX) jointly announced the pilot and initial results of the Fraud Intelligence Reciprocal Exchange (FIRE) via the AFCX Intel Loop in Australia.⁶

FIRE is a dedicated scam reporting channel between Meta and eligible financial institutions. It enables banks to share information about known scams directly with Meta to help combat scams that target both social media and banks. Based on these reports, Meta investigates and then shares aggregated information with the banks that identifies scam trends and content that Meta was able to take down.

Meta commenced the FIRE pilot with the AFCX Intel Loop in April 2024 and the early results and impact of the initiative have been positive. Of the 102 reports provided by the AFCX Intel Loop during the three-month initial pilot phase, Meta was able to conduct a wider investigation and identify and remove over 9,000 Pages and over 8,000 AI-generated celeb-bait scams across Facebook and Instagram. We continue to work with AFCX and the banks to further improve the FIRE initiative and look forward to continuing to grow our industry collaboration.

Advertiser and Marketplace seller verification

Meta is actively working to introduce new advertiser verification initiatives with the aim of providing a safer ad ecosystem across our services. Following an initial testing period in the first half of 2024, Meta has now fully launched phone verification for new advertisers

⁶ Meta (October 2024), Meta partners with the Australian Financial Crimes Exchange (AFCX) and Australian banking sector to combat scams
<https://medium.com/meta-australia-policy-blog/meta-partners-with-the-australian-financial-crimes-exchange-afcx-and-australian-banking-sector-to-7b7b26227360>

globally - including in Australia.⁷ New advertisers may now be required to have a verified phone number associated with their ad account before publishing ads. The required step will prompt an account admin to verify a phone number by confirming a randomly generated code sent by Meta via SMS, Voice, or WhatsApp, before publishing ads. Phone verification is an additional requirement that builds on the existing foundation of measures we have for advertisers before they publish ads on our platform.

We also launched SMS verification for higher-risk sellers on Facebook Marketplace in August 2024. Higher-risk sellers must complete SMS verification with a valid Australian number (+61) before their listing is allowed to go live. To identify higher-risk sellers, we consider a variety of signals like user reports, age of account, listing behaviour, messaging behaviour, and other account signals. As mentioned above, we will also introduce financial services advertiser verification in Australia in the first half of 2025.

Proactive detection and enforcement

We continue to invest significantly in proactive detection technology, by using artificial intelligence and machine learning to identify and disrupt harmful content and behaviour on our services. Our detection efforts continue to evolve in an effort to better and more quickly identify and remove content that violates our policies.

As an example, in July 2024, Meta conducted a targeted search that led to the identification and removal of nearly 20,000 investment scam ads. To build on this investigation and prevent similar ads from running on our services, we then launched an auto-enforcement pipeline on July 15 2024. By August 4, this pipeline had taken down over 21,000 additional ads. Additionally, between July and August 2024, we also deleted more than 219,000 ads based on automatic detection of violating ads in Australia. These examples are intended to illustrate Meta's commitment to continually improving our systems and processes so that we can identify and remove scam ads more quickly and before people see them.

Beyond enforcing on specific content and users on our services that violate our policies, in recent years, Meta has also brought legal action against individuals and entities responsible for using our platforms to scam people. For example:

- In 2019, we filed suit in California against a company called ILikeAd Media International Company Ltd. and two individuals for violating our Terms and Advertising Policies.⁸

⁷ See: <https://www.facebook.com/business/help/1064155054687612>.

⁸ Meta, 'Taking Action Against Ad Fraud', Newsroom, 5 December 2019, <https://about.fb.com/news/2019/12/taking-action-against-ad-fraud>

- In 2021, we filed a case against four individuals residing in Vietnam, who used a technique known as “session theft” or “cookie theft” to compromise accounts of employees of advertising and marketing agencies and then ran unauthorised ads.⁹
- In 2022, Meta and a financial services company filed a joint lawsuit, the first of its kind, against two Nigerian-based individuals who engaged in phishing attacks to deceive people online and gain access to their online financial accounts. We had taken several prior enforcement actions against the defendants, including disabling Facebook and Instagram accounts, blocking impersonating domains on its services and sending a cease and desist letter. This joint lawsuit represented a major step forward in cross-industry collaboration against online impersonation.¹⁰
- In 2022, we filed a lawsuit against an Australian resident, Chad Taylor Cowan, for providing a fake engagement service directed at Facebook. Cowan operated a website that provided fake reviews and feedback to businesses in order to artificially increase their Customer Feedback Score.¹¹

