Submissions in response to Scams — Mandatory Industry Codes Consultation Paper

2 February 2024

Executive Summary

Thank you for the opportunity to comment on the proposed scams framework (**Framework**) outlined in the Government's Scams — Mandatory Industry Codes Consultation Paper (**Consultation Paper**).[1]

Google is committed to tackling scams and protecting Australians on our platforms and services. 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. Our multi-pronged approach aims to create a safer and more secure online environment for everyone, while balancing the interests of legitimate content creators and businesses that use our services.

We support the Australian Government's focus on reducing serious consumer harm caused by scams on an ecosystem-wide basis. To that end, we support a phased approach: industry-led, voluntary codes first, followed by mandatory obligations and penalties as needed. We suggest as a first step that the digital platforms sector be tasked with drafting voluntary commitments. Existing international efforts provide a useful model for a voluntary code in the Australian context, notably the UK Online Fraud Charter, developed by TechUK in conjunction with industry, and signed by Google, YouTube, Amazon, Facebook, Instagram, Microsoft, TikTok, and others.

If mandatory obligations are required, we suggest changes to the proposed Framework to maximise effectiveness while minimising unintended consequences, including:

1. **A single-layered, flexible, risk-based framework**, consisting of sector-specific codes registered by regulators, which would be simpler and more effective than a framework containing two layers of obligations. If a two-layer framework is adopted, the overarching layer should be limited to objectives and desired outcomes.

2. Recognition that the **diverse nature of services provided by banks, telecommunications providers, and digital platforms requires tailored solutions**, not prescriptive one-size-fits-all rules. A co-regulatory approach should be adopted, with industry working with Government and regulators on agreed principles and standards.

3. **The definition of "scam" should focus on bad actors obtaining a benefit**, consistent with the definition of "fraud" in the current Commonwealth Fraud Control Policy.

4. **The regime should be evidence-led**, including to ensure that the resources and attention — of firms and regulators — are focused on the areas of greatest concern, where intervention could make the greatest practical difference to Australians. The focus of the Framework should be on services that are demonstrably exploited by scammers and start

[1] Australian Government / Treasury, Scams —- Mandatory Industry Codes Consultation Paper, https://treasury.gov.au/sites/default/files/2023-11/c2023-464732-cp.pdf, November 2023.

with clear and practicable obligations for those, before expanding if necessary. For example, unpaid search and news aggregation should be out of scope.

5. **Obligations on platforms should involve considerations of practicality and proportionality**, consistent with international approaches. This is critical given the global nature and scale of our and others' businesses.

6. **Empowering a regulator to issue specific take down notices** for scams would help ensure digital platforms' enforcement efforts are focused on combating legitimate risks and remove incentives to over-remove content based on consumer reports.

7. **The regime should not subject digital platforms to claims from individuals** for compensation for losses incurred to a scammer. Enforcement of obligations should be by a regulator.

8. The obligations should be cognisant of the **balance to be struck between transparency and the protection of sensitive information** that could be exploited by bad actors.

9. We support **voluntary information sharing through the NASC**, however the proposed mandatory information sharing has legal and practical challenges.

10. The consequences of **non-compliance should be aligned to existing industry codes**, with penalties proportionate to the severity of a breach.

Introduction

Google is committed to combating scams and supports the Government's efforts to address the serious harm caused by bad actors perpetrating scams online.

We're aware from the ACCC's "Targeting scams" report that people in Australia reported $3.1 billion in losses in 2022, an increase of 80% on losses reported in 2021. While the top reported contact methods used by scammers are text messages (79,835 reports) and telephone calls (63,821 reports), the report finds that scams are to a lesser extent also perpetrated by scammers via email, using the Internet, and via social networking / online forums.[2]

Digital platforms have strong incentives to take measures to stop scams being present on our platforms. Scam content is harmful to consumers and legitimate traders, and undermines individual users' trust in our platforms. Accordingly, we invest heavily in combatting scams. For example:

- Google's Messages and Phone apps filter scam and spam messages[3] and calls.[4]
- Gmail blocks 99.9% of spam, malware, and dangerous links from reaching users' Gmail inboxes.
- Google Safe Browsing helps keep users secure from bad websites, automatically protecting more than 5 billion devices.
- We use a combination of automated flagging and human detection to enforce YouTube's Community Guidelines,[5] which include policies prohibiting spam, misleading practices and scams.
- We detect scam ads through a combination of both artificial intelligence (**AI**) and human evaluation, a process which helps ensure ads on our platform are adhering to the strict policies we have in place.[6]
- We've also expanded our financial services verification[7] program to Australia, which requires financial services advertisers in Australia to demonstrate that they are authorised by the Australian Securities and Investment Commission (**ASIC**) in order to promote their products and services through ads.

The Annexure to this submission contains more information about how some of Google's products combat scams.

---

[2] ACCC, Targeting scams: report of the ACCC on scams activity 2022, https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2022, 17 April 2023, page 3. See also earlier ACCC Scamwatch reports, from 2018 onwards.

[3] Google, Messages, Your chats stay private with spam detection, https://support.google.com/messages/answer/9327903.

[4] Google, Phone App Help, Use Caller ID & Spam Protection, https://support.google.com/phoneapp/answer/3459196.

[5] Google, YouTube Help, YouTube's Community Guidelines, https://support.google.com/youtube/answer/9288567?hl=en.

[6] Google, Advertising Policies Help, Google Ads policies, https://support.google.com/adspolicy/answer/6008942?hl=en.

[7] Google, Advertising Policies Help, About Australian Financial Services Verification, https://support.google.com/adspolicy/answer/12175793?hl=en.

We welcome the Government's proposal for banks, telecommunications providers, and digital platforms to meet certain reasonable minimum standards with respect to their anti-scam efforts and appreciate the Government's consultative approach to ensure that the manner in which those standards are implemented is technically feasible and effective.

In this submission, we provide our perspective on the following issues raised in the Consultation Paper:

- Part A: International developments including the UK Online Fraud Charter
- Part B: The Framework (questions 1-7)
- Part C: The definitions (questions 8-14)
- Part D: Ecosystem-wide obligations (questions 15-33)
- Part E: Sector-specific codes and standards (questions 34-42)
- Part F: Enforcement and Penalties (questions 43-45)

As we explain below, a number of the proposals would, in their current form, create a material level of uncertainty for businesses covered by the Framework. Several of the proposals are unworkable in practice and would have negative unintended consequences. Given the high fines as well potential consumer redress requirements, these unworkable proposals entail significant risk for businesses and challenges for effective enforcement by regulators.

We agree with the Government's objectives and have suggested ways to make the proposed obligations clearer in order to minimise the associated risk while still requiring industry to do more to take appropriate, proportionate action to combat scams.

Part A: International developments

Combatting online scams is not a problem that is unique to Australia. Other jurisdictions are also grappling with how best to address rising losses to scams. The Consultation Paper references some of the different proposals being pursued internationally, namely: by Singapore (limited to requirements for the banking and telecommunications sectors to combat phishing scams) and by the UK (through voluntary charters for telecommunications and retail banking sectors, the Online Safety Act enacted on 26 October 2023, and reimbursement requirements for banks, introduced by the UK Payments System Regulator for authorised push payment scams).

A further development in the UK, since the release of the Consultation Paper, is the introduction of the voluntary Online Fraud Charter 2023 (UK). On 30 November 2023, Google and YouTube became signatories to the Online Fraud Charter along with other online platforms (such as Amazon, eBay, Meta, Microsoft) and the UK Government. The Online Fraud Charter is specifically configured to drive targeted action by the signatories to mitigate risks posed by online fraud and scams.

We support adopting a similar approach in Australia to the UK's voluntary Online Fraud Charter in the first instance. A voluntary code would foster a positive environment giving rise to the following benefits to most effectively address potential harm from scams:

- **Flexibility** — an industry-led approach would allow for more flexibility in addressing online scams which are evolving rapidly;
- **Collaboration** — it would promote collaboration and cooperation between the Government and online platforms which would lead to increased sharing of ideas, expertise, and best practices;
- **Cost effectiveness** — it would reduce costs typically associated with complex and rigid regulations for the Government and businesses covered by the Framework;
- **Innovation** — incentives to innovate technologies and measures to combat scams would be encouraged through a collaborative regime; and
- **Global harmonisation** — online platforms are typically multinational and a uniform approach between jurisdictions can promote consistency and efficiencies, and facilitate effective efforts to tackle cross-border scams.

We suggest as a first step that the digital platforms sector be tasked with drafting voluntary commitments, drawing on international precedent — notably the UK Online Fraud Charter — tailored to Australian circumstances. A voluntary industry-led online scams code could form the basis for a sector-specific standard or code for digital platforms, if the Government considers mandatory obligations are necessary.

