

**Submissions in response to Scams  
Prevention Framework — Exposure Draft  
Legislation**

**4 October 2024**

## Introduction

Google appreciates the opportunity to comment on the Scams Prevention Framework (**Framework**) Exposure Draft and accompanying Explanatory Materials (**EM**) in the Government's Scams Prevention Framework — Exposure Draft Legislation consultation.

According to the ACCC's "Targeting scams" report, people in Australia reported \$2.74 billion in losses in 2023.<sup>1</sup> This represents a 13% decrease on losses reported in 2022, but also an increase in total reports. While the top reported contact method used by scammers is still text messages (109,621 reports), the report finds that scammers also regularly make contact by email (85,941 reports) and telephone calls (55,418 reports), and to a lesser extent by social media (17,568 reports) and "the Internet" (17,568 reports). We agree that there is more work to do to protect Australians from scams.

### What Google is doing to combat scams

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 users' trust in our platforms.

Accordingly, we work hard every day to make our products safer. We are constantly improving our technology to stay ahead of threats and protect Australians online. In particular, Google invests significant resources to prevent scams across our products, including by stopping scam ads, blocking phishing emails, and warning people before they navigate to fraudulent websites.<sup>2</sup> Please see the [Annexure](#) for some examples of the work we do to combat scams.

Our approach is proactive — we do not wait for these issues to emerge before taking action. That's why, for example, after recognising a rise in attempted financial fraud in advertising, we expanded our financial services verification program in 2022 to Australia, to require advertisers of financial services to demonstrate they are authorised by ASIC.<sup>3</sup> This measure alone has added an important new layer of security against fraudsters to safeguard Australians from financial scams.

We also invest in broader consumer awareness raising exercises such as promoting Google's Security Checkup<sup>4</sup> on the Google homepage in Australia, posting practical tips on how to stay safe online on our Safety Centre,<sup>5</sup> and working with consumer organisations

---

<sup>1</sup> Australian Competition and Consumer Commission, [Targeting scams: report of the ACCC on scams activity](#) (28 April 2024).

<sup>2</sup> Google Australia, ['How we're stopping scams and working to create a safer internet'](#), *Google Australia Blog* (6 February 2024).

<sup>3</sup> Google, ['About Australian Financial Services Verification'](#), *Google Advertising Policies Help* (accessed 3 October 2024).

<sup>4</sup> Google, ['Security Checkup'](#), *Google account* (accessed 3 October 2024).

<sup>5</sup> Google, ['Google Safety Centre'](#) (accessed 3 October 2024).

such as ACCAN to heighten understanding of gift card scams. Over the past year, we've also worked closely with regulators, including the ACCC's National Anti Scams Centre (**NASC**), on initiatives to stop scams across Australia.

In July 2024, we also became a founding signatory of the Australian Online Scams Code (**AOSC**) launched by DIGI.<sup>6</sup> The AOSC is a proactive effort from the digital industry in line with the Government's wider legislative agenda on scams, and an important step in realising the Government's 2022 pre-election commitment for a social media scams code.

### The Framework

We welcome the Government's efforts to combat scams and are committed to working collaboratively with the Government to protect Australians online.

The proposed Framework is both novel and complex. It is important to get it right. We are concerned that the short consultation period (3 weeks from 13 September to 4 October 2024) is not sufficient to ensure the design of the Framework is fit for purpose and to ensure all relevant voices and experts in this field have been included, consulted and heard. Legislation of this nature, which will have potentially significant unintended consequences for Australian small businesses in particular, should entail a consultation period that gives stakeholders an opportunity to properly engage.

We urge the Government to extend this consultation or conduct further rounds of consultation. The Government should also bring forward as part of that consultation critical details, for example the exact services to be designated, designation instruments, and draft codes to be developed under the Framework (**SPF Codes**). It is difficult to meaningfully comment on the Framework with so much uncertainty as to the impacted services and the scope of proposed obligations.

Failing that, we submit that as far as possible the Framework should not prescribe obligations, but should establish the principles and processes by which the SPF Codes will be made. This would enable critical consultation to continue while SPF Codes are developed.

With these limitations, in this submission we have outlined our key concerns with the Framework:

1. [Unintended consequences: The impact of over removals, especially for SMBs](#)
2. [Scope: The Framework should not apply to services outside Australia](#)
3. [Global harmonisation: Harmonisation could promote consistency and efficiencies, and facilitate more effective efforts to tackle cross-border scams](#)

---

<sup>6</sup> Digi, '[Scams and Consumer Protection](#)' (Accessed 3 October 2024).

4. Privacy: Serious privacy risks from Framework obligations
5. EDR Scheme: Consumers' rights should be subject to consultation as part of the development of the SPF Codes
6. Lack of details: Difficult to engage on the Framework without details on the sector-specific codes
7. Competition: The Framework will distort competition and leave consumers exposed.

We look forward to engaging further with Treasury and the Government on the Framework and ultimately the SPF Codes.

# 1. Unintended consequences: The impact of over removals

The Framework as drafted will inevitably lead to regulated entities removing legitimate content, and suspending legitimate Australian businesses from their services, in order to manage their risk of liability. This consequence is a result of the combination of the:

- a. obligations to take action on information received from consumers (even though consumer reports can be inaccurate or even abusive, and often include only opaque assertions);
- b. obligation to take action once a regulated entity objectively has “reasonable grounds to suspect” that content *may* be a scam (even though they may not believe that the content is a scam);
- c. uncertainty inherent in any obligation to take “reasonable steps”, at least until an SPF Code is in place;
- d. short and rigid timeframes in which action is required to be taken; and
- e. ability for consumers to bring claims for breach of the Framework (rather than just for breach of an SPF Code) before an External Dispute Resolution (**EDR**) scheme or a Court, as well as the extreme maximum penalties applicable to contraventions of the Framework and SPF Codes.

## (a) The Fallibility of Consumer Reports

The Framework requires regulated entities to take reasonable steps to prevent a person from committing a scam relating to a regulated service of the entity.<sup>7</sup> Taking reasonable steps in this context will require “more than merely acting on actionable scam intelligence”,<sup>8</sup> suggesting a regulated entity must *at least* act on actionable scam intelligence that gives it reasonable grounds to suspect that content is a scam.<sup>9</sup>

Google’s products enable consumers to report content. More than a billion pieces of content are reported each year globally via Google’s legal removal reporting channel. In relation to Google Ads alone, we also separately receive millions of consumer reports each year of alleged contraventions of our policies, including those relating to scams.