Strategic network disruption

Our ongoing work to identify and disrupt large and sophisticated scam networks is key to stopping scam activity at its source. In July 2024, for example, we announced the strategic network disruption of two sets of accounts in Nigeria that were affiliated with the cybercriminal group known as the Yahoo Boys, and which were attempting to engage in financial sextortion scams.¹² This included the removal of around 63,000 Instagram accounts in Nigeria, which included a smaller coordinated network of around 2,500 accounts that were linked to a group of around 20 individuals. We were able to identify this coordinated network through a combination of new technical signals that we developed to help identify sextorters and in-depth investigations by our expert teams.

Improving our policies and enforcement relating to scam content

As scam activity has become an increasing global challenge, we have recognised the need to continue to review and strengthen our policies to enable us to more strictly enforce on scam content. Over the last six months, we have made the following updates to our

⁹ Meta, ‘Combating E-Commerce Scams and Account Takeover Attacks’, Newsroom, 29 June 2021, <https://about.fb.com/news/2021/06/combating-e-commerce-scams-and-account-takeover-attacks>

¹⁰ Meta, ‘Taking Legal Action Against Financial Services Scams’, Newsroom, 8 February 2022, <https://about.fb.com/news/2022/02/taking-legal-action-against-financial-services-scams>

¹¹ Meta, ‘Taking Action Against Fake Customer Feedback and Reviews’, Newsroom, 16 March 2022, <https://about.fb.com/news/2022/03/taking-action-against-fake-customer-feedback-and-reviews/>

¹² Meta, ‘Combating financial sextortion scams from Nigeria’ <https://about.fb.com/news/2024/07/combating-financial-sextortion-scams-from-nigeria/>

enforcement policies:

- Stronger, Specific Enforcement Actions for Scam Violations: Identification of fraud and scam types that carry more serious risk to users (e.g. celeb-bait and finance scams). We have increased the relevant enforcement actions to ensure that users who repeatedly post these types of scams are penalised and/or removed from the platform more rapidly than in the past.
- Heightened Enforcement of Ads Violators: We have increased our enforcement on scam and fraud violations in advertising products. Accounts and Pages found to violate these policies will be permanently banned from advertising and upon further violations, will have their accounts removed altogether.
- Removing Networks of Accounts with High Signal of Fraud: We have built a system to detect when networks of accounts collectively post content violations highly correlated with online fraud, which aims to enable us to enforce across the network. We have found that scam networks will often spread violations and tactics across accounts to evade detection and enforcement from our systems, so this change ensures pre-emptive enforcement on accounts that consistently disregard our warnings and continue behaviour that is highly correlated with fraud.
- Increasing Cross-Platform enforcement on fraud across Facebook and Instagram: We have strengthened our cross-app enforcement for violating actors of Scams, Sextortion and Deceptive Identity across Facebook and Instagram. This means that when we disable an account for one of these reasons, we will simultaneously disable associated Facebook and Instagram accounts where we have high confidence in their linkage, which is backed by expert audits.

Consumer awareness raising

We continue to build on our ongoing efforts to educate Australian consumers and businesses on our platforms on how to identify and avoid scams. In August 2024, we launched a new WhatsApp scam awareness campaign, which has been run across Facebook and Instagram and focuses particularly on sharing tips and advice about how to identify and avoid investment, employment and romance scams. We are also planning further new scam awareness campaigns in the coming months across Australia.

Local and regional partnerships

We have continued to develop our scam prevention partnerships and initiatives with key not-for-profit organisations, not only in Australia, but across the broader Oceania region. Most recently, this work includes:

- Supporting national non-governmental organisation IDCARE's Cyber Resilience Outreach Clinics (CROC) community scam awareness initiative;
- Partnering with the Council of Small Businesses Organisations Australia (COSBOA) to promote scam and cybersecurity awareness amongst Australian small businesses through 'Meta Boost' training workshops and developing a new awareness campaign launching in Q4 of 2024;
- Joining the Global Anti-Scams Alliance (GASA) Oceania Chapter Establishment Group, which is being led by our longstanding safety partner, Netsafe New Zealand. Meta is already a global member of GASA, a prominent international network committed to protecting consumers from scams.