While legislated obligations to address scams have been imposed on platforms in some jurisdictions, no international proposal or regime contains a complex two-layer framework, enforced by multiple regulators, such as that proposed in the Consultation Paper. No other

regime purports to apply to the breadth of services that would come under the proposed 'digital communications platform' umbrella, or to impose such onerous and extensive obligations that apply to "*a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means*". And importantly no international regime or proposal requires digital platforms to reimburse users for losses from scams. For example, under the EU Digital Services Act (**DSA**), which recognises the nature of intermediary services provided by digital platforms, platforms are not liable for losses from scams until and unless the platform receives actual knowledge of the illegal content (and fails to remove the content expeditiously).

In 2023, the Council of the OECD (of which Australia is a member) adopted Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders.[8] In line with those guidelines, we would encourage the Government to engage with OECD counterparts, and adopt approaches based on relevant best practice in other jurisdictions. For global businesses that rely on global infrastructure and resources to combat scams, international alignment in respect of obligations would assist with the effectiveness and efficiency of compliance efforts and ensure that Australians and Australian businesses operating globally can do so under consistent regulatory frameworks.

[8] OECD Legal Instruments, Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders https://legalinstruments.oecd.org/public/doc/184/184.en.pdf, 2023.

Part B: The Framework

Questions on the proposed Framework (Q1-7)
<u>Summary of Google's position:</u> Mandatory obligations should only be considered if evidence from the implementation of voluntary measures shows they are ineffective. Google is willing to work with other digital platforms to develop voluntary commitments, and can assist the Scams Taskforce understand the ways in which voluntary measures can be designed, implemented, and tested. If there is an evidenced case for mandatory obligations, a flexible, single-layer framework would reduce uncertainty, complexity, and burden for industry and regulators. The diversity of regulated sectors makes consistent obligations challenging and potentially unworkable. Empowering a *single* regulator for each industry to register tailored codes of conduct addresses the complexity and challenges of the currently proposed Framework, while meeting the Government's objective of creating a framework that is sufficiently flexible to allow for future regulation of additional sectors.

The effectiveness of voluntary industry-led measures to combat scams should be considered in the first instance, before introducing mandatory obligations: As noted above, we suggest as a first step that the digital platforms sector be tasked with drafting voluntary commitments, with the effectiveness of those voluntary commitments being considered before mandatory codes are introduced.

The benefits of an industry-led approach include that it is cost effective, with costs largely borne by industry, rather than Australian taxpayers. Industry-led processes also enable closer collaboration with industry participants that will be subject to the code, ensuring the code benefits from industry's experiences of what is technically possible and effective, and can be more easily future-proofed.

A flexible, single-layer framework would reduce uncertainty and complexity, while enabling more tailored and effective obligations: We support, in principle, the Government's objective of creating a framework that is sufficiently flexible to allow for regulation of services if they become a target for bad actors and regulatory intervention is required to address harms to Australians. It makes sense to empower regulators to register codes with respect to a broad range of services where there is evidence of harm and voluntary measures have not been implemented or have consistently proven to be ineffective.

In our view, however, the proposal to have two layers of obligations in both legislation (be it the *Competition or Consumer Act 2010* (Cth) (**CCA**) or otherwise) and mandatory industry codes is unnecessarily complicated and in parts, unworkable. It:

1. **risks duplication of obligations**, leading to confusion about which regulator is responsible for enforcement. For example, it is currently proposed that each layer will have obligations relating to prevention, detection, disruption and response. The same

conduct could be alleged to contravene obligations in both layers of the Framework. For example, a business that is perceived to be slow to act on a consumer report of a potential scam may be alleged to be in breach of the proposed overarching obligation to "act in a timely manner on scam intelligence" (enforced by the ACCC) and the digital platform code proposed obligation to "have in place processes to act quickly on information that identifies a user or interaction is likely to be or is a scam" (enforced by the ACMA);

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.

These risks would not arise if there was only one layer of obligations in sector-specific codes. Regulators could be empowered to register codes for services where there is evidence of harm. This would deliver on the Government's objective of creating a framework that is sufficiently flexible to allow for future regulation of sectors, should they become a target for bad actors.

Overarching legislation should be limited to objectives: The risks outlined above could be addressed under a two-layer framework in which overarching legislation sets out objectives for the various codes and the outcomes those codes should be seeking to achieve, rather than a separate set of obligations.

We agree that all three identified industries should be required to meet a minimum standard with respect to addressing scams. However, the nature of the services, the way scammers use these services and the steps that each industry can take are vastly different. For example, it is not feasible for digital platforms that automatically surface relevant links to websites or content in *unpaid* search results in response to user queries to verify the identity of website operators or assess the veracity of every piece of content on the web or the intent of its creators. This is because general search engines typically only link to content available on the open web — with hundreds of billions of URLs in Google's search indexes, it is not possible to make such assessments. Similarly, it is also not viable to verify the identity of every creator or assess the veracity or intent of every piece of content on a video sharing platform like YouTube where 500 hours of video are uploaded every minute, and which are surfaced in response to user queries or recommendations. By contrast, where Google provides ads services, we have a business relationship with the advertiser. In that context, Google can (and does) offer advertiser verification (which all advertisers will eventually be required to complete), which helps reduce scam ads (although verification has practical limitations, particularly at the scale we operate).

For these reasons, we are concerned that a number of the proposed ecosystem-wide obligations in the Consultation Paper are unworkable across many sectors and poorly suited to

combating the underlying problem we are trying to address. In case the proposed Framework with overarching obligations is retained, we explore some of the obligations we believe should be more appropriately moved to sector-specific regulation (so they can be better tailored to the sector) in Part D.

The ACMA should have responsibility for any mandatory obligations that apply to digital platforms. The ACMA already has related powers and experience dealing with similar issues, including spam and phishing, as well as the telecommunications industry-developed *Reducing Scam Calls and Scam Short Messages Code*. We support the ACCC's role in facilitating coordination and cooperation across sectors on scams via the NASC and, as described below, would support the ACCC also being given notice and takedown powers with respect to specific examples of scam content.

Part C: The definitions

Questions on definitions (Q8-14)
<u>Summary of Google's position:</u> The definition of "scam" should be focused on the obtaining of a benefit and incorporate an element of objectively provable dishonesty, with express carve outs for the issues not intended to be covered (unauthorised fraud and consumer disputes about misleading or deceptive practices relating to sale of goods or services). The regime should be evidence-led, including to ensure that the resources and attention — of firms and regulators — are focused on the areas of greatest concern, where intervention could make the greatest practical difference to Australians. The definition of "digital communications platform" adopted from the misinformation context is not fit for purpose in a scams context, and is too broad and unclear. To ensure best use of government and industry resources, obligations should be imposed only on those services where evidence suggests they are most targeted by scammers or vulnerable to scams, based on the ACCC's Scamwatch reports over recent years. For example, unpaid search and news aggregation should be out of scope. A Minister or the regulator could be empowered to regulate additional services if evidence supports doing so in the future. The same obligations should not be imposed on all digital platforms. Unlike banks and telecommunications providers, each digital platform service is very different. However, the same types of online services should be regulated consistently (that is, equivalent obligations should apply on all providers of the relevant service in Australia, regardless of their size).

Definition of "Scam"

The Consultation Paper proposes the following definition of "scam" (emphasis added):

> *A scam is a dishonest **<u>invitation, request, notification or offer, designed to obtain personal information</u>** or a financial benefit by deceptive means.*

The Consultation Paper also suggests that the definition of "scam" is modelled on the definition of "fraud" in the current Commonwealth Fraud Control Policy (**CFCP**) (emphasis added):[9]

> *fraud is defined as '**<u>dishonestly obtaining</u>** a benefit or causing a loss by deception or other means'.*

The definition of "scam" proposed in the Consultation Paper focuses on invitations, requests, notifications and offers designed to obtain personal information or a financial benefit, whereas the definition of "fraud" in the current CFCP focuses on the completion of a scam ("*obtaining* a benefit or causing a loss").

[9] Australian Government, Commonwealth Fraud Control Framework, https://www.ag.gov.au/sites/default/files/2020-03/CommonwealthFraudControlFramework2017.PDF, 2017. We acknowledge the announcement on 1 February 2024 that the Commonwealth's fraud framework will be amended to include corruption, effective from 1 July 2024, and that the new framework will contain an amended definition of fraud. We consider the definition of fraud from the current CFCP to be more appropriate for the scams context.

