Submission in response to Scams Prevention Framework Bill 2024

9 January 2025

Introduction and Executive Summary

Thank you for the opportunity to comment on the proposed scams prevention framework (**Framework**) outlined in the Government's Scams Prevention Framework Bill 2024 (**Bill**).

Scams are harmful to consumers and legitimate businesses, and undermine individual users' trust in the services they use. We support the Australian Government's focus on reducing serious consumer harm caused by scams on an ecosystem-wide basis, and are committed to playing our part.

In this submission, Google makes the following comments and recommendations on the Bill:

1. **Google is committed to combating scams and the criminals behind them.** Google addresses scams in various ways: utilising powerful technology to detect and remove harmful content, collaborating with the National Anti-Scam Centre (**NASC**) and similar bodies around the world, and empowering users with tools to report issues and information to stay safe. Scams are a whole-of-society threat, most often driven by organised crime, operating across borders. This necessitates a cross-industry response as well as collaboration internationally and across multiple stakeholder groups, from government and law enforcement, to sectors such as financial institutions and telecommunication service providers. It is important to ensure that the Framework does not: impede the good work already being done to combat scams, make Australia a greater target for scammers, nor reduce Australian consumers' vigilance against scams.

2. **Consumers should be protected from online scam ads across like services.** If the Minister intends to designate paid advertising services on general search engines, the Minister should also designate paid advertising services on specialised search services, and other online paid advertising services, including shopping platforms, as well as "answer engines" that display ads, which are also susceptible to scammers.

3. **A low threshold for sharing scams intelligence will lead to false positives and over removal. It is critical that the Framework sets a sensible threshold for sharing scams intelligence**. Otherwise, legitimate content will be blocked or removed to minimise the risk of penalties or consumer action. Regulated entities should be required to maintain reasonable policies prohibiting scam content and to share information where they have, acting reasonably, concluded that content is contrary to those policies (rather than where they might merely suspect that content is or could be associated with a scam).

4. **The proposed internal dispute resolution (IDR) and external dispute resolution (EDR) processes are extremely complex and could lead to perverse outcomes — including making Australia more appealing to scammers rather than less**. Consumer groups have confirmed the current proposal would be "unworkable" for consumers.[1] As outlined below in section 4, this is because the processes are unclear and would, in practice, be very complex and likely frustrate consumer claims, and delay recovery of losses. It would also risk reducing consumers' vigilance against scams and, rather than improving the situation, lead to a situation where Australia is seen as a prime target for scammers. The complexity would also leave the process susceptible to exploitation by bad actors who

[1] See for example, Consumer Law Action Centre's submission to Treasury (4 October 2024) at pages 19-28.

could seek to recover their losses from multiple entities. It is critical that the complaints and liability regime is revisited and, at the very least, simplified, to enhance consumer outcomes and minimise unintended consequences.

5. **Overlapping obligations in legislation and codes should be removed** to minimise complexity and uncertainty. Overarching legislation should be limited to setting broad principles / objectives that the SPF codes should be designed to implement in industry-specific contexts.

6. **There should be a required minimum transition period before obligations come into effect and regulated entities are exposed to liability.** Based on Google's past experience internationally, we expect it would take at least 12 months to develop and be ready to implement a compliance program of the magnitude contemplated by the Framework.

1. Google is committed to combating scams and the criminals behind them

Since the earliest days of Google, our teams and systems have been dedicated to protecting users by combating scams and scammers. Google fights scams and fraud by taking a three-pronged approach to protect users from harm, deliver reliable information, and partner to create a safer Internet. We provide some examples of actions we've taken to combat scams below.

- **Protecting users from harm:** Google has a long history of deploying tools and techniques to combat scams and scammers, including by using the latest AI technology. Our teams have developed industry-leading tools that effectively fight back against scammers, including proactively blocking 99.9% of spam and malware on Gmail and protecting consumers from dangerous calls and messages on Google's Phone and Messages apps. In 2023 alone, we blocked or removed more than 5.5 billion advertisements for violating our policies, capturing many different scams and tactics. And while we are developing technology to combat these scams, we also regularly file affirmative litigation to stop bad actors and create legal precedent that allow us to act.[2]

