Australian Government
The Treasury

Scams Prevention Framework

Summary of reforms

September 2024

treasury.gov.au

Manager
Media Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

In the spirit of reconciliation, the Treasury acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples.

Introduction

Scams present a significant and unacceptable threat to the Australian community. Scammers stole $2.7 billion from Australian consumers in 2023. The digital economy has fundamentally altered how business is conducted, how payments are made, and how individuals communicate with each other. This evolution, whilst bringing gains in speed and convenience, has been accompanied by a rise in sophisticated scams which manipulate consumers, result in harm, and undermine trust in digital services.

The Scams Prevention Framework (the framework) is an economy-wide reform to protect the Australian community from scams. It recognises that a whole-of-ecosystem approach is required to reduce gaps which can be exploited by scammers, and that everyone, including industry, government, and consumers, have a role to play to combat scams. The design of the exposure draft bill was informed by a previous consultation which ran from 30 November 2023 to 29 January 2024. This paper sets out a summary of the proposed amendments, primarily to the *Competition and Consumer Act 2010,* that would establish a new framework to protect consumers against scams.

The framework imposes strong obligations to drive meaningful action against scam activity, with tough penalties for non-compliance and dispute resolution pathways for consumers to seek redress. The Government recognises that these reforms represent significant uplift and change across the scams ecosystem, particularly given the differing levels of maturity in the current anti-scam initiatives in place by entities.

Under the framework, the Treasury Minister intends to designate banks, telecommunication providers, and digital platform services, initially social media, paid search engine advertising and direct messaging services – as each represent significant vectors of scam activity. The framework includes a mechanism enabling expansion to other sectors as scammers shift their activity to target consumers through other channels.

The framework will strengthen the work of the National Anti-Scam Centre (NASC), which was established in July 2023 and is the Government's primary weapon to detect, disrupt and deter scammers and tackle online fraud. The NASC combines the expertise of Government and the private sector to disrupt scams and uses cutting-edge technology to share intelligence across Government and authorised industry participants to interrupt scams in real time. It also raises consumer awareness on the risk of scams and how to avoid them.

The establishment of the Scams Prevention Framework contributes to the broader effort by the Government to modernise Australia's laws for the digital age, including reforms to Australia's privacy, money laundering and cyber settings, modernisation of the payment systems, introduction of online safety measures, as well as the rollout of Digital ID and eInvoicing infrastructure for businesses.

As part of the consultation process, Treasury is seeking stakeholder feedback on whether the framework reflects the Government's policy intent as set out in this paper and explanatory materials. Treasury is also seeking feedback on privacy and compliance cost impacts of the proposed framework.

Interested stakeholders are invited, but not required, to provide relevant information in response to questions outlined in Appendix A as part of their submissions.

How to make a submission

Email – preferred method

Email: ScamsPolicy@treasury.gov.au

Post

Address written submissions to:

Scams Taskforce
Market Conduct Division
Treasury
Langton Cres
Parkes ACT 2600

The Government welcomes views on the exposure draft legislation via submissions to inform the final bill and explanatory memorandum.

Proposed legislation

The draft bill contains the following key features to establish the Scams Prevention Framework (SPF).

- Australians, visitors to Australia, and small businesses will be protected by the framework.
  - The framework is designed to introduce wide-ranging protections, reflecting the broad reach of scam activity and the extent of the threat faced across the economy.
  - The framework protects the following consumers (defined as SPF consumers):
    - those that are in Australia, ordinarily reside in Australia, or are a citizen or permanent resident of Australia; and
    - a business with less than 100 employees and a principal place of business in Australia.
  - In practice, this means Australian residents (including Australians abroad), visitors to Australia, and small businesses will be protected.
- A "scam" captures conduct involving an attempt, successful or otherwise, to deceive the consumer into performing an action that results in a loss or harm to the SPF consumer.
  - The definition of scam captured by the framework reflects the wide range of activities scammers engage in and is designed to capture evolving behaviours over time.
  - A scam includes both successful scams and unsuccessful scam attempts, to ensure that regulated entities are taking appropriate steps to address scam activity at all stages of the lifecycle, including where a loss may not have yet occurred.
  - The proposed definition is not intended to capture unauthorised fraud, such as cybercrimes that may use hacking and data breaches that do not involve the deception of a consumer into performing an action that results in loss or harm, including unauthorised payments. This is because scams are related to, but distinguished from, other types of fraud.
- The framework will introduce strong principles-based obligations.
  - Regulated entities will be required to adhere to principles-based obligations to take reasonable steps to prevent, detect, report, disrupt and respond to scams, and implement appropriate governance arrangements.
    - Prevent obligations broadly require a regulated entity to take reasonable steps to stop scam activity from reaching or impacting SPF consumers. This means that the steps a regulated entity may take to meet its obligations in relation to scam prevention are likely to be focused on introducing robust systems and procedures that prevent scammers from accessing or using its platform to perpetuate scam activity and educating its staff and consumers.
    - Detect obligations broadly require a regulated entity to take reasonable steps to detect scams, which includes identifying SPF consumers that are or could be impacted by a scam in a timely way. This includes taking steps to detect scams as they are happening, or after they have happened, including where a SPF consumer has already incurred a loss or before a loss has occurred.