Consumer reports are an important signal that our Trust & Safety teams use to assess whether to take action to remove particular content or to suspend particular accounts. We don’t, however, automatically remove content simply because a consumer has reported it. Not all reports are legitimate complaints. A significant proportion of reports are baseless, taste or preference related, confused, or worse — malicious and abusive and aimed at intentionally inflicting harm on a business, competitor, or individual. For example, one of the most-flagged videos on YouTube is a benign video by a popular music artist; not because there is anything wrong with the video, but rather because some people just don’t like it.

---

<sup>7</sup> [Treasury Laws Amendment Bill 2024: Scams Prevention Framework](#), (‘Bill’), s 58BJ.

<sup>8</sup> Bill, s 58BL.

<sup>9</sup> Bill, s 58AI.

This risk is particularly severe given the potential for bad actors to weaponise the Framework, particularly to harm Australian small and medium sized businesses. For instance, in 2023, 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.<sup>10</sup>

Under the proposed Framework, it would be straightforward for a business to target its competitors with illegitimate complaints, leading to the removal (even if only temporary) of the competitor's legitimate content. The removal of ads or account suspension for a small business, even for a short period of time, can have a significant impact on their revenue and operations.

It is common practice for businesses to engage firms to search the web for content that might infringe the business's rights, including potentially similar competitor brands. It is not uncommon for these firms to be financially compensated not for the accuracy of their reports, but rather according to the number of notices they submit, on the brand's behalf, to entities such as digital platforms. There is therefore an unhelpful financial incentive for certain actors in the ecosystem to over-report, which could lead to a significant number of reports of 'suspected scams' being inaccurate and potentially negatively affecting entirely legitimate businesses that advertise online.

It is for these reasons that Google does not rely solely on consumer content flags. In addition to our proactive work to combat scams, we invest heavily in our priority flagger program, which provides channels for participating trusted organisations to notify us of potentially harmful issues on certain of our products and services that violate our policies and community guidelines.<sup>11</sup> Partner entities will generally have access to:

- a dedicated intake channel used to inform us of potential policy violations which will be reviewed at priority; and
- ongoing discussions and feedback about Google and YouTube content policies.

Our priority flagger program is most suitable for organisations such as NGOs and government agencies with an identified expertise in recognising and fighting harm online.

In addition, we have previously proposed that the ACCC (or another regulator) be empowered to issue specific takedown notices in respect of scams, with appropriate safeguards.<sup>12</sup> This is a preferable approach because the ACCC (or another regulator) is independent and is better placed than a regular consumer to assess whether or not particular content is a scam. The ACCC, through the NASC in particular, has the capacity to collect intelligence, identify where action is needed, and direct removals as appropriate. Empowering the ACCC with additional takedown powers (with appropriate safeguards)

---

<sup>10</sup> Google, '[Taking legal action to protect users of AI and small businesses](#)', *The Keyword* (13 November 2023).

<sup>11</sup> Google, '[Partner Programs](#)', *Google Transparency Centre* (accessed 3 October 2024).

<sup>12</sup> Google, '[Google's Response to Government Consultation on ACCC Report on Platform Regulation](#)' (28 February 2023), pp 9, 38-43.

would be the most effective way to reduce the harm caused by scams without leading to the over-removal of content and unintended damage to Australian small businesses. We strongly recommend that the Government consider this as part of its approach.

### **(b) Suspicion as a threshold**

The fallibility of consumer reports would not be a concern if it were possible for a digital platform to review a piece of flagged content and know one way or the other whether the content was a scam. Unfortunately, that is not possible in most cases.

In many cases, no amount of investigation of the available facts would give certainty as to whether a piece of reported content is a scam. This is particularly true when, as is often the case, a particular digital platform is used as an initial (ostensibly legitimate) contact method, before a scam is completed off platform or indeed offline. Inevitably there will be some reported content which a digital platform does not think is a scam but about which the platform cannot be sure, even with extensive investigation.

Reasonable minds will differ as to when a regulated entity has “reasonable grounds to suspect” content is a scam. Consumers and regulators may take an expanded view without understanding the full context. Regulated entities will not have confidence about the approach regulators and Courts might take when assessing the question with the benefit of hindsight and visibility of the scam’s journey (which we do not have). To minimise potential liability (we discuss the impact of the proposed penalties and redress mechanism in [Part 1\(e\), below](#)), regulated entities could take a conservative approach that tends towards over removal, especially impacting small businesses with less digital proficiency.

Because reasonable minds can differ as to what is reasonable, the outcomes in different cases that turn on what is reasonable may be different. This will be a particular risk if there is an EDR scheme handling a high volume of consumer complaints and the administrator of the scheme has to assess all the evidence and determine what is reasonable in each circumstance, many times over. Regulated entities will need to take a lowest common denominator approach in order to treat their users consistently.

Further, the EM uses the expression “potential scam”. This would necessarily expand the amount of content about which a regulated entity is unsure, and would likely be inclined to remove. The question would no longer be whether the regulated entity believes that the content is part of a scam or not, but whether there are objectively reasonable grounds to suspect that the content is part of a scam or even a “potential scam”; which is a more uncertain threshold and too low a bar to be manageable.

It is also important to note that many regulated entities will be subject to international obligations which preclude them from taking enforcement action on the basis of “suspicion” alone (and in relation to which an Australian safe harbour will not assist). For example, in France, a competition authority injunction prevents Google from enforcing

against advertisers on the basis of suspicion alone.<sup>13</sup> Recital 51 of the EU Digital Services Act (DSA) also notes:

*Having regard to the need to take due account of the fundamental rights guaranteed under the Charter of all parties concerned, any action taken by a provider of hosting services pursuant to receiving a notice should be strictly targeted, in the sense that it should serve to remove or disable access to the specific items of information considered to constitute illegal content, without unduly affecting the freedom of expression and of information of recipients of the service.<sup>14</sup>*

Under the DSA, notices provided by consumers to a hosting service will only lead to an obligation to act to remove or disable access to content "where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination".<sup>15</sup> This standard allows regulated entities to apply a consistent standard without over removing.

We recommend consideration of appropriate language to ensure over removal does not significantly impact Australian small businesses and consumers.

### **(c) Reasonable steps**

We acknowledge the need for the Framework to outline high level principles that apply across very different industries and sub-industries. The proposal to outline in the SPF Codes what would be considered to be "reasonable steps" in connection with each of the SPF principles has considerable merit.