  Additionally, advertiser verification is an area where we have pioneered industry leading approaches, such as robust verification techniques in high-risk verticals, like financial services. Since August 2022, to advertise financial services in Australia, advertisers must complete a verification process demonstrating they are licensed to provide those services and their registration number, among other things.[3] To date Google has been the only digital platform to require this level of advertiser verification in Australia. These sorts of

[2] Examples include: (1) In April 2022, Google filed a consumer protection lawsuit against an actor who used a network of fraudulent websites that claimed to sell basset hound puppies — with alluring photos and fake customer testimonials — in order to take advantage of people during the pandemic. (2) In November 2022, Google filed a lawsuit against scammers who sought to defraud hundreds of small businesses by impersonating Google through telemarketing calls. They also created websites advertising the purchase of fake reviews, both positive and negative, to manipulate reviews of Business Profiles on Google Search and Maps. (3) In December 2021 Google filed a lawsuit and took other action to disrupt the operations of Glupteba, a multi-component botnet targeting Windows computers. (4) In April 2023, Google filed a lawsuit against the malware distributors of Cryptbot, which we estimate infected approximately 670,000 computers that past year and targeted users of Google Chrome to steal their data.
[3] See Google Advertising Policies Help page "Financial Services Verification: Relevant Regulators and Enforcement Dates".

actor verification techniques should play a role in a future Ads SPF Code.

- **Delivering reliable information:** We strive to enable confidence in the information and content on our platforms by delivering reliable information and best-in-class tools that put users in control of evaluating content. We created a number of features that help users have more context around what they're seeing online. For instance, in 2022, we launched My Ads Center, which gives people more control over their ad experience on Google's sites and apps.[4] Within My Ads Center, people can block sensitive ads and learn more about the information used to personalise their ad experience. In 2023, we announced the Ads Transparency Center, a searchable hub of verified advertisers where users can view basic information about the advertiser and see the other ads they are running on our platforms.[5] We also regularly post blog posts warning consumers about the risk of scams, including as recently as December 2024, and we have plans for more consumer outreach in 2025.

  We believe that this type of consumer outreach — highlighting emerging scam trends that have the highest prevalence or potential for harm — is a more effective way to inform consumers about scams and to encourage caution than retrospective warnings with respect to specific exposures to scam content.

- **Partnering to create a safer internet:** We scale our industry-leading practices to keep users safe online through proactive partnerships and communication with experts and organisations such as national anti-scam agencies. We have been working closely with the NASC since its inception and are working on additional collaborations which we hope to be able to announce soon. In October, we announced a global partnership creating a platform for sharing information about scams and fraud.[6] And, we just published our first Scams Advisory to highlight the most recent online fraud and scams trends and tactics.[7]

Google's white paper on Tackling scams and fraud together provides more detail on how Google responds to online scams and offers policy recommendations for how we can better partner across the ecosystem to maximise the impact of our efforts to tackle this criminal threat to society and the economy.[8]

Scammers are continuously developing sophisticated new methods and finding loopholes.[9] For example, despite our significant (and, industry-leading) efforts to combat ads featuring investment scams, we are unable to stop every single instance of such ads. Bad actors operating with more sophistication and at a greater scale constantly change their tactics and the methods with which they interact with victims in an attempt to evade detection — this includes impersonating genuine licence holders and using text or image manipulation to circumvent automatic detection. We also found scammers using cloaking to show our ad reviewers and systems different ad content than they showed users. Once we become aware of these practices, we develop strategies to address them — but this isn't always straightforward and can take time to implement. This is especially as we are usually exposed to only a small element of the

[4] See Google Blog Post, "Your ads, your choice" (20 October 2022).
[5] See Google Ads Transparency Center.
[6] See Google Blog Post, "The new Global Signal Exchange will help fight scams and fraud" (9 October 2024).
[7] See Google Blog Post "A new way we're helping others track frauds and scams online" (14 November 2024).
[8] See Google, "Tackling scams and fraud together - Google White Paper" (December 2024) at page 6.
[9] See The Guardian, "Celebrity scam ads still targeting Australians despite tech giants' crackdowns" (5 December 2024).

entire 'scams lifecycle' which may appear inconspicuous, or at least difficult to assess as fraudulent on its own.