We consider the definition of “fraud” in the CFCP to be more appropriate; without requiring the element of a financial benefit to the scammer, the proposed definition of “scam” is far too broad, opening up scope for ambiguity on the intent behind the design of the invitation or offer (e.g. what is dishonest design?). This would divert scarce compliance and regulatory resources away from identification of genuinely problematic activity and lead to regulated companies taking an overly conservative approach, leading to over-removal of content or actors (including content or businesses that are in fact legitimate). We understand the Government’s intention is also to regulate dishonest schemes to obtain users’ personal information, where that information is then used to obtain a financial benefit by deceptive means — that can be achieved using the definition of “fraud” in the current CFCP.

The Consultation Paper also states that the definition is not intended to capture:

- Unauthorised fraud, such as cybercrimes that may use hacking, data breaches and identity theft, that do not involve the deception of a consumer into “authorising” the fraud; and
- Consumer disputes about misleading and deceptive practices relating to the sale of goods and services, other than where a seller profile or website is not legitimate.

It is important that these activities are expressly carved out from the definition. The measures needed to address these kinds of harmful conduct are different to those contemplated by the Consultation Paper.

Definition of “Digital communications platform”

We have three primary concerns with the proposed application of the Framework to “digital communications platforms” and the definition of “digital communications platform”:

a. **There is no apparent rationale for aligning the anti-scam regulatory Framework with misinformation legislation:** We note that the definitions of “digital communications platform” and its sub-categories have been drawn from the exposure draft *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023*. However, the scope of services properly regulated by misinformation/disinformation legislation is very different to those properly regulated under a framework to limit the impact of scams. Perpetrators of disinformation are motivated by disseminating disinformation at scale through services that enable mass distribution, while scammers are financially motivated and therefore the services they choose to exploit to extract financial benefits from victims will differ.

   Further, the definitions of “digital communications platform” and its three sub-categories, drawn from the misinformation legislation — content aggregation services, connective media services, and media sharing services — are confusing, unfamiliar to industry, and potentially overlapping; particularly given there is no apparent distinction between the obligations imposed on each of the (very different) types of service.

   It would be much clearer to specify the types of service intended to be covered by the Framework by reference to their function (eg “messaging”, or “ads”).

b. **Application to too broad a set of services would lead to unnecessary burden, inefficient compliance work, and increased costs for Australian taxpayers. For example, unpaid search and news aggregation should be out of scope. The case has not been made for the need to regulate "content aggregation services" and "media sharing services" perhaps except to the extent that these services also provide paid advertising services.**

We agree that the Framework and other scams-related activity (such as through the NASC) will not eradicate all scams and that the Framework should be flexible and responsive to future changes in the scams ecosystem.[10] To ensure the best use of limited government and specialist industry resources, obligations should only be imposed on services where there is evidence (such as the ACCC's annual Scamwatch report, Targeting scams: Report of the ACCC on scams activity 2022),[11] that scams are prevalent or that the service is susceptible to scams, and where the most improvement can be achieved.

We have no evidence that substantial financial losses are arising from scams initiated via unpaid Google Search or Google News (which the proposed broad definition of 'content aggregation services' would cover), or that these services are commonly used by scammers to target victims. Moreover, Google has a limited ability to assess whether a website or content on those services is associated with a scam.

If obligations to prevent scams are imposed on services like Google Search (in respect of web listings), there is real risk of harm to the legitimate businesses that use those services. For example, it is not feasible nor desirable for a general search engine to verify the identity of every single website on the web. In general, search engines have no relationship (contractual or otherwise) with the sites they include in their results, other than having crawled those sites on the Web in the same way as a user with a Web browser might. Inevitably regulation of the kind being proposed, particularly given the proposed extreme penalties and novel consumer redress obligations, will incentivise platforms to remove content about which they receive a complaint, even where they are not sure that it is in fact part of a scam. And given that dynamic, there will be significant incentive for businesses' competitors and motivated individuals to submit false or aggressive removal requests to suppress their competition. We regularly encounter such gaming behaviour (see the examples of the existence and scale of this kind of behaviour in the discussion of Consumer Reports and requirements to act on such reports on pages 24-25). This would be detrimental to legitimate businesses, particularly smaller businesses that benefit disproportionately from digital platforms' referral traffic.

Similarly, it is difficult to conceive of how a news aggregator such as Google News (or Apple News), which displays or links to mainstream media news articles, could be

[10] Pages 6-7 of the Consultation Paper.
[11] Targeting scams: report, op. cit.

susceptible to scams. To the extent that scam content surfaces in the underlying articles, users who read those articles on the relevant mainstream media news website are equally susceptible to being scammed as users who click through to those articles from a news aggregator.

As regards liability, the proposed Framework — as it could apply to content aggregation services — sits in stark contrast with the recently announced amendments to the model defamation provisions which will (when passed by each State and Territory) effectively exempt search engines from liability for defamation where the facts of a situation are not well-established. The State and Territory Attorneys-General have recognised the burden that individual defamation complaints about digital platforms have imposed on Australian courts and sought to limit them.

A Minister or regulator could be empowered to impose obligations on additional services in response to shifting threats, but in the meantime over-regulating services that are not of material relevance to scammers would consume critical scam-fighting resources with inefficient compliance work. There should be consultation before the Framework applies to new types of digital platform services to allow businesses an opportunity to raise any nuances and provide sufficient time to prepare for compliance.

c. **Different obligations should apply to different types of digital platform service.** We would urge caution before imposing the same obligations on all "digital communications platforms" from the outset, without regard to:
    i. the extent to which those particular types of services are being used by scammers — or are susceptible to such use; and
    ii. how those services work, how they are used by scammers, and what action may be feasible.

    Unlike banks and telecommunications providers, digital platforms are very different from one another, and are used by scammers to different extents and in different ways. Some are more susceptible to use by scammers than others. Regulation should be tailored accordingly.

Large and small players that provide the same service should be covered: if the Government identifies a type of digital platform service as being a target for scammers, all businesses that supply that type of service in Australia should be subject to the Framework. Scammers are agile, and consumers should be protected from harm regardless of whether they are dealing with a large provider or a small provider.

Part D: Ecosystem-wide obligations

Questions on overarching principles-based obligations (Q15-19)
Summary of Google's position: If the two-layer approach is retained, the overarching legislation should contain objectives and outcomes for the various codes, rather than enforceable obligations. If obligations are retained in the overarching legislation, they should be high-level and several of the proposed obligations should be moved to sector-specific codes because they are not applicable or not workable for digital platforms at an overarching level. Any obligations on platforms should involve considerations of proportionality. Businesses that satisfy code requirements should be exempt from action for breach of any ecosystem-wide obligations and non-compliance should be enforced by the regulator, not subject to claims by individuals or other organisations seeking redress.

Part B outlines our position on the proposed Framework. If, however, the Government proceeds with the two-layer Framework proposal then:

- **The overarching legislation should be limited to objectives and outcomes:** Instead of two layers of overlapping and potentially conflicting obligations, the overarching legislation could set out objectives for the various codes and the outcomes those codes should be seeking to achieve.

- **Alternatively, the overarching legislation should contain only the highest level obligations:** Several of the overarching obligations set out in the Consultation Paper do not readily apply to digital communications platforms, or are otherwise not workable. Those obligations should be moved to the relevant sector specific codes (see **Table A**, below on page 17), or otherwise reframed in a more applicable way.

- **If overarching obligations are retained, they should be partnered with tailored, specific, and clear obligations in sector-specific codes:** A preferable option to the current proposal would be to have:
    i. High level obligations in the CCA / primary legislation, which could require designated businesses to, for example, take proportionate and reasonable steps to detect and respond to scams;[12] and
    ii. More detailed obligations in codes that set out what specific steps / measures the designated business in the relevant sector needs to take, which, if taken, are then deemed to satisfy the high level obligations in the CCA / primary legislation.

  The benefits of this approach include:
    i. Minimising uncertainty about what action would constitute "reasonable steps".

[12] The concept of proportionality is used in the UK's recently enacted Online Safety Act 2023 (c.50) (**OSA**), e.g. section 10(2) and 10(3).

ii. Avoiding a potentially overwhelming caseload of protracted/complex disputes about whether 'reasonable steps' have been taken, particularly if consumers have a right of redress including through an ombuds scheme.
iii. Giving business regulatory certainty that where they comply with an applicable code they will not be exposed to liability under the overarching reasonable steps obligation.