While industry waits for the SPF Codes to be developed, however, it faces considerable uncertainty as to what a Court will consider reasonable and whether regulated entities' internal thresholds and processes will satisfy the applicable requirements. Uncertainty equals risk, which when combined with the other factors referenced here will encourage regulated entities to take a more conservative approach to compliance, increasing the risk of over removal. For example, the Framework would require regulated entities to take reasonable steps to prevent scams. A regulated entity would likely take a conservative approach to this obligation: if a consumer nonetheless suffers scam losses an EDR scheme or Court is likely to take a critical view as to the reasonableness of the steps taken by regulated entities in the lead-up to those losses.

A preferred policy making approach would be to consider the Framework at the same time as draft designation instruments and draft SPF Codes. It is difficult to comment on the Framework without knowing exactly which services will be in scope and what will be prescribed as reasonable steps. We discuss this issue further in [Part 6, below](#).

---

<sup>13</sup> Autorite de la concurrence, '[Decision 19-D26 of 19 December 2019 regarding practices employed in the online search advertising sector](#)' (19 December 2019), p 130.

<sup>14</sup> See also [Regulation \(EU\) 2022/2065 \(Digital Services Act\)](#) ('DSA'), art 17.

<sup>15</sup> DSA, art 16(3).

Alternatively, to address this issue, the Framework should not prescribe obligations. Rather the Framework should establish the principles and processes by which the SPF Codes will be developed, and enable critical consultation to continue during this process. This is the model adopted in the UK's *Digital Markets, Competition and Consumer Act 2024*.

#### **(d) Timeframes**

The practical challenges outlined above are compounded in circumstances where the EM appears to foreshadow a regulated entity being required by the SPF Codes to take steps to investigate all reported scam advertisements within 48 hours and to remove reported scam content within 24 hours.<sup>16</sup> These timeframes are simply not workable at the scale at which Google operates and given the number of 'reports' that we receive, which require appropriate review and due process. As mentioned, in relation to Google Ads alone, Google receives millions of consumer reports each year of alleged contraventions of our policies, including those relating to scams.

Fixed timeframes inevitably lead to rushed decisions, which in the normal course will see regulated entities apply automatic decisions that over-index on removal (which as we discuss [below](#) will have a disproportionate impact on small businesses).

The norm here should ensure an appropriate balance between speed and accuracy of removal. Therefore, providers should remove content "with all due speed," "without undue delay," or "expeditiously." This is the approach taken in the EU's Copyright Directive, for instance, which stipulates at Article 14 that: "*(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.*"

#### **(e) Liability**

Ordinarily, while each of the factors above would be problematic, a regulated entity might be comfortable taking what it considers to be a reasonable approach to compliance on the basis that a regulator or Court is likely also to have a commensurate view of what is reasonable.

The Framework, however, contemplates that consumers will be able to bring Court proceedings against regulated entities for allegedly contravening the Framework's requirements that regulated entities take reasonable steps. Consumers could also approach an EDR scheme with claims for compensation based on alleged contraventions of the high-level and often ambiguous obligations in the Framework.

In the absence of SPF Codes, there will necessarily be uncertainty about how Courts and the EDR scheme operator will apply the Framework's obligations. In establishing their approach to compliance, regulated entities will need to address the possibility not only of legitimate claims, but also of illegitimate or at least ambitious claims. As currently drafted, it

---

<sup>16</sup> [Treasury Laws Amendment Bill 2024: Scams Prevention Framework Exposure Draft Explanatory Materials](#) ('EM'), p 50.

is inevitable that consumers will bring large volumes of claims under the Framework and SPF Codes that, while ultimately not successful, will impose considerable burden not only on regulated entities but also Courts and the EDR scheme.

At the same time, regulated entities also face penalties up to 30% of turnover. As global businesses, this kind of penalty would expose digital platforms to disproportionate and commercially unreasonable risks from their Australian operations.

Knowing this, regulated entities will be likely to take a conservative approach to compliance processes, further raising the risk of over removal.

### **Impact on small businesses**

In sum, if a regulated entity is:

- a. required to take action on consumer reports (notwithstanding their limitations);
- b. required to take action at an uncertain standard of “suspicion” that content is a scam or a potential scam;
- c. operating with uncertainty about what is meant by “reasonable steps”;
- d. required to take action within a short and rigid time frame; and
- e. faced with a likely high volume of consumer claims, many of which may lack merits, as well as significant penalties commensurate with those applied for cartel conduct,

it is inevitable that the entity will face strong incentives to remove considerably more content and to suspend more advertising accounts than it otherwise would.

No doubt the drafters intend for regulated entities to take a cautious approach to scams, however the potential unintended consequences of the Framework as drafted are significant. While regulated entities can draw some comfort from the proposed safe harbour from claims by entities that will be adversely affected by these over-removals,<sup>17</sup> small businesses could still be severely impacted. This is because small businesses are often the hardest to verify, operate small accounts that do not have dedicated account management, and will not have a long-established trading relationship with the digital platforms that help to serve their digital advertising needs. As a result, strict precautionary measures and enforcement mechanisms necessitated by the requirements of the Framework will unavoidably hit small businesses and Australian start ups the hardest.

It’s critical that the Government considers the potential adverse impact of the Framework on Australian small businesses and startups to ensure these impacts have been properly considered and minimised. With respect to our services, for example, Google Search Ads are a powerful tool for Australian small business advertisers to reach national and global

---

<sup>17</sup> Bill, s 58BZ

audiences they otherwise could not reach.<sup>18</sup> Many Australian YouTube creators are small businesses. Small businesses often do not have the web presence, digital proficiency, or other trust signals that might allow our Trust & Safety teams to form a confident view that their content is not in any way associated with a scam. We are deeply concerned about the impact the proposed Framework would have on Australian creators and small businesses if not carefully crafted and balanced.

In our view, the Government could drive effective improvements in regulated entities' efforts to combat scams without leading to the over removal of content including by making the following recommended changes to the proposed Framework.