It is important that the Framework does not impede the good work already being done — by Google and others — to combat scams, for example, by introducing complexity, uncertainty or requirements that divert resources from critical scam combatting activities. The obligations on platforms must be realistic — a standard of zero scams is not achievable, and what constitutes "reasonable steps" should take into account the ingenuity of cybercriminals and the many and evolving threat vectors that platforms face. A disputes and liability regime that makes platforms and other intermediaries liable for compensating consumers for losses from scams is likely to, perversely, reduce Australian consumers' vigilance against scams and make Australia a greater target for scammers, contrary to the Government's objectives.

The Government also should not overlook taking action to stop scams at the source — ie: rather than going after legitimate business intermediaries, law enforcement efforts should focus on going after the scammers, who are usually criminal gangs that operate transnationally. Only targeting intermediaries would fail to penalise and dis-incentivise scammers and would reduce consumer agency to protect themselves against scams. A critical element of the Government's anti-scam policy should be to enable and encourage information sharing and facilitate law enforcement work, especially cooperation across borders to catch criminals. Google has detailed these recommendations and made a global call to action for strengthened cooperation among law enforcement, industry and other expert stakeholders.[10] We encourage the Australian Government and its relevant agencies to focus their work on the international effort to go after scam criminals.

2. Protecting consumers from online scam ads across like services

Online scams are a growing global problem and scammers are constantly evolving their tactics and taking advantage of new technologies and social trends.

Designating paid advertising on some search services but not others would leave gaps that scammers could take advantage of and could also interfere with competition between ads service providers. Consumers will have consistent expectations across the ads they view and as such all ads service providers should provide at least some protections. For example, we believe that **all** digital ads platforms should be required to verify that advertisers of financial services in Australia are registered with ASIC to ensure a consistently robust approach to combatting investment scams. Google was the first to adopt such measures in Australia, and, recently, Meta has followed suit. Financial services advertiser verification has greatly reduced the incidence of investment scam ads on Google ads — but many platforms do not yet have such safeguards in place.

To protect consumers from online scam ads across services and ensure a level playing field, we recommend:

- If the Minister intends to designate paid advertising services on general search engines, the Minister should also designate paid advertising services on specialised search

[10] See Google, "Tackling scams and fraud together - Google White Paper" (December 2024) at pages 19-21.

services, and other online paid advertising services, including shopping websites, as well as "answer engines" that display ads, which are also susceptible to scammers. This should be done to future-proof the SPF, as the way consumers search for information is rapidly evolving.

- The s58AE(1)(a) matters that the Minister must consider before designating a sector should include the impact of designating a sector on competition (for example, the potential for the designation to distort competition between services by imposing a significant regulatory burden and cost on some entities, but not their competitors).

3. A low threshold for sharing scams intelligence will lead to false positives and over removal

Google supports sharing scams intelligence to combat scams. In October 2024 Google entered into a partnership with the Global Anti-Scams Alliance (**GASA**) and DNS Research Federation (**DNS RF**) to launch the Global Signal Exchange (**GSE**). The GSE aims to become a global clearing house for online scams and fraud bad actor signals, with Google becoming its first Founding Member. The collaboration brings together GASA's unparalleled global network of stakeholders, DNS Research Federation's data platform which is already storing over 40 million signals, and Google's deep expertise in fighting scams and fraud, AI capabilities and funding. By combining our efforts, and creating a central platform, GSE will fill a gap of how abuse signals are exchanged to identify and disrupt fraudulent activity faster across different sectors, platforms, and services, in a way that is easy to use, efficient, and works at the scale of the Internet.

However, reporting about all *suspected* scam activity, especially if this leads to an expectation to remove the suspected content, will result in false positives. Google receives millions of removal requests daily. Over half a billion (approx. 650 million) pieces of content are reported each year globally via Google's legal removal reporting channel. Not all of these are legitimate complaints. Many of these include user reports that are baseless, confused, or worse — malicious and abusive.

If the threshold for actioning suspicious content or accounts is set too low (as is the case in the Bill), or is uncertain, providers covered by the Framework will be forced to over-remove — that is, some genuine content and advertising is likely to be removed to minimise risk, harming legitimate businesses, **especially small to medium businesses**, who rely upon platforms to reach new customers. In addition, higher volumes of lower threshold signals can result in more noise which in turn will make it harder to identify the true badness. This is particularly problematic given, for example, proposed section 58BX, which requires disruption of "scams" where a regulated entity "has reasonable grounds to suspect" that activity may be a scam; this will clearly disrupt legitimate businesses.