Comments on the Exposure Draft Legislation

Core Concerns

As noted above, Meta has significant concerns about the proposed SPF. Properly combatting scam networks – which are highly adversarial, sophisticated and incentivised – needs to be at the core of any effective legal and regulatory framework and government response aimed at protecting consumers from scams. To that end, for example, we welcome the United States Government's recent decision to impose sanctions on a business leader/ politician and several related entities in response to his role in the trafficking, forced labour and abuses in online scam centres in Cambodia.¹³

The proposed SPF includes several proposed obligations that instead risk diverting industry resources because of a significant new compliance burden that is unlikely to incentivise stronger ecosystem-wide cooperation.

Fundamentally problematic is the proposed external dispute resolution regime, which includes compensation for redress, and could perversely create an insurance policy for transnational organised crime and make Australia an even more attractive target for scammers. Having the reassurance that any scam losses they may incur will be reimbursed will increase consumers' risk tolerance and therefore lower their guard when

¹³ US Department of the Treasury, 'Treasury sanctions Cambodian Tycoon and businesses linked to human trafficking and forced labor in furtherance of cyber and virtual currency scams', 12 September 2024. <https://home.treasury.gov/news/press-releases/jy2576>

engaging with potential scam actors. This would inevitably lead to a higher success rate for scammers and a ballooning of their activities targeting Australia.

To be effective, the SPF should focus on a broader scope of solutions beyond shifting liability. The apportioning of liability between regulated entities whose different services may have been abused by the scammer across the 'attack chain' would be an extremely complicated task, inevitably leading to disputes. To illustrate this point, a single scam may be conducted using a mix of digital (including social media, private messaging, email or website) *and* telecommunications (SMS or phone call) services, before ending in a transfer of funds between financial institutions. This risks leading regulated entities to make claims or cross-claims against other regulated entities in Australian courts; in effect, encouraging adversarial blame-shifting among regulated entities that should otherwise be collaborating more closely with the shared goal of reducing scam activity.

Finally, the SPF will incentivise companies in a regulated industry to over-enforce on potential scam activity on their services, in order to avoid civil penalties and liability under the proposed compensation scheme. This is likely to have negative unintended consequences for Australian consumers, small businesses and other organisations, for example, in the case of social media, leading to the inadvertent removal of benign content and advertising.

We encourage the Government to carefully consider the negative consequences that will arise from the proposed SPF and to draw on a robust evidence base in finalising the scam prevention legislation and subsequent codes to ensure that they can achieve their intention of providing the most effective protections for Australian consumers from scam activity.

Feedback on specific provisions of the Exposure Draft

Outlined in this section of the submission are elements of the Exposure Draft that we consider to be uncertain or unworkable from a practical perspective, and that would therefore benefit from clarification.

Reporting and notification requirements may overwhelm or desensitise consumers and detract focus away from high-risk scams

The objectives of the SPF would be better served by introducing a framework for regulated entities to share broader intelligence and trends with both regulators and law enforcement to facilitate the identification and prevention of scams, rather than

mandating data sharing with respect to each individual suspected scam after-the-fact.

The sheer number of regulator reports triggered in respect of each suspected scam or item of actionable scam intelligence will significantly burden both regulated entities and regulators and unlikely assist in achieving the SPF's objectives. It will be very hard to spot the signal in the noise.

To illustrate this point, year to date for 2024, the NASC reports that it received 181,408 scam reports.¹⁴ If, for example, 50% of those generated actionable scam intelligence, under the SPF, over 90,000 reports would need to be submitted. There may also be significant duplication in the provision of duplicative reports to regulators from different regulated entities.

In this context, it is uncertain whether the regulator would have sufficient capability to meaningfully receive and share actionable scam intelligence with other entities in a timely manner, or to prioritise intelligence about high risk scams.

At a minimum, we recommend narrowing the scope of the reporting obligations by limiting reporting to: (1) circumstances where the reporting entity has reasonable grounds to believe that the communication, transaction or other activity is a scam, and (2) only in respect of those scams that present a serious risk of harm to consumers.