**Recommendations:**

- The Framework should not itself prescribe obligations. Rather, the Framework should establish the principles and processes by which the SPF Codes will be made. This would enable critical consultation to continue while SPF Codes are developed.
- Introduce a takedown power for the ACCC (with appropriate safeguards). The ACCC, through the NASC in particular, has the capacity to collect intel, identify where action is needed, and direct removals as appropriate. Empowering the ACCC with additional takedown powers (with appropriate safeguards) would be the most effective way to reduce the harm caused by scams without leading to the over-removal of content and damage to Australian small businesses.
- Delete section 58BL(1) and address the question of what is reasonable in the SPF Codes, as contemplated by section 58BL(2). The SPF Codes can provide more detail about the context in which a consumer report should require action, depending on the type of service to which it relates.
- Replace the requirement for action based on “reasonable grounds to suspect” with action once the regulated entity reasonably believes that the reported content is a scam. Alternatively, Australia could adopt the standard set out in the DSA, which requires action where a report allows a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination.
- The Framework should not be considered by Parliament until draft designation instruments and draft SPF codes are prepared. Failing that, the Framework should stipulate (a) a minimum transition period of 2 years after both a designation instrument and an SPF Code are in place before the Framework will apply (we explain further in [Part 6, below](#), why a transition period is required); and (b) that compliance with an SPF Code will satisfy the commensurate obligation under the Framework.
- Replace any suggestion in the EM of a fixed turnaround time with a reference to

---

<sup>18</sup> Access Partnership, [Economic Impact Report: Turning Australia's AI opportunities into impact with Google](#), (June 2024), p 18.

In 2023, Australian SMBs gained \$30.6 billion of economic activity through their use of Google Search, Google Ads, Google AdSense, Google Play, Google Cloud, and Ad Grants.

“expeditious” or “promptly” or similar. We note that the EU E-Commerce Directive (**eCD**), DSA and UK Online Safety Act (**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.

- If consumers are to bring Court or EDR scheme claims against regulated entities, they should be for alleged contraventions of the SPF Codes, not the Framework. (We discuss the EDR Scheme further in [Part 5, below.](#))
- Penalties for non-compliance with the SPF Codes should be commensurate with those in other industry codes, as submitted in our [February 2024 submission](#) to Treasury on mandatory industry codes.
- The proposed remedial directions power in section 58FZB is excessively broad. It should not apply where a regulator suspects that a regulated entity “will fail to comply”, and must include safeguards, including (a) a formal investigation of the suspected failure to comply; (b) the direction must be reasonable and proportionate, (c) the direction must be workable and practical in the context of global compliance efforts; (d) the direction must achieve the purpose and objectives of the Framework / obligation; and (e) the regulated entity must have an opportunity to present alternative steps that comply with the obligation and the ACCC must be expressly required to consider the regulated entity’s alternative proposal.

## 2. Framework should not apply to services outside Australia

It is unclear whether the Framework is intended to apply to services supplied outside of Australia. As presently drafted, the Framework would appear to have that effect. The definition of “SPF consumer” includes a natural person who is either in Australia, ordinarily resident in Australia, an Australian citizen or permanent resident, or a small business with a principal place of business in Australia. It applies whether or not the regulated business knows that the person is an individual or small business connected with Australia.

If the concept of an SPF consumer is intended to capture for example an Australian citizen or permanent resident who views a Search Ad while they are located outside Australia, the Framework would appear to be seeking to influence services offered in jurisdictions outside Australia. In many cases, digital platforms will not be able to identify a given user of their services. Even if a consumer is signed in, we have no way of knowing whether they are an Australian citizen or permanent resident, but happen to be in another jurisdiction at the time (for example, viewing a Search Ad on the UK or US version of the Google Search service). We do not typically collect sensitive information about our users such as their residency or citizenship status and would consider it contrary to privacy best practices to do so unless necessary. (We outline in [Part 4, below](#), our other privacy related concerns with the Framework.)

Identifying an SPF consumer 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, which the consumer carries with them regardless of where they are located. By contrast, many users of digital platform services like a search engine will use the service without being logged into their account, in which case we use their IP address (generally determined dynamically by the internet connection they are using at the time) and other location based signals to assess their location.

As drafted, the Framework would potentially have implications for our operations beyond Australia — we might need to treat every user globally as a potential SPF consumer. This would be inconsistent with international norms and impose an unworkable burden on our business, particularly given that the Framework would impose obligations inconsistent with other countries’ laws. For example, as discussed in [Part 1\(b\). above](#), in Europe we are currently prevented from removing advertiser content based on suspicion alone, and under the DSA, we are required to take action that is “*strictly targeted... without unduly affecting the freedom of expression and of information of recipients of the service.*”

**Recommendation:** Amend the Framework and SPF Codes to make it clear that they only apply to digital services supplied in Australia, including ads shown in Australia, and do not capture digital services supplied outside Australia and ads shown outside Australia, even if those services or ads are accessed by an Australian resident or citizen who happens to be in another country at the time.

### **3. Global harmonisation: Harmonisation could promote consistency and efficiencies, and facilitate more effective efforts to tackle cross-border scams**

To the extent the Framework applies to digital platforms operating globally, there would be a significant advantage in harmonising the Framework's obligations with similar regulations globally. This opportunity arises in two areas in particular:

- a. harmonisation of compliance processes, to enable global businesses to dedicate resources to combating scams rather than building country-by-country compliance processes, while also facilitating product roll outs to Australia that might otherwise be held up by additional compliance requirements; and
- b. intelligence sharing, to enable global businesses to share global information with Australian regulators and businesses using global processes and taking advantage of global information sharing networks.

#### **(a) Harmonisation of compliance processes**

In order to comply with the highly prescriptive overarching principles in Division 2 of the Framework, regulated entities would need to develop a bespoke compliance system and processes for their regulated services specific to Australia. This Part of the submission considers two of the SPF principles by way of example.

##### Principle 1: Reporting and record keeping

SPF principle 1 relates to a regulated entity's obligations to have governance arrangements in place in relation to scams. We agree that regulated entities should have effective governance policies, procedures, metrics, and targets in place to combat scams (i.e., an 'anti-scam strategy') and that this should be formally documented. It is also appropriate for the regulator to be able to request copies of a regulated entity's anti-scam strategy and other documents related to its compliance with the SPF provisions (subject to strict and explicit confidentiality obligations). However, record keeping and reporting obligations should be reasonable and proportionate, taking into account the nature and scale of our and other digital platforms' global businesses.

We already publish regular transparency reports outlining our efforts to combat scams — for example, our Ads Safety Report<sup>19</sup> and our YouTube Community Guidelines Enforcement Report.<sup>20</sup> Similarly, we share regular updates on our efforts on our blog, with examples including posts on *How to spot scams, and what to do if you encounter one*,<sup>21</sup> *How we*

---

<sup>19</sup> Google, '[Our 2023 Ads Safety Report](#)', *Ads and Commerce Blog*, (27 March 2024).