It is critical that the Framework sets a sensible threshold for sharing scams intelligence in order for it to be effective. Rather than being required to share information where an entity has "reasonable grounds to suspect" that content may be associated with a scam, regulated entities should be required to maintain reasonable policies prohibiting scam content and to share information where they have, acting reasonably, concluded that content is contrary to those policies. Another way to express this might be, "when an entity has reasonable grounds to

believe that content is associated with a scam". This would greatly reduce the risk of false positives and over removal.

It should also be made clearer (that is, section 58BK(1) should be clarified) that a regulated entity that takes reasonable steps to investigate actionable scams intelligence (properly defined), and does not take action on grounds that it is not satisfied that there is a scam, should not be liable if in fact the content/account is later determined (with 20/20 hindsight) to be a scam.

4. The proposed IDR and EDR processes would be extremely complex, frustrate consumer claims, and could lead to perverse outcomes

The proposed IDR and EDR processes are unclear, and would be extremely complex, legalistic, and time and resource-consuming in practice. This would likely frustrate consumer claims and could lead to perverse outcomes, as outlined below. To improve consumer outcomes and reduce unintended consequences, it is critical that the complaints and liability regime is simplified.

Complexity and uncertainty arises in the following ways:

- **Without SPF codes in place, regulated entities' obligations under the Framework are unclear**, meaning the circumstances in which a consumer would be entitled to recover losses from a regulated entity are also unclear.

- In defending its actions as "reasonable", regulated entities would need to adduce in evidence extremely sensitive information about how they combat bad actors. Such information is tightly guarded even within Google to ensure that it is not leaked and abused by bad actors. The disclosure of such information in IDR/EDR risks the information falling into the wrong hands, thereby facilitating bad actors to circumvent detection and protections. This is a significant problem with the current Framework proposal, and risks undermining its objectives.

- **If a regulated entity is found to have contravened its obligations under the Framework, and the consumer has acted negligently or is a bad actor involved in the scam, the extent to which the regulated entity should bear losses is unclear**. In the UK, a consumer who has been negligent or is involved in the fraud is not entitled to claim compensation; the position under the SPF should be clarified.

- **There is also uncertainty as to how to apportion liability for losses** among the various regulated entities whose services were used in connection with a particular scam loss. If an ad on social media led the consumer to share their phone number with a scammer, which the scammer used to send SMSes to the consumer, leading to the consumer transferring money from their bank account to the scammer — and each of those services complied with their obligations under the framework to varying degrees — to what extent should each be responsible? The Bill does not address this.

  Where multiple regulated entities may be responsible for loss from a scam, consumers will bear the burden of pursuing claims through multiple forums (including regulated entities' IDR processes and EDR processes). In a context where multiple entities are involved in the scam chain and potentially liable, it is unclear how

individual IDR processes could effectively resolve disputes. Without visibility over other regulated entities' involvement in the scam and approach to compensating the consumer, the regulated entity would likely either reject the claim or offer compensation that results in the consumer being undercompensated; it is also, theoretically, possible that the consumer could be 'overcompensated'.

The proposal foreshadowed by s58BZE to have IDR guidelines prescribed by the SPF rules on how to apportion liability between multiple regulated entities defers grappling with these challenges to after the Bill is passed. The proposal is novel and, in our view, requires further consideration, impact assessment and development. These important details should be published and consulted on before the Bill is passed. It is not appropriate to simply assume that there will be a workable solution to the challenges we and other stakeholders like consumer groups have identified.

It is not clear to us how any guidelines or rules could deal with the practical issues that arise when multiple entities are involved, and each is assessing, internally, its own compliance with the range of obligations in the SPF (including rules and guidelines), and not in a position to test other entities' involvement and compliance with the SPF.

This complexity will likely frustrate consumer claims and delay recovery of losses. Consumer groups have confirmed this would be bad for consumers, especially because it places the onus on an already vulnerable consumer to demonstrate that their bank, telco and/or social media platform did not meet certain (unclear) obligations under the SPF.[11] It will likely take consumers months, if not years, to recover compensation through the current proposed SPF dispute resolution scheme.

The proposed apportionment of liability between multiple regulated entities also carries the risk of fostering an adversarial environment of blame-shifting, rather than one of working together with a common goal of reducing scam activity.