- **Non-compliance with the overarching obligations should be enforced by the regulator, not subject to claims by individuals or other organisations seeking redress.** It would be extremely burdensome for covered businesses if their compliance with the overarching obligations proposed in the Consultation Paper was open to challenge by individuals (or organisations beyond the responsible regulator). In this regard, please also see our comments on Consumer Reports below (on page 24 onwards). For example, covered businesses could be exposed to potentially a huge number of claims about whether they complied with obligations to "develop, maintain, and implement an anti-scam strategy", "implement anti-scam systems", "train staff to identify and respond to claims" and so on. It is not clear whether the Government intends this, but inclusion of such obligations in legislation such as the CCA would appear to enable such claims to be brought and a range of orders to be sought from the court, leading to a fragmented and inconsistent enforcement practice which engenders further uncertainty on the interpretation of the obligations. Such disputes would likely also require the disclosure of commercially sensitive information about platforms' internal strategies and systems in discovery processes. The prospect of such claims or disputes is even more likely if an external ombuds is empowered to hear claims.

  If the Government intends for individuals to be able to bring claims alleging failure to comply with the overarching obligations, and to seek redress, the scope of the obligations must be narrowed and there should be further consideration of the obligations in respect of which such claims should be capable of being brought, taking into account issues such as burden on businesses, impost on courts / ombuds schemes, proportionality, and the extreme sensitivity of confidential information about how businesses combat scams. It would be extremely concerning and counterproductive to our efforts to combat scams if this type of information was made public.

- **Obligations should be engaged where content meets internal thresholds of suspicion, or there is actual knowledge:** In respect of the definition of a "scam", the application of the regime should incorporate some element of objectively provable dishonesty. A digital platform may not be in a position to ascertain whether a seller profile or website is legitimate, and indeed many are not able to assess with any degree of certainty the legitimacy of third party content accessible on the Web. We suggest a standard that applies where content meets providers' "internal thresholds of suspicion", consistent with the approach adopted under the UK Online Fraud Charter. Alternatively, a standard that involves considering whether the platform (or other covered business) had actual knowledge of the dishonest scheme would be appropriate, and consistent

with the approach under the DSA. Under the DSA, a platform is regarded as having actual knowledge (which gives rise to an obligation to act to remove or disable access to relevant content) if it receives a notice about the content and a diligent provider can identify the illegality of the relevant activity or information without a detailed legal examination.

If the threshold for actioning suspicious content or accounts is set too low, or is uncertain, providers covered by the Framework will over-remove, creating friction or harming legitimate businesses, especially small to medium businesses, who rely upon platforms to reach new customers.

While Google considers that its scam-combatting activities and associated processes would already comply with some of the proposed obligations, we would need to make operational changes to meet other obligations, and implementation of the requirements in the context of some of our products would pose particularly significant challenges. **Table A** below sets out our key comments on the obligations outlined at page 12 of the Consultation Paper. We are also concerned that compliance with some of the proposed obligations would disproportionately divert specialist resources deployed to combating and staying ahead of scammers and other bad actors.

Table A: Proposed ecosystem-wide obligations — Google's key comments

Proposed obligation	Google's position
Prevention	
A business must take all reasonable steps to prevent misuse of its services by scammers, so that an undue burden is not placed on consumers or other market participants to prevent scams.	The proposed obligation, backed by substantial penalties, risks incentivising platforms to remove legitimate content, negatively impacting users and potentially harming businesses — especially SMBs — that use intermediary services to support their economic livelihood. **Reasonable steps**: While a "reasonable steps" obligation has the benefit of flexibility of application to particular circumstances, it entails a significant degree of uncertainty about what measures would satisfy the obligation and what would fall short of it. In other contexts, this uncertainty is addressed through case law (while under the proposed Framework the covered businesses would be exposed to liability and potentially significant penalties from the outset). An obligation to take "all" reasonable steps arguably imposes a higher (but still uncertain) burden, and could lead to interpretations that require a business to, effectively, take all conceivable steps to minimise liability and disputes. The unintended consequences of this obligation could result in online services over-removing legitimate content to limit their

Proposed obligation	Google's position
	potential exposure. There is currently no technology that could provide full effectiveness in filtering and blocking illegal content. Not only can available technologies be circumvented; they are also imperfect in distinguishing what may be considered to be illegal or legal. This is particularly true for scams, where scam actors quickly adapt their methods and operations. Reliance on imperfect technology creates real risks that platforms over remove legitimate content. **Proportionality**: It is unclear whether the proposed obligation to take all reasonable steps would involve consideration of proportionality, consistent with the approach in other jurisdictions. For example, the principle of proportionality is a central concept in the UK's Online Safety Act. This concept should be expressly included in the proposed Framework. A principle of proportionality would enable covered businesses to take into account factors such as the level of risk, likelihood of loss, and impact on merchants / advertisers. For example, Google has more stringent requirements for advertisers of financial services in Australia because of the greater potential for harm to consumers and historical risks experienced in that context. At the same time, Google is mindful that there is a tradeoff in introducing friction and degrading value for small businesses / merchants and advertisers if such stricter requirements were to be applied across the board, beyond financial services. **Prevent misuse:** Similarly, a broadly defined underlying obligation to "prevent misuse" leaves services and regulators without legal clarity or certainty and risks fundamental rights. Other jurisdictions recognise the importance of intermediary liability protections. For example, EU law prohibits proactive monitoring obligations and imposes liability on where a platform has "actual knowledge" (see page 7, Part A and the discussion of Obligations should be engaged where content meets internal thresholds of suspicion, or there is actual knowledge on page 16 above).
Detection and disruption	
A business must seek to detect, block and prevent scams from initiating contact with consumers.	It is unclear what action would satisfy the standard of "seek to" detect, block and prevent. In this context, clarity is important. A requirement to engage in general monitoring to detect all scams would be problematic for the reasons set out in the row above. An obligation that includes a proportionality standard, like that

Proposed obligation	Google's position
	adopted in the UK OSA, would be preferable. We recommend that the currently proposed obligation is replaced with an obligation to "Have proportionate systems and processes for detecting and blocking scams that meet internal thresholds of suspicion".
A business must seek to verify and trace scams where scam intelligence has been received.	The definition of scam intelligence needs to be developed and the requirement to "verify and trace" is unclear in a digital platform context. It is also unclear how this obligation fits with the proposed obligation in the row below. If the expectation is to trace all scams on a digital platform, that is not possible at the scale of the Internet.
A business must act in a timely manner on scam intelligence received through information sharing, consumer reports, complaints and other means.	A requirement to act on all consumer reports would be problematic for the reasons set out in the discussion of Consumer Reports and requirements to act on such reports, below (on page 24 onwards). Any obligation to act should be limited to scams that meet internal thresholds of suspicion. As noted above, a requirement to take down scams upon notices from the ACCC/ a regulator would be preferable. This does not preclude a platform from acting on user notices, however it affords the platform flexibility when dealing with notices other than from a regulator (noting platforms' existing incentives and policies to remove scam content when detected).
Where a business receives intelligence that a consumer is or may be a target of a scam, the business must take steps to disclose this to the consumer in a timely manner to minimise the risk of consumer harm or loss.	This obligation is more difficult to apply in a digital platform context than in the context of a relationship between a bank and its customer or a telecommunications provider and its customer. ● For valid privacy reasons, consumers often use digital platforms anonymously (e.g. as signed-out users), such that they cannot be contacted in the future. ● Google already takes actions to filter spam and scam SMS, telephone calls, and emails, and Google Safe Browsing already warns users about potentially harmful content on the Web. ● It would likely be difficult for a user to connect a warning to a past exposure. In the digital platform context, at the scale at which we operate, a blunt requirement to provide further warnings is likely to lead to over-warning and warning fatigue, with limited real impact for consumers. Google is exploring what changes it could usefully make in

Proposed obligation	Google's position
	this respect, but it would be unhelpful to mandate this obligation in legislation.
Response (obligations with respect to consumers)	
Where a consumer has identified they have been affected by a scam, businesses must take all reasonable steps to prevent further loss to the consumer and treat consumers fairly and consistently.	See our comments on the similar obligation in the row above. It is not clear how a digital platform could prevent further loss to a consumer given transactions are completed off-platform. It would be preferable to include sector-specific obligations in a code that set out what reasonable steps would be in that context. A proportionality element should be incorporated.
A business must have user-friendly, effective, transparent, and accessible complaints handling processes for consumers or users to make a complaint about how a scam report was handled or in relation to a business's response to scam activity (including steps taken to prevent, detect, disrupt and respond to scam activity).	We support the objective of ensuring businesses have user-friendly and effective complaints handling processes, and deal with consumer complaints fairly and promptly. However, we need to make sure that systems are proportionate and effective, and do not create perverse incentives. Please see our comments on Dispute resolution requirements and processes should be proportional to the nature of the service and the potential consumer harm in response to the questions on consumer reports, complaints handling, and dispute resolution below (pages 26-27).
Where a consumer escalates concerns with a business, they should be dealt with fairly and promptly, and consumers should be given access to information about dispute resolution options where applicable.	
Reporting (obligations to regulators and other businesses)	
A business must take reasonable steps to notify other businesses, the NASC and relevant regulators promptly of intelligence about suspected or identified organised large-scale scam activity as well as rapidly emerging or cross-sectoral scam activity.	Please see our responses below to the Questions on information sharing requirements for legal and practical impediments (pages 23-24). This kind of activity is better developed voluntarily, and should be directed through the NASC.