<sup>20</sup> YouTube, '[How does YouTube enforce its Community Guidelines](#)', *Youtube community guidelines* (accessed 3 October 2024).

<sup>21</sup> Google, '[How to spot scams and what to do when you encounter one](#)', *The Keyword* (2 October 2024).

*fought bad apps and bad actors*<sup>22</sup> and *How we fought Search spam*.<sup>23</sup>

In our view, the reporting and record keeping obligations in the Framework should be less prescriptive. More detail should be provided in the SPF Codes. Accommodation should be given to global businesses to allow them to apply a globally consistent approach to combating scams without having comparable but different processes in each jurisdiction in which they operate.

Further, the obligation to provide reports to a regulator within five days will be nearly impossible to comply with. The period should be no shorter than 28 days, consistent with other record keeping rules administered by the ACCC (for example the Telstra Customer Access Network Record Keeping Rules).<sup>24</sup>

The Framework (and SPF Codes) should not be prescriptive about which senior officer or 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 CEO or board in the ordinary course, it would be disproportionate to require their sign-off on the proposed prescriptive requirements for an anti-scam strategy or strategies, particularly on an annual basis. Such a requirement could also discourage agile evolution of strategies to meet emerging threats and leverage developments in technology and capability.

Highly prescriptive rules that expose regulated entities to potentially significant liability (and impose burdensome requirements that are costly to implement) can have enduring impacts on innovation in the Australian market. The Framework would raise regulatory barriers to the launch of new features, products, and services in Australia by regulated entities and potential new entrants.

Prescriptive requirements, such as those contemplated in the Framework, also risk consuming critical scam-fighting resources with compliance work. These resources could be better directed toward innovation projects designed to fight scams.

## Principle 2: Prevention

SPF principle 2 requires regulated entities to take reasonable steps to identify the “classes of SPF consumers” who have a higher risk of being targeted by a scam relating to the regulated service, and to provide warnings to each consumer belonging to such a class. Google is uncertain about how to seek to comply with this obligation. First, it is unclear to Google how to identify the relevant classes, and what type of classes the legislation envisages (e.g., what kinds of characteristics should be used to class SPF consumers as

---

<sup>22</sup> Google, ‘[How we fought bad apps and bad actors in 2022](#)’, *Google security blog* (27 April 2023).

<sup>23</sup> Google, ‘[How we fought Search spam on Google Search in 2022](#)’, *Google search central* (11 April 2023).

<sup>24</sup> ACCC, *Telstra Customer Access Network Record Keeping and Reporting Rules* (21 December 2022) <https://www.accc.gov.au/system/files/Telstra%20CAN%20RKR.pdf>

higher risk). Second, if an SPF consumer includes a user of Google Search or YouTube who is not signed into their account, Google does not have identity information about that consumer. Even for consumers that are signed in, Google may have little or incorrect information about their particular characteristics, and, therefore, face extreme difficulty in determining whether they are at higher risk of being targeted by a scam.

**Recommendations:**

- The Framework should not itself prescribe obligations. Rather, the Framework should establish the principles and processes by which the SPF Codes will be made. This would enable critical consultation to continue while facilitating the development of detailed reporting and record keeping requirements in the SPF Codes.
- Amend the Framework to:
  - clearly identify the circumstances in which the regulator can request copies of SPF compliance records (for example, if there is a reasonable suspicion of non-compliance);
  - extend the time within which a regulated entity must comply with a request under section 58BH to be no shorter than 28 days; and
  - be less prescriptive about the executive sign-offs required for compliance purposes.
- Remove the section 58BK(2) obligation to identify and warn high risk classes of SPF consumers.

**(b) Advantages of global intel sharing networks**

SPF principle 4 requires regulated entities to provide the regulator reports of any actionable scam intelligence the entity has about suspected scams.<sup>25</sup> Based on the notes in section 58AI of the draft Framework and the EM, it appears that a single consumer report could be sufficient to constitute “actionable scam intelligence”, provided the report contains enough information to raise a reasonable suspicion of scam activity.

As noted above, Google receives millions of content removal requests daily across our products, some of which are reported scams. If ‘actionable scam intelligence’ is intended to capture single consumer reports about a potential scam, the obligations in sections 58BR, 58BS, 58BT and 58BU of the Framework would seem to require a regulated entity to provide almost every consumer report of a scam to the regulator. This could lead to millions of reports being submitted to the ACCC. Not only will an inundation of reported scams overwhelm the ACCC (and put pressure on its resources), but it will also impose a significant burden on regulated entities (and their resources).

---

<sup>25</sup> Bill, s 58AI; EM p 23.

We and other other stakeholders will likely face the following potential impediments and challenges in complying with the reporting obligations in sections 58BR, 58BS, 58BT and 58BU:

- We would be required to update our current reporting tools so that they ask users for the specific information required by the regulator, which according to Note 2 under section 58BS could include demographic information about the impacted SPF consumer, the details of the method of contact used by the scam, the form of loss or harm caused by the scam, and so forth. (We address in [Part 4, below](#), our key privacy concerns with the Framework.)
- As the Business Council of Australia has noted, regulated entities would shift resources away from directly preventing and disrupting scams to building the highly prescriptive compliance processes required by the Framework.
- Even if we deployed additional resources to compliance, the sheer volume of reports, and investigation of potential reports received by other regulated entities, with likely less or no relevance to our services, would overwhelm our systems and undermine the efficiency and effectiveness of current processes to focus our attention on strong scam signals.

Appropriate and effective reporting requirements should be developed after more extensive consultation with regulated entities through the mandatory code development processes, and can be reflected in subordinate legislation relating to the mandatory codes. Such consultation should, among other things, enable service providers to reconcile their competing obligations under privacy laws in Australia and, if applicable, abroad.

A uniform approach between jurisdictions in these areas would promote optimal consistency and efficiencies, and facilitate more effective efforts to tackle cross-border scams. 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.<sup>26</sup> 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.

It will also be important for Australia to regulate this space in a way that does not impede or duplicate broader global efforts. The Global Anti-Scam Alliance (GASA) and the DNS Research Federation have been developing a Global Signal Exchange (GSE) as a platform that will serve as a global clearinghouse for online scams and fraud bad actor signals. The exchange will allow ecosystem players to share real-time information and data on scams. The exchange will enable scam signal sharing across industries, allowing sectors from

---

<sup>26</sup> OECD, '[Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders](#)', 2023.

banks, to telecommunication services, to digital platforms and law enforcement to detect and take down scams faster. The Framework should be flexible enough to enable regulated entities to meet their reporting obligations through participation in such global exchanges. We are keen to work with the Australian Government on implementing this initiative in Australia. We believe this would be an effective and efficient way to enable information exchange between the NASC and regulated entities under the Framework.