The complex regime could have the perverse effect of increasing the number of scams in Australia. A regime in which multiple regulated entities are potentially responsible for compensating a consumer for losses from a scam (but have no visibility over other entities' involvement or compensation payments), could also be exploited by bad actors, who could seek to recover their loss from multiple regulated entities. If regulated entities are inundated with a large number of claims, they may take a practical approach of compensating "small" claims without investigation to minimise drain on internal resources. Similar problems arise in a regime that compensates consumers who have been negligent — or worse, are involved in the fraud themselves. Contrary to the intent of the Framework, this would make Australia an even more attractive target for scammers.

As a starting point, Australia should evaluate the relative merits of the UK's tried and tested single-sector recovery model for authorised push payment fraud. The UK reimbursement model only became mandatory in October 2024, but in 2023, UK banks taking part in the voluntary code on average reimbursed approximately 67% of money lost to APP scams, with

[11] See for example, Consumer Law Action Centre's submission to Treasury (4 October 2024) at pages 19-28. See also, Law Council of Australia's submission to Treasury (17 October 2024) at pages 18-24.

some banks refunding almost 90%.[12] The UK's reimbursement cap has been finalised at £85,000 which will cover an estimated 99% of scam claims. A review will be conducted in 12 months. In contrast, Australia's banks compensate just 2-7% of scam losses.[13] The UK model is rapidly gaining traction around the world, with similar models being considered in New Zealand[14] and the USA.[15]

Requiring banks to be accountable for consumer redress does not mean that other sectors are not regulated. Regulators would still hold other sectors to the high standards set out in the Framework. Google and other participants would still be committed to taking reasonable steps to prevent, detect, report, disrupt, and respond to scams, including as outlined in Part 1 of these submissions. This recognises that: (1) consumers will almost always go to their bank first for help when they have lost money; (2) banks are uniquely positioned to assess the legitimacy of payment recipients and identify potential bad actors in payment scams (e.g., through transaction monitoring), whereas digital platforms and telecommunication providers have more limited visibility into the transaction of payments; and (3) banks are the best placed and most resourced to identify actual scam losses, including, whether and how much money has been lost.

Even if consumers are only permitted to recover scam losses from a bank where the bank has contravened its obligations under the SPF (or an SPF Code) (so that consumers are encouraged to remain vigilant), this would be a significantly simpler process than the proposal to require apportionment of liability among multiple sectors.

The effectiveness of a UK style model could be revisited after the Framework has been operative for a period of time (for example, 12-24 months). If the model is found to not be delivering effective consumer outcomes, and it is found that banks are bearing risks arising from the failures of other regulated entities to comply with the Framework, the redress and liability regime could be adjusted at that time.

If the Government is not prepared to proceed with a UK style model and insists on proceeding with a multi-party liability regime (now or after testing a UK style model), to enhance consumer outcomes and minimise unintended consequences:

- **Consumers should not enforce the high level obligations in the Framework, but instead could be given enforceable rights in SPF codes.[16] SPF codes must set out in detail (a) the circumstances in which consumers could recover losses from particular regulated entities and (b) the amount of losses they could recover in those circumstances.** This should follow industry consultation. Relevantly, any IDR or EDR process which requires an assessment of the reasonableness of steps taken by regulated entities and disclosure of information about their internal processes should be avoided, in order to both (i) make dispute resolution faster and more straightforward; and (ii) ensure bad actors are not armed with information that enables them to circumvent regulated entities scam combating processes. This would not preclude the production of confidential information (subject to appropriate safeguards) to regulators enforcing the Framework.

[12] UK Payment Systems Regulator, "Authorised push payment (APP) scams performance report" (July 2024) at page 10.
[13] ASIC, "Anti-scam practices of banks outside the four major banks" (August 2024) at page 10.
[14] New Zealand Banking Association media release, "Banks seek government support for Anti-Scam Centre" (15 April 2024).
[15] PYMNTS, "75% of Large Banks Agree to Reimburse Authorized Fraud Victims" (14 May 2024).
[16] As noted in section 5 below, it would be preferable for the high-level obligations in the Framework to be replaced with broad principles and objectives that the SPF codes should be designed to implement in industry-specific contexts.