Proposed obligation	Google's position
A business must share data and information on the incidence of scams, and action taken in response, with designated industry bodies, law enforcement and regulators, and the NASC.	Digital platforms would have data about the number of notifications they receive, and content removed, but that data (a) may not differentiate between "scams" and other types of harmful content; and (b) would not address the actual incidence of scams (given scams are completed off-platform). More consideration should be given to the utility of digital platforms sharing the kind of information that is available to them, given the high burden involved in creating additional processes. Reporting obligations should be imposed only if the utility of reporting outweighs the burden on business, and does not require disclosure of information that may compromise efforts to combat bad actors. Please see our responses below to the Questions on information sharing requirements (pages 23-24).
A business must respond to an information request from the ACCC within the timeframe specified.	This obligation should be subject to guardrails so that the ACCC's powers are exercised reasonably and proportionately.

Questions on anti-scams strategy obligation (Q20-25)
Summary of Google's position: The Framework should not be prescriptive about which governing body within the business should be responsible for signing-off on anti-scams strategies. Regulator involvement in anti-scams strategies should be limited to guidance and oversight. Reporting obligations should be imposed only if the utility of reporting outweighs the burden on business, and does not require disclosure of information that may compromise efforts to combat bad actors.

Google products operate in very different ways, each with different approaches to scams, reflecting their nature, users' expectations, and risks. A requirement to have an anti-scams strategy should accommodate tailored approaches to scams within a business, its different products, and their different risks and features. The requirements should also take into account the structure and global nature of many digital platforms' businesses. Relevantly:

- **Governing body for sign-off on anti-scam strategy:** We agree that anti-scam strategies should be signed off by a high level of governance within a business, however the code should not be prescriptive about which governing body should sign-off on the strategy. Many platforms have specific divisions responsible for combating bad actors and scams, and it may be more appropriate for the leadership of those divisions to approve the scams strategy. Given the structure and global nature of our business, and the matters which are signed-off by the Alphabet board in the ordinary course, it would be disproportionate to require that governing body to sign-off on the anti-scam strategy / strategies. Such a requirement could also discourage agile evolution of strategies to

meet emerging threats and leverage developments in technology and capability.

- **Frequency of review:** The frequency at which businesses should review their anti-scam strategies can vary based on factors such as the nature of the industry, the evolving landscape of scams, and the specific risks associated with the business model. It is in a business' own interests to review and keep up to date its anti-scam strategy, so we do not consider it necessary to mandate a requirement that businesses review their strategies at a particular cadence.

- **Regulator involvement:** It is important that businesses should be able to receive guidance from regulators in respect of their anti-scams strategies, if needed. However, their level of engagement should be balanced, providing guidance and oversight without imposing undue burdens on businesses. We therefore do not support the proposal that a business' anti-scam strategy should be subject to review by the ACCC, and that the ACCC could play a role in working with businesses on their anti-scam strategies to ensure they are fit-for-purpose and consistent with similar businesses in their sector. This seems disproportionate when compared to the treatment of other types of conduct that have the potential to result in significant harm to consumers, such as cartel conduct. The ACCC does not review and input on business' competition compliance policies or strategies (except in some instances where the business has contravened the law).

- **Transparency and reporting:** We already publish regular transparency reports outlining our efforts to combat bad actors — for example, our Ads Safety Report[13] and our YouTube Community Guidelines Enforcement Report.[14] Similarly, we share regular updates on our efforts on our blog, with examples including posts on How we fought bad apps and bad actors[15] and How we fought Search spam.[16] However, there are dangers with unbounded transparency. There is a balance to be struck between the interests of providing transparency to the reporting user / public, and the risk that the increased transparency could reveal commercially sensitive information, or otherwise be misused by bad actors, leading to greater harm. We agree that businesses should be able to determine the level of detail on their anti-scam strategy that could be made available to the public.

[13] Google, Ads and Commerce Blog, Our 2022 Ads Safety Report https://blog.google/products/ads-commerce/our-2022-ads-safety-report/, 29 March 2023.
[14] YouTube Community Guidelines enforcement, op. cit.
[15] Google, Security Blog, How we fought bad apps and bad actors, https://security.googleblog.com/2023/04/how-we-fought-bad-apps-and-bad-actors.html, 27 April 2023.
[16] Google, Search Central Blog, How we fought Search spam on Google Search in 2022, https://developers.google.com/search/blog/2023/04/webspam-report-2022, 11 April 2023.

Questions on information sharing requirements (Q26-29)
<u>Summary of Google's position:</u> We support voluntary information sharing via the NASC. Mandatory information sharing raises legal and practical issues that would need to be worked through.

Voluntary information sharing via the NASC should continue: In principle, we support information sharing through the NASC as a central contact point between all stakeholders. The NASC is already playing an important role and is making investments in building its data-sharing capability and tech, as acknowledged in the Consultation Paper.

Google is already receiving some scam intelligence from the NASC and acting promptly on that intelligence. Currently, we are ingesting scam intel from the NASC manually. Technology solutions would be required for Google to be able to ingest and act on greater volumes of scam intelligence. These processes are better arranged voluntarily and flexibly than by regulation.

Mandatory information sharing raises legal and practical issues that need to be worked through: We and other stakeholders face the following potential impediments and challenges with sharing scams intel, which should be considered further and would need to be addressed:

a. **Data sharing should only be through the NASC and should not be mandated directly between businesses:** It would be highly inefficient to require businesses to build data connections with each other business covered by the Framework.

b. **Legal impediments / risks of information sharing**, including the following:

   i. Potential exposure to liability to users (particularly business users) if scam intelligence is incorrect (e.g. the business / actor is legitimate, but has been disabled / removed from platforms, even if such action is corrected and therefore temporary).

   ii. Competition law risks. Businesses could be subject to allegations that they have engaged in a collective boycott of a business / customer, or restricted supply to that business / customer in contravention of the prohibitions on cartel conduct. Additionally, to the extent that the obligations require regular interactions with competitors, such engagements are inherently risky and competition law risks that may arise would need to be managed.

   iii. Data privacy concerns, especially if the data contains personally identifiable information or sensitive details.

   iv. Cybersecurity risks: concerns about the cybersecurity measures in place at the receiving organisation may discourage information sharing.

c. **Practical impediments to effective information sharing in the digital communications platform context**: Identifying the scam / scammer in a digital platforms context is more challenging compared to other sectors — for example, banking relies on unique account numbers, and telecommunications relies on unique phone numbers. A user may have different identifiers across digital platforms (such as a URL, an email address, multiple bespoke usernames, etc), and the identifier used on Google's platforms may not match the scammer's identifier used on Facebook or TikTok.

Questions on consumer reports, complaints handling and dispute resolution (Q30-33)
<u>Summary of Google's position:</u> We do not believe there is a clear need for mandatory industry-specific Internal Dispute Resolution (IDR) and External Dispute Resolution (EDR) obligations for digital communications platforms. We look forward to engaging with the Government on its proposal that the digital platforms industry develop voluntary IDR standards. If the Government considers that an additional external ombuds scheme for digital platforms is required, the process and scope of that scheme need to be very carefully designed through a clear framework to ensure that the cost and complexity of adjudicating complaints can be kept proportionate to their seriousness, including (where relevant) the amount of money at stake.

Consumer report and redress issues require further consideration, to avoid unintended consequences: Before we address the questions relating to IDR and EDR, we draw the Government's attention to four key issues relating to consumer reports and consumer redress:

a. **Consumer Reports and requirements to act on such reports:** The Consultation Paper states that a designated business "*would be required to have a reporting mechanism in place for users to report scams, including in cases where they have identified but not been affected by a scam. This will allow users to notify the business of scam activity for investigation*". The business would also be required to act in a timely manner on scam intelligence received through consumer reports, to take all reasonable steps to prevent further loss to the consumer, and provide accessible complaints handling processes for consumers to make a complaint about how a scam report was handled.