**Recommendations:**

- The Framework should harmonise with global approaches and scam signal exchanges. Consistency with other proposals being pursued internationally (for example by the EU, Singapore and the UK) will ensure Australia is following best global practice. The Framework should not require regulated entities to create burdensome reporting processes that duplicate or impede other processes.
- At a minimum, Australia should ensure that the Framework does not create compliance obligations that jeopardise a platform's ability to comply with other regulations, such as the DSA or competition laws.

## 4. Privacy: Serious privacy risks from Framework obligations

In addition to the issues raised elsewhere in this submission, two aspects of the Framework would have particularly serious privacy implications:

- a. regulated entities could be required to share the personal information of reporters (potentially from anywhere in the world); and
- b. regulated entities would be required to notify consumers each time it is discovered that they could have in the past interacted with scam content.

Ultimately, requiring regulated entities to collect additional personal information from users is inconsistent with Government reforms in other areas.

### (a) Reporters' PII

The proposed reporting obligations would involve sharing a vast amount of user and non-user information (including personal information) with the regulator. For example, the Framework envisages regulated entities being required to share the personal information of:

- a. a person reasonably suspected of committing a scam, or being knowingly involved in the commission of a scam;
- b. an SPF consumer who was engaged (or was attempted to be engaged) as part of a scam;
- c. a person who reports a scam on behalf of an SPF consumer; and
- d. a person who a scam deceptively impersonates in connection with a regulated service.<sup>27</sup>

Given the global nature of digital platforms' businesses, much of the above information would involve sharing personal information that is subject to protections by overseas laws. In these circumstances, the mere fact that the production of the information is compelled by Australian law is unlikely to be a sufficient justification under those overseas laws. It will create a serious conflict of laws situation for any Australian companies that have a presence overseas. In particular, US companies are subject to various US laws that impose non-disclosure obligations. Similarly, section 58BT is unlikely to assist regulated entities dealing with claims by individuals overseas.

The risk might to an extent be mitigated if the obligation to share information were limited to information in relation to individuals in Australia and without any overseas connections. (See also in [Part 3, above](#), our concerns about overly burdensome information sharing obligations in general.)

---

<sup>27</sup> Bill, s 58BS(3).

## **(b) Notifying impacted consumers**

The Framework proposes to require regulated entities to take reasonable steps:

- to identify SPF consumers of the regulated service who have been impacted by a scam;<sup>28</sup>
- to identify each SPF consumer of that service who is or could be impacted by the suspected scam;<sup>29</sup> and
- to disclose to SPF consumers sufficient information to enable those consumers to act in relation to the suspected scam.<sup>30</sup>

Obligations to warn users are 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. A bank and a telecommunications provider will, in the ordinary course, have detailed information about its customers (including their name, address, and contact details). Meanwhile:

- For valid privacy reasons, consumers often use digital platforms with settings that would make it impossible to contact them 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. Often a device or account log-in will be used by multiple individuals, making warnings potentially confusing.

In the digital platform context, at the scale at which we operate, a blanket requirement to provide further warnings is likely to lead to over-warning and warning fatigue, with limited real impact for consumers. Furthermore, it is likely to require regulated entities to collect more personal information than necessary, and possibly retain it for longer than they normally would for business purposes, just in case they need to fulfil this obligation. In other words, this trade-off could weaken privacy protections while offering dubious benefits in scam prevention.

### **Recommendations:**

- Reporting, disclosure, and warning obligations should be dealt with in SPF Codes, rather than the Framework, to account for the different nature of services and their relationship with reporters, consumers, and customers.
- Remove the reporting obligation in section 58BX to avoid duplicative and unworkable obligations.

---

<sup>28</sup> Bill, s 58BN(3).

<sup>29</sup> Bill, s 58BO(1).

<sup>30</sup> Bill, s 58BX(1).

## 5. EDR Scheme: Consumers' rights should be subject to consultation as part of the development of the SPF Codes

The Framework envisages consumers being able to enforce its obligations to take reasonable steps in a Court<sup>31</sup> and through an EDR scheme.<sup>32</sup> We are concerned that the inevitable ambiguity associated with the high level obligations in the Framework will lead to a high volume of ultimately unsuccessful consumer claims, which will impose significant burden on Courts, the EDR scheme, and regulated entities, and ultimately will not serve consumers' interests. In our view, if consumers are to be entitled to bring claims at all, those claims should be limited to relatively clear obligations in the SPF Codes.

For example, regulated services could be exposed to a large number of claims about whether they complied with obligations to “have appropriate strategies for preventing, detecting, reporting, disrupting and responding to scams”, “develop and implement governance policies, procedures, metrics and targets for combatting scams” and so on. It is not clear whether the Government intends this, but inclusion of such obligations would lead to a fragmented and inconsistent enforcement practice which engenders further uncertainty on the interpretation of the obligations.

We query whether an EDR scheme has the necessary resources and expertise across the regulated sectors to make the determinations contemplated in the legislation, particularly if large numbers of claims are brought forward. Currently, the AFCA adjudicates complaints brought by consumers and small businesses about various financial services arising from a customer relationship with the relevant financial services entity. The Framework, however, envisages a process whereby the AFCA would hear extensive evidence about regulated entities' (including in the telecommunications and digital platform industries) efforts to prevent, detect, and disrupt scams, assess whether those efforts were reasonable, and then somehow apportion liability between however many services were used by the bad actor behind the scam in each case (as well as the individual themselves). These kinds of issues are usually the purview of a Judge.

Disputes under the Framework in relation to whether a platform has taken “reasonable steps” would likely also require the disclosure of commercially sensitive information about platforms' internal strategies and systems and how these are designed to combat scams in the course of discovery processes. It would be extremely concerning and counterproductive to our efforts to combat scams if this type of information was made public through the EDR scheme (intentionally or unintentionally), as it could find its way into the hands of the bad actors that are actually perpetrating the scams. This sort of information could be more safely shared with regulators and Courts (subject to confidentiality obligations), but it would be deeply concerning if regulated entities needed

---

<sup>31</sup> Bill, s 58FZE.