- **There must be appropriate exclusions.** For example, where consumers have acted fraudulently, with negligence or where claims are false, vexatious or not in good faith, regulated entities should not be required to compensate those consumers. The lack of these exclusions would incentivise bad faith claims and more scam activity, and may lead to Australian consumers letting their guard down.
- **Reasonable timeframes to bring a claim should be specified**, noting that the proposal of six years is excessively burdensome and does not align with international practice.
- **Appropriate caps on liability should be included**, to avoid disproportionate risk and uncertainty of liability for regulated entities. Without liability caps, regulated entities will need to price the potential risks of a significant number of unbounded claims into their products and services, resulting in increased costs for consumers.

5. Overlapping obligations in legislation and codes should be removed to minimise complexity and uncertainty

The Framework is currently highly complex to navigate. The overarching legislation contains six SPF Principles that include numerous broad obligations, and further specific obligations are to be introduced in SPF rules and mandatory industry codes.

A single-layered, flexible, risk-based framework, consisting of sector-specific codes registered by regulators, would be simpler and more effective than a framework containing two layers of obligations. Overarching legislation should be limited to setting broad principles and objectives that the SPF codes should be designed to implement in industry-specific contexts. At the very least, overlapping obligations in legislation and codes should be removed to minimise complexity.

Having obligations in both legislation and codes (in addition to rules and guidelines) has several adverse consequences. It:

1. **risks duplication of obligations**, leading to confusion about which regulator is responsible for enforcement;
2. **could lead to inconsistent obligations**, particularly if the codes evolve over time while the legislation remains unamended;
3. **increases the burden on industry** by requiring compliance with two levels of obligations and dealings with multiple regulators on the same issue;
4. **increases cost for Australian taxpayers** by entrusting multiple regulators with responsibilities for overlapping obligations; and
5. **is inconsistent with the principles of good administration** for firms to be exposed to two sets of penalties under the same framework for the same conduct.

For example, one issue that should be addressed in relevant SPF codes and not the overarching legislation is the extent to which regulated entities can and should identify SPF consumers impacted by scam activity. This is because, as previously submitted, identifying an SPF consumer

in a digital platforms context is more challenging compared to other sectors.[17] For example, banking relies on unique account numbers, and telecommunications relies on unique phone numbers. By contrast, many users of digital platform services like a search engine will use the service without being logged into their account. For valid privacy reasons, consumers often use digital platforms with settings that would make it impossible to contact them in the future. Additionally, often a device or account log-in will be used by multiple individuals, further complicating the identification of individuals. The challenges with identifying consumers were seemingly recognised by the Government when it moved from its exposure draft to the Bill tabled in Parliament, deleting section 58BK in the process. The Government has retained, however, what is now section 58BO(1)(b), which would require regulated entities (across all regulated sectors) to take reasonable steps to identify the persons who were SPF consumers of that service at the time when the persons were or may have been impacted by the scam activity. This section too should be deleted so the issue can be dealt with in detail in relevant SPF Codes.

These risks would not arise if there was only one layer of obligations in sector-specific codes. A single-layered framework would better deliver on the Government's objective to take robust steps to prevent and respond to scams impacting consumers.

If obligations that require regulated entities to take "reasonable steps" are retained (whether that is in the primary legislation or Codes), the concept of "reasonable steps" should be defined and assessed by reference to the adequacy of the systems, processes and procedures that a regulated entity has in place to prevent and respond to scams rather than actions taken in the context of an individual scam incident. Section 58BB of the Bill acknowledges that "reasonable steps" will vary depending on a regulated entity's size, the regulated services concerned, its consumer base and so on, but it does not provide any meaningful guidance on what action is required to not to be in breach of the Framework. Consideration of the adequacy of systems and processes as part of whether a regulated entity has taken reasonable steps would give regulated entities more certainty about what is expected of them, incentivise investment in improving systems and processes, and lead to more consistent liability outcomes.

6. There should be a required minimum transition period before obligations come into effect / regulated entities are exposed to liability

As with any other legislative amendment that introduces new obligations, a grace period should be provided to ensure adequate time for compliance. Based on Google's past experience internationally, we expect it would take at least 12 months to develop and be ready to implement a compliance program of the magnitude contemplated by the Framework.

[17] See Google's submission of 4 October 2024 at pages 13 and 20.