   In general, Google's products enable consumers to report content, including scams. Requiring all digital platforms "to act" on reports, however, and "to take all reasonable steps to prevent further loss to the consumer" and have processes for complaints about how a scam report was handled, would impose a significant burden. Some of our free services (which would appear to be in scope of the proposed Framework) have more than a billion users. 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. For instance, bad actors in the USA weaponised copyright law to harm competitors by submitting thousands of bogus takedown reports targeting over 600,000 URLs. This resulted in over 100,000 business websites being removed and cost millions of dollars and thousands of hours lost in employee time.[17] A requirement to investigate every allegation of scam content to the point of certainty, particularly given the regularity with which we receive abusive reports, would not be workable for a business of our scale.

As discussed above, if businesses are faced with potential liability for not removing notified content in a timely manner, they will have strong incentives to remove all content of which they are notified. This would lead to the over-removal of content, to the detriment of consumers and legitimate businesses.

If obligations to act on scam reports are retained, they must be limited to scams that meet internal thresholds of suspicion, as opposed to all scam reports made by consumers. Under the DSA, for example, notices provided by consumers to a hosting service will lead to an obligation to act to remove or disable access to content only "where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination" (art.16(3) DSA).

b. **Empowering regulators to issue takedown notices:** Other options for enhanced scam protection could be explored, such as empowering the ACCC to issue specific takedown notices for scams. We have previously proposed that the ACCC (or another regulator) be empowered to issue specific takedown notices in respect of scams, with appropriate safeguards.[18] This is a preferable approach because the ACCC (or another regulator) is independent and has the expertise to assess whether or not there is a scam. There would need to be an appeal mechanism for the owners of content that is removed.

c. **Redress issues to be worked through:** The Consultation Paper provides, in relation to the requirement to have IDR and EDR processes, that *"This is intended to ensure that when a business has not met its obligations under the Framework, either the business or an EDR process can consider whether the consumer should be compensated for any losses they have incurred to a scammer*".

   No other international regime or proposal requires digital platforms to reimburse users for losses from scams. Before such a requirement is implemented with respect to digital platforms in Australia, there would need to be:

   i. greater certainty about the obligations that apply to businesses and what activities will satisfy those obligations so that businesses can appropriately manage their potential exposure.

[17] Google, Taking legal action to protect users of AI and small businesses (November 2023), available at https://blog.google/outreach-initiatives/public-policy/taking-legal-action-to-protect-users-of-ai-and-small-businesses/.
[18] Google's Response to Government Consultation on ACCC Report on Platform Regulation, 28 February 2023, at pages 9, and 38-43.

ii. further consideration of whether it is fair and appropriate for digital platforms that provide free services that simply automatically surface relevant websites or content to be exposed to liability for third party scams ultimately completed using other services.

iii. further consideration of how redress should be apportioned where the consumer was reckless/negligent/ignored warnings. Relatedly, there should be further consideration of whether a redress regime would create risk-taking incentives and result in more scams — users deliberately engaging with scams in the knowledge that they would be compensated or taking risks that they otherwise would not take. It is not appropriate for businesses to provide insurance in this way.

iv. further consideration of how redress should be apportioned where multiple businesses (whether in the same sector or across sectors) have not met their obligations. We note that the Consultation Paper seeks views on this (as well as compensation caps), but there are critical threshold issues to be worked through before this detail can properly be addressed.

In this context, it's worth bearing in mind that the e-Commerce Directive (eCD) and the DSA in the EU, provide hosting services, like video-sharing services and social networks, with certain protections from liability for user content. Similarly, section 230 of the Communications Decency Act in the United States provides intermediaries with protection from such claims.

d. **Potentially disproportionate regulatory burden:** Enabling consumers to make claims against digital platforms on the basis of allegations that, for example, a platform has not taken reasonable steps to prevent misuse of its services, and have such claims dealt with in EDR, could lead to large numbers of complex claims for compensation. EDR bodies may not be well placed to handle such claims. The Government resources required to adjudicate such complaints, and business resources to defend them, could far outweigh the amounts in dispute.

   For example, in respect of Search, there are trillions of webpages on the world wide web, which are constantly being updated, and hundreds of billions of webpages in Google's index. Billions of searches are conducted around the world every day, and around 15% of the searches we see each day are searches we've never seen before. Whilst Google continues to invest in tools, processes, automated detection technology, and teams that help us elevate trustworthy information and remove inappropriate content across our services, it is not feasible for Google to prevent all scam websites from surfacing in unpaid Search results. The Framework could therefore open Google up to a huge number of claims for compensation from individuals where Google cannot realistically control its exposure.

Dispute resolution requirements and processes should be proportional to the nature of the service and the potential consumer harm: As a general proposition, we agree that business users and consumers should have access to effective processes for resolving disputes, and we strive to provide effective customer support and dispute resolution mechanisms to businesses and consumers. However, the requirements and processes should be proportional to the nature of the service and the potential consumer harm.

Google already takes the following steps in respect of consumer reports, complaints handling, and dispute resolution:

a. **IDR:** each of Google's products has tailored policies and enforcement and dispute resolution processes reflecting the nature of the product, its users, and the type of issues and complaints that arise. These processes may involve a combination of machine learning, AI, and specialist review teams and address the vast majority of issues before they result in a complaint or a dispute. We provide online tools to seek support (including the ability to request refunds) and raise complaints, and we believe our processes enable us to to ensure that a consumer communication is directed to the team most likely to be able to assist and give the best overall service in order to resolve issues in a timely manner, bearing in mind the complexities of scale.

   We also note that the Government has indicated that it will call on the digital platforms industry to develop voluntary IDR standards by July 2024.[19] We look forward to engaging with the Government on this initiative.

b. **EDR:** In addition to Google's IDR, Australian consumers and businesses have access to a range of EDR mechanisms. This includes (depending on the nature of the complaint): the Australian Small Business and Family Enterprise Ombudsman; the State and Territory Small Business Commissions; Ad Standards (for complaints by consumers about 'offensive' advertising); various Civil and Administrative Tribunals, such as ACAT, NCAT, VCAT, and QCAT; the State and Territory Offices of Fair Trading and the ACCC; the OAIC; the ACMA; the eSafety Commissioner's Office; the AEC (in relation to election advertising) and the Australian Financial Complaints Authority (in relation to payment services).

In light of the above, there is not, in our view, a clear need for mandatory industry-specific IDR and EDR arrangements for digital communications platforms. If the Government considers that an additional external ombuds scheme for digital platforms is required, the process and scope of that scheme need to be very carefully designed through a clear framework to ensure that the cost and complexity of adjudicating complaints can be kept proportionate to their seriousness, including (where relevant) the amount of money at stake.

[19]Government Response to ACCC Digital Platform Services Inquiry, 8 December 2023, available at https://treasury.gov.au/sites/default/files/2023-12/p2023-474029.pdf, p3.

Part E: Sector-specific codes and standards

Questions on sector-specific codes (Q34-42)
Summary of Google's position: Flexible, sector-specific obligations, that recognise differences between digital services, are more likely to be effective in addressing harms from scams, which are ever-evolving. Any mandatory obligations should involve consideration of proportionality, consistent with the standard in the UK's OSA.

At the sector-specific level, the Government has proposed two alternative means of developing scam-related obligations for digital communications platforms: (1) obligations developed by the ACMA in consultation with the industry; or (2) obligations developed by digital communications platforms to be registered and enforced by the ACMA, if deemed necessary. Google supports an industry-led approach. As outlined above, we suggest as a first step that the digital platforms sector be tasked with drafting voluntary commitments.

Any digital platform-specific scams code should have tailored obligations for the different types of digital platform services that it covers, reflecting the different nature of those services. This is the approach taken in the UK Online Fraud Charter, which contains categories of obligations that apply to all signatories and additional obligations that apply to specific types of services.

Our key comments on the possible digital communications platform specific obligations outlined on page 21 of the Consultation Paper are set out in **Table B** below.

Table B: Possible digital communications platform specific obligations — key comments

Possible obligation	Google's position
Prevention	
A provider of a digital communications platform must implement processes to authenticate and verify the identity and legitimacy of business users and advertisers, to prevent users from selling or advertising scam products and services on the platform.	Google could not comply with such an obligation if 'business users' includes websites that are displayed in unpaid search results in response to users' searches, or all forms of creator content displayed on YouTube. Google cannot authenticate or verify the identity of websites on unpaid search or of creators using standard features on YouTube. Google already offers authentication and verification measures for all advertisers (although they are not always mandatory), and it already requires this in respect of financial services, online pharmaceutical, and online gambling advertisements in Australia.[20]

[20] Google, Advertising Policies Help, Verification programs, https://support.google.com/adspolicy/topic/9646742.