- Reasonable grounds to believe: Regulated entities are likely to face significant uncertainty in determining whether there is “reasonable grounds to suspect” that a communication, transaction or activity is a scam. It is unclear, for example, whether a single user report would trigger the requisite suspicion. This uncertainty, coupled with the potential for substantial penalties, is likely to result in over-enforcement and over-reporting. Obligations should only be triggered where there are “reasonable grounds to believe”, consistent with the approach under the *Privacy Act 1988* (Cth) (Privacy Act) Notifiable Data Breach Scheme.
- Likelihood of serious harm: Regulated entities will need sufficient time to review and investigate possible scams. Reporting obligations should follow only if a scam is likely to result in serious harm to consumers, aligning with the approach taken under the Privacy Act. The Privacy Act also includes exemptions from the notification requirements covering circumstances where the risk of serious harm has been eliminated after the data breach occurred.

¹⁴ See ScamWatch, <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>.

Finally, the definition of “scam” is overly broad:

- Inclusion of the “obtaining of personal information” potentially overlaps and duplicates obligations under the *Privacy Act 1998* (Cth). This could potentially give rise to duplicative notification obligations to the OAIC, the SPF General Regulator and the SPF Regulator. It could also require regulated entities to send two different notifications to the same affected consumer, creating unnecessary consumer confusion and uncertainty.
- In any event, it is uncertain whether the reference to “including obtaining personal information” is intended as an example of a particular form of loss or harm, or whether personal information is required to be obtained to meet the threshold definition.

Consumers may be inundated by potential scam notifications, risking desensitisation and inaction

Given the broad and uncertain definition of “actionable scam intelligence”, there is a real risk that consumers are overwhelmed with notifications about scams and potential scams (potentially the same notifications from multiple entities), drowning out core messaging in relation to scam prevention, and creating notification fatigue that may risk inaction on the part of the consumers.

A more effective way to inform consumers about scams and to encourage caution may be to require regulated entities to provide visible and relevant notifications to consumers about emerging scam trends (for example through on-platform ads, educational campaigns, help centre materials and blog posts), with the ability to focus in particular on scam types that have the highest prevalence or potential for harm.

Compensation framework requires careful consideration

We have already outlined our overarching concerns above with respect to the SPF’s proposed compensation regime. While Meta firmly disagrees that a compensation regime will be effective in tackling the underlying causes and manifestations of scams, for completeness, we highlight below important safeguards that are missing from the proposed SPF.

1. Clarity as to requirements for consumer claims, and safeguards to prevent abuse.

This should include, for example:

- a. Appropriate materiality thresholds. Under the SPF, regulated entities could be required to provide redress (or other compensation) for any SPF consumer loss or damage caused by a scam, irrespective of the materiality of the loss. For example, a consumer under the SPF could claim compensation for \$10 lost to a scam. Without any materiality threshold, a large volume of immaterial claims for compensation could overwhelm a regulated entity's IDR system, or the EDR regime, without appropriately prioritising high-risk harms.
 - b. Timeframes to bring a claim, noting the proposal of 6 years is disproportionately burdensome. For comparison, the US *Electronic Funds Transfer Act* requires consumers to notify financial institutions of most unauthorised transfers within 60 days of the transfer.¹⁵
 - c. Minimum standards for substantiation of claims and appropriate exclusions. Clarity is needed as to what evidence a consumer needs to provide in support of any claim, for example to establish proof of causation. Further, there should be no ability to make a claim in circumstances where a consumer has acted fraudulently or with gross negligence. For example, the UK's authorised push payment scheme includes a "Consumer Standard of Caution" exception reflecting that no compensation or redress should be given where a consumer has acted fraudulently or with gross negligence (other than in the case of a vulnerable consumer).¹⁶ Similarly, exclusions should apply to claims that are false, vexatious or not made in good faith.
2. A process and timeframe for assessment by regulated entities on receipt of claims. Entities require a reasonable timeframe to assess complaints, and to seek to resolve it or provide its position to the complainant, before it is determined by the EDR provider.
3. A process for disputing and repudiating claims. There should be a process for entities to reject a dispute because it does not meet minimum standards (eg. the

¹⁵ US Electronic Funds Transfer Act (15 U.S.C. 1693 et seq.) of 1978.