<sup>32</sup> Bill, s 58DB.

to make substantial disclosures of sensitive information to individual claimants and through the EDR scheme.

We understand that Treasury initially recommended 'a mechanism to determine redress and reimbursement of funds for breaches by a bank':

*An external dispute resolution (EDR) mechanism (such as through AFCA) to determine redress and reimbursement of funds to a consumer where a bank has breached its obligations under the sector-specific code.*

*Developing and implementing a multi-sector EDR scheme would be complex and time consuming, and would be a future consideration.*

*Clear obligations on businesses and strong penalties in the Framework will provide incentives for businesses to reduce scam losses, and the need for a multi-sector EDR scheme would be considered at a later stage.<sup>33</sup>*

Google agrees with the above assessment from Treasury. If the Government wishes to provide consumers with timely redress and reimbursements, then a simple EDR scheme for financial services would make sense. Should the Government insist on including a multi-sector EDR scheme Framework, it should be first explored in detailed consultations.<sup>34</sup>

**Recommendations:**

- If the Government intends for individuals to be able to bring claims for redress, those claims should be limited to breaches of specific obligations in the SPF Codes, not the overarching principles in the Framework. 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 / EDR schemes, proportionality, and the extreme sensitivity of confidential information about how businesses combat scams.
- The Government should consider whether an EDR scheme has the necessary resources and expertise (across the regulated sectors) to make the determinations contemplated in the Framework, particularly if large numbers of claims are brought (as is likely to be the case).

<sup>33</sup> Department of Treasury, '[FOI 3675 - Scams](#)', (2 October 2023) (FOI).

<sup>34</sup> FOI, p 123.

## 6. Lack of details: Difficult to engage on the Framework without details on the sector-specific codes

To achieve its goal of protecting Australians against scams, the Framework relies on the overarching principles in Division 2 together with the creation of sector-specific codes that apply to regulated sectors in Division 3. The two components of the Framework are interrelated and together will create the regulatory framework that will govern regulated entities. Whilst there is an indication of the parameters within which sector-specific codes must be developed (section 58CC), it is difficult for a platform to fully engage on the impact of the regulatory framework without (a) clarity on which services will be designated and (b) more detail on what will be in the sector-specific codes for online platform services. For example we cannot:

- provide an accurate estimate of the costs of compliance with the Framework without understanding what obligations will be contained in the sector-specific codes (including specificity regarding the reasonable steps required to comply with the obligations to prevent, detect, and disrupt scams); and
- take steps to develop a compliance plan before the legislation or codes apply to Google. There is no mandatory transition period and the EM states that regulated entities may be subject to the Framework upon designation. Based on Google's past experience internationally, we expect it would take approximately 24 months to develop and be ready to implement a compliance program of the magnitude contemplated in the Framework.

### **Recommendations:**

- The Government should release exposure drafts of the sector-specific codes including outlining the reasonable steps required to be taken by the different categories of regulated entities. These can be subject to further consultation after the enactment of the primary legislation.
- Include a mandatory transition period of at least 24 months.

## 7. Competition: The Framework will distort competition and leave consumers exposed

We understand the Minister proposes to designate:

- a. banks
- b. telecommunications and
- c. digital platform service providers – beginning with:
  - i. social media
  - ii. paid search engine advertising
  - iii. direct messaging services.<sup>35</sup>

We understand from the example on page 46 of the EM that the Minister intends to include, within the proposed designation of “social media”, ads on a social media service.

It is not clear whether this also extends to broader elements of the social media service like marketplaces. Clarification of the intended scope of “social media” would be helpful and provide consumers and service providers with guidance.

We are concerned about the proposal to designate paid search engine advertising, and not other online paid advertising services.

Scammers are agile and resourceful. In our experience, combating scams is a constant cat-and-mouse game. If only certain platforms are regulated, bad actors will migrate to unregulated platforms. If search engine advertising is a regulated service under the Framework, but other online paid advertising is not, scammers are likely to migrate to unregulated providers of online paid advertising, including specialised search services (such as Amazon, Yelp, booking.com etc). Australians may be led into a false sense of security about the protections they have when interacting with those digital platforms. Australians should benefit from robust consumer protections consistently across the online paid advertising ecosystem, not just one part of it. If the intent is to protect consumers, serious consideration should be given to whether the proposed approach of limiting obligations to search engine advertising achieves that objective.

The Framework should, therefore, avoid narrowly targeting general search engine advertising services. Rather, it should be expanded to include all online paid advertising services, including advertising on specialised search services that similarly display advertising on their results pages.

Otherwise, the Framework would leave a significant protection gap for Australian consumers and likely see bad actors focus on products that aren't in scope.

We are also concerned that the designation of only paid search engine advertising will impose a significant compliance burden on Google Search Ads, including significant costs,

---

<sup>35</sup> EM, p 6.

which will not also be borne by other ads services with which it competes and which are also susceptible to scammers. This is in circumstances where Google Search Ads already provide best in class protections against scams.

Imposing requirements only on certain firms would interfere with the competitive process, by limiting the activities (and raising the costs) of those firms subject to regulation relative to their competitors. This would put firms subject to regulation at an undue competitive disadvantage and be contrary to the objectives of promoting competition on the merits and fair trading.

**Recommendations:**

- Online paid advertising: If the Minister intends to designate paid advertising services on general search engines, the Minister should also designate paid advertising services on specialised search services, and other online paid advertising services, which are also susceptible to scammers.
- Large and small players that provide the same service should be covered: If the Government identifies a type of digital platform service as requiring designation, 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.

## 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<sup>36</sup> 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.<sup>37</sup> In addition, we make it easy for people to report scam ads<sup>38</sup> if they see them.

We publish an annual Ads Safety report<sup>39</sup> 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 2023:

- we blocked and removed 5.5 billion bad ads
- we also blocked or restricted ads from serving on over 2.1 billion publisher pages and took broader site-level enforcement action on over 143,000 publisher sites
- we suspended over 12.7 million ad accounts for policy violations.

In 2020, we announced an advertiser identity verification program<sup>40</sup> 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 directly viewable for every individual ad in My Ads Center and available for anyone to see in the searchable Ads Transparency Center database.<sup>41</sup>

We also expanded<sup>42</sup> our verification program<sup>43</sup> for financial services advertisers to Australia in June 2022. This requires financial services advertisers in Australia to demonstrate that

---

<sup>36</sup> Google, '[Security Checkup](#)', *Google account* (accessed 3 October 2024).