Possible obligation	Google's position
	In respect of financial services advertiser verification, additional relevant data could be shared by ASIC to assist verification: We see opportunities for the Government / regulators to facilitate the identification and prevention of scams by sharing relevant information with industry participants and individuals. For example, our Australian Financial Services Verification program[21] for financial services ads in Australia relies on financial services licence information held by ASIC. ASIC maintains various professional registers which can help consumers and businesses verify the legitimacy of registered entities by checking the business name, address, licence number etc. The professional registers do not currently publish details of the licensee's website. Including licensees' website details on ASIC's registers (or at least giving licensees the option if they prefer) would assist our verification process (as well as being a useful check point for consumers and businesses to assess the veracity of a financial services provider with which they are dealing). **The requirement to authenticate "legitimacy" is unclear.** Google's verification measures for advertisers check whether the person is who they say they are or that the business is a registered business; they do not (and could not) detect fraudulent activity nor enable better content classification.
A provider of a digital communications platform must have in place processes and methods to detect higher risk interactions, and take appropriate action to warn the user, block or disrupt the interaction, or take other measures to reduce scam activity, content or profiles such as blocking or disabling accounts based on shared intelligence.	To account for differences in digital platforms' services and the way in which users interact with them, it would be preferable to limit obligations to having "proportionate systems and processes" to minimise the presence of scams (consistent, for example with the obligations in the UK OSA). This would enable systems and processes to be tailored taking into account the nature of the service and risk assessment. It should be open to covered businesses to determine the appropriate response to shared intelligence, based on its internal thresholds of suspicion and review of the intelligence. A requirement to block or disable accounts based on shared intelligence (without scrutiny of that intelligence) could result in the removal of legitimate content / disabling of legitimate accounts. We support, in principle, a requirement to act on takedown notices issued by a regulator.

[21] About Australian Financial Services Verification, op. cit.

Possible obligation	Google's position
Detection and disruption	
A provider of a digital communications platform must have in place methods or processes to identify and share information with other digital communications platform providers and the NASC that an Australian user is likely to be or is a scammer.	Please see the issues raised under the heading Questions on information sharing requirements (on pages 23-24).
A provider of a digital communications platform must have in place processes to act quickly on information that identifies a user or interaction is likely to be or is a scam, including blocking or disabling the account being used by the scammer.	"Is likely to be" is too low a threshold, which could result in large scale removal of legitimate content and potentially inconsistent enforcement decisions. This obligation should be matched to the service's internal standards of suspicion. Strict timelines would lead to over-removals, as discussed below under this table.
Response (obligations to consumers)	
A business must respond to an information request from the ACMA within the timeframe specified.	This obligation should be subject to guardrails so that the ACMA's powers are exercised reasonably and proportionately. It is important that the Code specifies ACMA's role and responsibilities to avoid any duplication with ACCC inquiries, for example.

We consider that sector-specific codes should not specify rigid timeframes for a business to take action. We support the use of flexible standards such as "promptly" or "expeditiously". Rigid timelines for acting on scams are likely to lead to over-removal of content to the detriment of legitimate traders. It is important that complaint systems are able to remain sufficiently flexible to allow platforms to take a risk-based approach, enabling them to respond more quickly to urgent issues where there is a high risk of broader harm, while allowing sufficient time to properly consider more nuanced issues. We note that the eCD, DSA and OSA do not have strict turnaround times, giving review teams time to make appropriate decisions before removing content. The DSA also requires users to substantiate their notices, which helps services review complaints expeditiously and accurately.

Part F: Enforcement and Penalties

Questions on approach to oversight, enforcement and non-compliance (Q43-45)
Summary of Google's position: Penalties for non-compliance with mandatory obligations should be proportionate to other industry codes. A business should not be exposed to two sets of penalties for the same conduct, particularly with respect to new and untested obligations.

Penalties for non-compliance with mandatory obligations should be proportionate and the usual principles for determining penalties should apply. A business should not be exposed to two sets of penalties for the same conduct, particularly with respect to new and untested obligations.

The proposed maximum penalties under the CCA are significant, excessive and disproportionate compared to penalties applicable to other industry code breaches. For example, in respect of prescribed industry codes under the CCA:

a. The Franchising Code (an industry code under the CCA): most breaches attract maximum penalties of 600 penalty units ($187,800) except certain contraventions which, since 2022, attract penalties of the greater of $10m, 3x the benefit gained or 10% of turnover.

b. The Horticulture Code and Dairy Code (also industry codes under the CCA): maximum penalties of 300 penalty units ($93,900) apply.

c. The Gas Market Code has a tiered penalty structure:

    i. Tier 1 pecuniary penalties apply to breaches of the following provisions: Price rules (sections 26-28), Good faith (sections 30-31), Compliance with exemption conditions (section 73). The maximum penalty for corporations is the greater of: $50 million, or if the Court can determine the 'reasonably attributable' benefit obtained, 3 times that value, or if the court cannot determine the value of the 'reasonably attributable' benefit, 30% of the corporation's adjusted turnover during the breach turnover period for the offence;

    ii. Tier 2 pecuniary penalties apply to breaches of the following provisions: Negotiation requirements (sections 10-21), Procedural rules for agreements (sections 24-25). The maximum penalty for corporations is $1,878,000 (6,000 penalty units); and

    iii. Tier 3 pecuniary penalties apply to breaches of the following provisions: Record keeping, information and publication (sections 33-41), Obligation to provide additional or corrected information (section 74). The maximum penalty for corporations is $939,000 (3000 penalty units).

Similarly, in other industry code contexts, the maximum penalties are significantly lower than those proposed in the Consultation Paper:

a. The online safety codes enforced by the eSafety Commissioner attract penalties of $156,500 (500 penalty units) if an industry participant covered by the code has contravened the code and failed to comply with a written notice from the eSafety Commissioner directing them to comply with the code (section 143 of the *Online Safety Act 2021*).

b. The Reducing Scam Calls and Scam Short Messages Code, enforced by the ACMA, attract penalties if an industry participant covered by the code has contravened the code and failed to comply with a written notice from the ACMA directing them to comply with the code (section 121 of the *Telecommunications Act 1997*). The maximum penalty for a body corporate is not to exceed $250,000 per contravention (section 570 of the *Telecommunications Act 1997*).

There should at the very least be a tiered penalty regime to ensure any penalties are proportionate. There should also be a grace period before penalties apply, as businesses adjust their operations to comply with the new obligations and there is greater clarity on the scope of those obligations (including from guidance by the regulators and case law).

We and other industry stakeholders have demonstrated that we recognise the harm from scams and are willing to implement, and already have implemented, measures to protect consumers. We are already incentivised to act to protect the interests of our customers. In this regard, significant penalties would be inappropriate and unnecessary to deter industry from refraining to address and attempt to prevent scams.

[Ends - Annexure follows]

Annexure — how Google combats scams

Google takes a multi-faceted approach to protecting people from scams. Our approach to combating scams varies across our business, which includes Google Ads, Android, YouTube, Gmail, and Google Safe Browsing. We also invest in broader consumer awareness raising exercises such as supporting Scamwatch during Scam Awareness Week, promoting Google's Security Checkup[22] on the Google homepage in Australia, and working with consumer organisations such as ACCAN to heighten understanding of gift card scams.

Google Ads

One of our key focus areas is protecting people from scam ads. We detect scam ads through a combination of both AI and human evaluation, a process which helps ensure ads on our platform are adhering to the strict policies we have in place, including policies against misrepresentation and enabling dishonest behaviour.[23] In addition, we make it easy for people to report scam ads[24] if they see them.

We publish an annual Ads Safety report[25] that highlights the work we do to prevent malicious use of our ads platforms. To give an idea of the scale of our ads services, in 2022:

- we blocked and removed 5.2 billion bad ads and restricted access to a further 4.3 billion ads globally (restricting ads allows us to tailor our approach based on geography, local laws and our certification programs, so that certain ads only show where appropriate, including under local law)
- we also blocked or restricted ads from serving on over 1.5 billion publisher pages and took broader site-level enforcement action on over 143,000 publisher sites
- we suspended over 6.7 million ad accounts for policy violations.

In 2020, we announced an advertiser identity verification program[26] that will ultimately require all advertisers that want to run ads on our platforms to go through a verification program to confirm their identity. Advertisers have to submit personal identification, business incorporation documents or other information that proves who they are and the country in which they operate. This information is available for anyone to see in the Ads Transparency Center.[27]

---

[22] Google, Account, Security Checkup, https://myaccount.google.com/security-checkup?hl=en.
[23] Google, Advertising Policies Help, Enabling Dishonest Behaviour, https://support.google.com/adspolicy/answer/6016086?hl=en-AU&ref_topic=1626336.
[24] Google, Ads Help, Report an ad/listing, https://support.google.com/google-ads/contact/vio_other_aw_policy.
[25] 2022 Ads Safety Report, op. cit.
[26] Google, Ads & Commerce Blog, Increasing transparency through advertiser identity verification, https://blog.google/products/ads/advertiser-identity-verification-for-transparency/.
[27] Google, Ads Transparency Center, Ad transparency for a safe and open internet, https://adstransparency.google.com/.