¹⁶ See Payment Systems Regulator, Authorised push payment fraud reimbursement The Consumer Standard of Caution Exception Guidance, December 2023:
<https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf>.

complainant has not established proof of loss) or the complaint is vexatious.

4. An appropriate cap on liability. The compensation regime fails to set out any caps or limits on claims for redress of compensation. This creates significant business risk and uncertainty for regulated entities of all sizes, as there is no meaningful way for an entity to estimate its potential liability.
5. Clarity as to the obligations of each regulated entity. Liability regimes need to have the ability to be effectively administered to avoid legal uncertainty for all market participants. Any liability regime should include express provisions to clarify which regulated entities are liable to compensate consumers for loss or damage, and under what specific conditions. Some overseas regimes, for example, make clear that the primary obligation rests with financial institutions in the first instance, who are uniquely positioned with visibility into the fraudulent payments occurring (in some instances turning next to telecommunications operators if the financial institution has fulfilled all its duties).
6. Industry should be afforded an opportunity to consult on the proposed SPF EDR scheme and its parameters. The SPF EDR scheme should be developed by, or in consultation with, entities that will become subject to the EDR, and who have an in-depth understanding of the complex and technical nature of preventing scams in their relevant sectors.

Duplicative and uncertain obligations under legislation and codes

The Exposure Draft includes dual standards of conduct under the SPF principles and the SPF Codes. The Explanatory Materials expressly contemplate that compliance with the SPF Codes is not sufficient to ensure compliance with the SPF Principles. This creates significant business risk and uncertainty, particularly where contraventions of the SPF principles attract the highest possible maximum penalties under the Competition and Consumer Act (CCA).

Rather than creating an overlapping set of obligations in the SPF principles, it would be clearer to set out all obligations within the SPF Codes. Alternatively, if the Government is minded to retain substantive obligations in the SPF principles, then at a minimum, the SPF Codes should be designed to ensure compliance with the SPF principles.

Governance

The requirement for a senior officer to certify a regulated entity's governance policies, procedures, metrics and targets to combat scams is out of step with other comparable

regimes in Australia (including, for example, the Privacy Act or the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act). Removing this provision would not impact the underlying obligation on, and accountability of, the regulated entity under the scheme.

Safe harbour protection

The proposed safe harbour for erroneous action to disrupt a suspected scam activity (for example, disabling a social media account suspected to be involved in a scam) has a number of practical difficulties that leave regulated entities significantly exposed.

- It requires regulated entities to form a definitive view as to whether something is a scam within 28 days. This may be difficult to do.
- The safe harbour appears to only relate to suspected scams; if a regulated entity has determined that something is a scam, it loses the benefit of any safe harbour protection for action taken in good faith.
- It would appear the safe harbour only applies with respect to civil action taken by consumers located in Australia, leaving regulated entities exposed to action (eg. defamation claims) by offshore individuals or entities.

Absence of any transition period

If the Government decides to proceed with the SPF with amendments to address the significant issues outlined above, we also recommend that a grace period be included. At present, the Exposure Draft contains no grace period before it comes into effect, and no minimum consultation period or notice period prior to any sector designation taking effect.

This is out of step with other Australian regimes involving incident reporting requirements, such as the Notifiable Data Breach Scheme (12-month grace period), or the SOCI Act (6 months to adopt a critical infrastructure risk management plan, and a further 12 months to establish a cybersecurity framework). It is also out of step with prior amendments to the *Competition and Consumer Act 2010* (Cth), such as the amendments to the unfair contract term regime under the Australian Consumer Law (12-month grace period).

We expect that compliance with the SPF (even if our and other companies' recommendations for improvement are accepted), in particular the reporting and notification requirements, will require entities of all sizes and across all sectors significant time to adjust their internal systems and processes. We recommend including a minimum 18 month grace period before implementation of the SPF, with further notice before the designation of sectors takes effect.

Given the rapid pace at which scammers shift their tactics, we would also recommend encoding a review mechanism in the SPF to assess whether it has been effective in achieving its policy objectives, including a meaningful reduction in scam activity.