<sup>37</sup> Google, '[Enabling Dishonest Behaviour](#)', *Advertising Policies Help* (Accessed 3 October 2024).

<sup>38</sup> Google, '[Report an ad/listing](#)', *Ads Help* (accessed 3 October 2024).

<sup>39</sup> Google, '[2023 Ads Safety Report](#)', *Ads & Commerce Blog* (27 March 2024).

<sup>40</sup> Google, '[Increasing transparency through advertiser identity verification](#)', *Ads & Commerce Blog* (23 April 2020).

<sup>41</sup> Google, '[Ad transparency for a safe and open internet](#)', *Ads Transparency Center* (Accessed 3 October 2024).

<sup>42</sup> Google, '[Australian Financial Services Advertisers Verification](#)', *Australia Blog* (9 June 2022).

<sup>43</sup> Google, '[About Australian Financial Services Verification](#)', *Advertising Policies Help* (accessed 3 October 2024).

they are authorised by ASIC,<sup>44</sup> 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<sup>45</sup> 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.<sup>46</sup>
- 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.<sup>47</sup>
- Manual review of potentially bad ads reported to us here.<sup>48</sup>



<sup>44</sup> Google, '[About Australian Financial Services Verification](#)', *Advertising Policies Help* (accessed 3 October 2024).

<sup>45</sup> Google, '[Abusing the ad network](#)', *Advertising Policies Help* (accessed 3 October 2024).

<sup>46</sup> Google, '[About verification](#)', *Advertising Policies Help*, (accessed 3 October 2024).

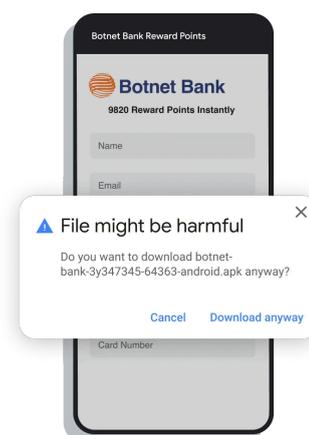
<sup>47</sup> Google, '[Advertising policies](#)', *Advertising Policies Help*, (accessed 3 October 2024).

<sup>48</sup> Google, '[Report an ad/listing](#)', *Ads Help* (accessed 3 October 2024).

## Android

Android incorporates multiple layers of protections, including:

- Phone by Google<sup>49</sup> 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<sup>50</sup> which uses AI to spot suspicious messages by assessing the reputation of the sender, looking for known patterns and dangerous links
- Chrome download warnings<sup>51</sup> 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<sup>52</sup> 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:<sup>53</sup> 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:<sup>54</sup> Under this policy, we do not allow content that is intended to impersonate a person or channel.
- Misinformation policy:<sup>55</sup> 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.
- External links policy: Links that send users to content that violates our Community Guidelines are not allowed on YouTube. This includes links to websites or apps phishing for a user's sign in or financial information.<sup>56</sup>

<sup>49</sup> Google Play, '[Phone by Google](#)' (accessed 3 October 2024).

<sup>50</sup> Google Play, '[Google Messages](#)' (accessed 3 October 2024).

<sup>51</sup> Google, '[The 5 best ways to stay secure online with Chrome](#)', *The Keyword* (25 October 2022).

<sup>52</sup> YouTube, '[YouTube's Community Guidelines](#)' (accessed 3 October 2024).

<sup>53</sup> Google, '[Spam, deceptive practices, & scams policies](#)', *YouTube Help* (2 May 2019).

<sup>54</sup> Google, '[Impersonation policy](#)', *YouTube Help* (accessed 3 October 2024).

<sup>55</sup> Google, '[Misinformation policies](#)', *YouTube Help* (accessed 3 October 2024).

<sup>56</sup> Google, '[External links policy](#)', *YouTube Help* (accessed 3 October 2024).

- Fake engagement policy: YouTube doesn't allow anything that artificially increases the number of views, likes, comments or other metrics either by using automated systems or serving up videos to unsuspecting viewers.<sup>57</sup>

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 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 April to June 2024, our Violative View Rate (VVR) was 0.09 - 0.11%, meaning that for every 10,000 views on YouTube, 9 - 10 of those are of content that violated our Community Guidelines. During the same period, we removed 2.6 million channels, more than 108,000 videos and more than 1.1 billion comments for violating our spam, scams and deceptive practices policy; as well as more than 148,000 channels and more than 104,000 videos for violating our misinformation policy. More details are in the YouTube Community Guidelines enforcement report,<sup>58</sup> 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<sup>59</sup> thwarts many account hijacking efforts, including phishing campaigns, from ever reaching the inboxes of users.

---

<sup>57</sup> Google, '[Fake engagement policy](#)', *YouTube Help* (accessed 3 October 2024).

<sup>58</sup> YouTube, '[How does YouTube enforce its Community Guidelines](#)', *YouTube community guidelines* (Accessed 3 October 2024).

<sup>59</sup> Google, '[Fighting phishing with smarter protections](#)', *The Keyword* (18 October 2017).

- 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<sup>60</sup> when we believe they may be the targets of government-backed phishing attacks. We have issued these warnings, which include advice about ways to improve the security of users’ Google accounts, since 2012.<sup>61</sup>

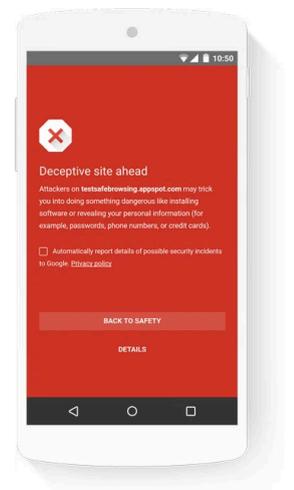
We’ve built new systems that detect suspicious email attachments and submit them for further inspection by Safe Browsing (see below). This protects all Gmail users, including enterprise Workspace customers, from malware that may be hidden in attachments.

## Safe Browsing

Launched in 2005 as an anti-phishing plugin for the Firefox browser, today Google Safe Browsing<sup>62</sup> 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.



<sup>60</sup> Google, [‘A reminder about government-backed phishing’](#), *Security Blog* (20 August 2018).

<sup>61</sup> Google, [‘Security warnings for suspected state-sponsored attacks’](#), *Security Blog* (5 June 2012).

<sup>62</sup> Google, [‘Making the world’s information safely accessible’](#), *Safe Browsing* (accessed 3 October 2024).