We also expanded[28] our verification program[29] for financial services advertisers to Australia in June 2022. This requires financial services advertisers in Australia to demonstrate that they are authorised by ASIC,[30] and have completed Google's advertiser verification program, in order to promote their products and services through ads. This helps people to make more informed decisions before they click on any links.

Bad actors are always looking for ways to take advantage of people online. Increasingly, we've seen them use sophisticated deceptive techniques[31] to hide from our detection or promote non-existent virtual businesses, to lure unsuspecting consumers off our platforms with an aim to defraud them.

We're tackling this adversarial behaviour in a few key ways:

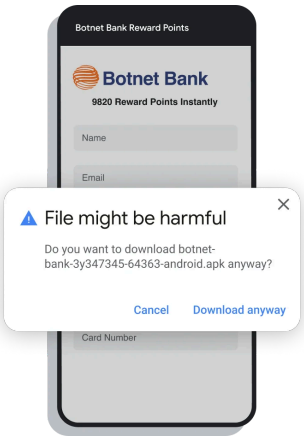
- The introduction of multiple new policies and programs including our advertiser identity verification program and business operations verification program.[32]
- Investments in technology to better detect coordinated adversarial behaviour, allowing us to connect the dots across accounts and suspend multiple bad actors at once.
- Improvements in our automated detection technology and human review processes based on network signals, previous account activity, behaviour patterns and user feedback.
- The use of automated and human evaluation to help ensure Google ads follow our ad policies.[33]
- Manual review of potentially bad ads reported to us here.[34]

[28] Google, Australia Blog, Australian Financial Services Advertisers Verification, https://blog.google/intl/en-au/australian-financial-services-advertisers-verification/.
[29] About Australian Financial Services Verification, op. cit.
[30] ASIC website, https://asic.gov.au/.
[31] Google, Advertising Policies Help, Abusing the ad network, https://support.google.com/adspolicy/answer/6020954?hl=en.
[32] Google, Advertising Policies Help, About verification, https://support.google.com/adspolicy/answer/9703665.
[33] Google, Advertising Policies Help, Advertising policies, https://support.google.com/adspolicy/topic/1626336?hl=en&ref_topic=2996750,1308156.
[34] Report an ad/listing, op. cit.

Android

Android incorporates multiple layers of protections, including:

- Phone by Google[35] which helps protect against voice phishing and scams with built-in caller ID, spam protection and Call Screen by blocking dangerous calls and warning you about suspicious callers
- Messages by Google[36] which uses AI to spot suspicious messages by assessing the reputation of the sender, looking for known patterns and dangerous links
- Chrome download warnings[37] that alert you if you're about to download an Android (APK) file, ensuring you're aware a link is about to trigger a download of an app.



YouTube

YouTube is a video platform where users can upload and share videos. YouTube has always had a set of Community Guidelines[38] that outline what type of content is not allowed on YouTube, designed to enable free and open exchange of ideas while keeping our community safe. Our Community Guidelines relevant for tackling scams include:

- Spam, scams, deceptive practices policy:[39] YouTube does not allow spam, scams, or other deceptive practices that take advantage of the YouTube community. We prohibit content offering cash gifts, "get rich quick" schemes, or pyramid schemes (sending money without a tangible product in a pyramid structure). We also don't allow content where the main purpose is to trick others into leaving YouTube for another site, including scam sites.
- Impersonation policy:[40] Under this policy, we do not allow content that is intended to impersonate a person or channel.
- Misinformation policy:[41] Certain types of misleading or deceptive content with serious risk of egregious harm are not allowed on YouTube. This includes content that has been technically manipulated or doctored in a way that misleads users (usually beyond clips taken out of context) and may pose a serious risk of egregious harm.

We take action to remove content that violates our policies as quickly as possible, using a combination of people and machine learning to detect and enforce on violative content at scale. Machine learning enables us to proactively identify and flag harmful content to our human

---

[35] Google Play, Phone by Google, https://play.google.com/store/apps/details?id=com.google.android.dialer.
[36] Google Play, Google Messages, https://play.google.com/store/apps/details?id=com.google.android.apps.messaging.
[37] Google, The Keyword, The 5 best ways to stay secure online with Chrome, https://blog.google/products/chrome/the-5-best-ways-to-stay-secure-online-with-chrome/.
[38] YouTube's Community Guidelines, op. cit.
[39] Google, YouTube Help, Spam, deceptive practices, & scams policies https://support.google.com/youtube/answer/2801973.
[40] Google, YouTube Help, Impersonation policy, https://support.google.com/youtube/answer/2801947.
[41] Google, YouTube Help, Misinformation policies, https://support.google.com/youtube/answer/10834785?hl=en.

reviewers, and automatically remove certain types of content very similar to what has been previously removed, such as spam. This allows us to take action on violative content often before it is widely viewed by users.

From July through September 2023, our Violative View Rate (VVR) was 0.10 - 0.11%, meaning that out of every 1,000 views on YouTube, only around 1 was of content that violated our Community Guidelines. During the same period, we removed 9.6 million channels and more than 362,000 videos for violating our spam, scams and deceptive practices policy; as well as more than 181,000 channels and more than 51,000 videos for violating our misinformation policy (including impersonation). More details are in the YouTube Community Guidelines enforcement report,[42] which is published every quarter.

Gmail

Spam, phishing, and malware continue to be serious threats to Gmail users. We have adapted to more sophisticated phishing campaigns, while also prioritising phishing protections that are most immediately threatening to users' data and credentials.

- Gmail blocks 99.9% of dangerous emails before they reach users every day (includes emails containing phishing links or harmful malware).
- 63% of the malicious documents we block in Gmail differ from day to day.
- 68% of the phishing emails blocked by Gmail today are new variations that were never seen before.

We've focused on developing security features that are deployed by default and that don't require people to be proactive in order to have a safe and secure web experience.

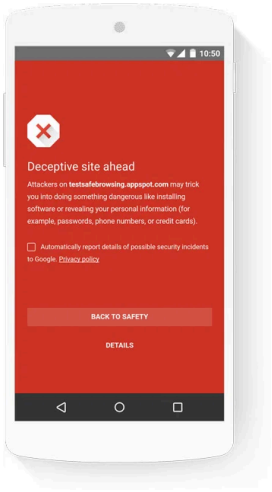
- For example, our Gmail malware scanner processes more than 300 billion attachments each week to block harmful content.
- Machine learning helps us with upwards of 95% of all spam and phishing identification in Gmail.
    - This is an area where more data enhances the protections we're able to offer to Internet users. Our improving technology in this area[43] thwarts many account hijacking efforts, including phishing campaigns, from ever reaching the inboxes of users.
    - In addition, Google's Threat Analysis Group, a dedicated team of security professionals, further detects, prevents, and mitigates government-backed threats.
    - Google continues to issue warnings to users[44] when we believe they may be the targets of government-backed phishing attacks. We have issued these warnings,

[42] YouTube Community Guidelines enforcement, op. cit.
[43] Google, The Keyword, Fighting phishing with smarter protections, https://www.blog.google/technology/safety-security/fighting-phishing-smarter-protections/, 18 October 2017.
[44] Google, Security Blog, A reminder about government-backed phishing, https://security.googleblog.com/2018/08/a-reminder-about-government-backed.html, 20 August 2018.

which include advice about ways to improve the security of users' Google accounts, since 2012.[45]

We've built new systems that detect suspicious email attachments and submit them for further inspection by Safe Browsing (see below). This protects all Gmail users, including enterprise Workspace customers, from malware that may be hidden in attachments.

Safe Browsing



Launched in 2005 as an anti-phishing plugin for the Firefox browser, today Google Safe Browsing[46] protects more than 5 billion devices across the world, and provides more protection in cases where a link may have looked legitimate.

Google Safe Browsing warns people if it looks like a site is dangerous and is attempting to phish their credentials. People can simply click on the "Go back to safety" option to avoid going to a malicious site or download a malicious file.

Google makes this technology freely available and it is deployed in multiple, competing browsers in addition to Chrome (e.g. Firefox, Safari) and across many different platforms, including iOS and Android.

[45] Google, Security Blog, Security warnings for suspected state-sponsored attacks, https://security.googleblog.com/2012/06/security-warnings-for-suspected-state.html, 5 June 2012.
[46] Google, Safe Browsing, Making the world's information safely accessible, https://safebrowsing.google.com/.