: **Report** obligations broadly require a regulated entity to report and share information indicating possible detected scam activity (known as actionable scam intelligence[1]) with the Australian Competition and Consumer Commission (ACCC) and if requested, scam reports received by the regulated entity, to either the ACCC or the sector regulator. The ACCC may then share this information across the ecosystem to support disruptive action. Treasury understands that these requirements may require a significant uplift in infrastructure and data-sharing capabilities across some regulated entities and is seeking feedback to better understand the impact of these obligations.

: **Disrupt** obligations broadly require a regulated entity to take reasonable steps to disrupt scams suspected to be in progress to prevent losses or further losses to SPF consumers. Steps a regulated entity may take to meet its obligations in relation to scam disruption are likely to include frictions/validations to increase the likelihood the scam is disrupted prior to success. A 28-day safe-harbour protection will enable regulated entities to take proportionate disruptive steps to respond to actionable scam intelligence while an investigation into the nature of that activity is underway.

: **Respond** obligations broadly require a regulated entity to have accessible mechanisms for their consumers to report scams, and an accessible and transparent internal dispute resolution (IDR) mechanism for consumers to complain about scams (including the entity's conduct relating to scams). Entities that provide a service that is regulated by the framework must become a member of an external dispute resolution (EDR) scheme that is authorised by the Treasury Minister for their sector. The Treasury Minister intends to prescribe the Australian Financial Complaints Authority (AFCA) as the single EDR scheme for the three initial sectors designated under the framework.

: **Governance** arrangements broadly require a regulated entity to develop and implement governance policies, procedures, metrics and targets to combat scams. This obligation ensures that regulated entities have documented and dynamic policies and procedures for managing the risk of scams.

- **Sector-specific codes will outline additional detailed and mandatory obligations.**
  - The Treasury Minister will make sector-specific codes that set out additional requirements detailed for regulated entities under the framework relating to the principle-based obligations set out in the draft Bill.
  - The codes will outline sector-specific prescriptive obligations for each sector that are consistent with the principles-based obligations. This will enable the codes to provide specific obligations tailored to the scam activity in different sectors. The codes will also provide flexibility to adapt to new and emerging scams, reflecting the fast changing and dynamic nature of scam activity in the digital economy.
  - The codes will not set out an exhaustive list of obligations to satisfy compliance with the principles-based obligations, but rather will include a set of minimum standards that may be directed at addressing sector-specific harms related to scams.

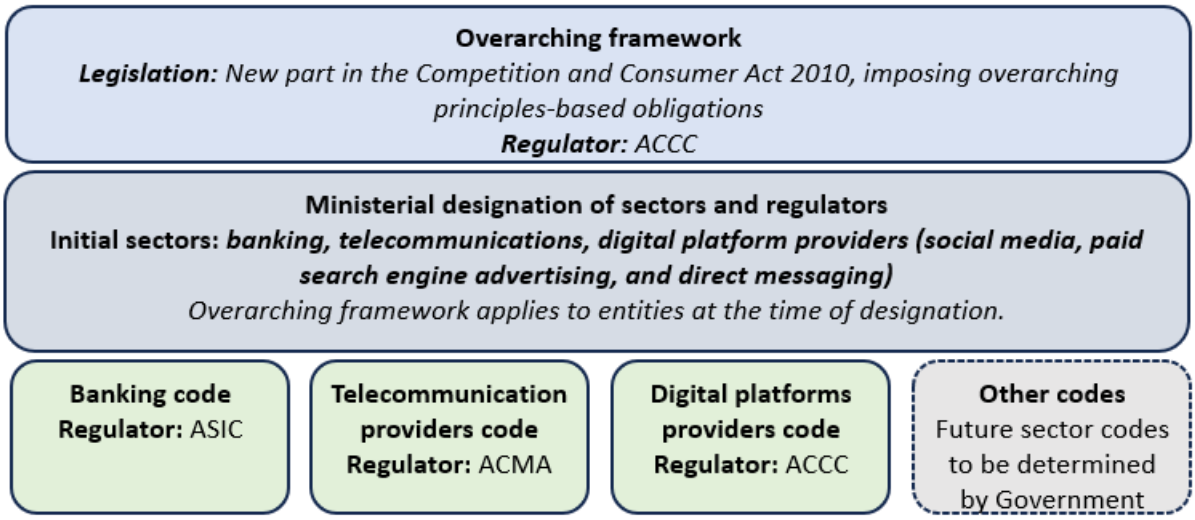
[1] 'Actionable scam intelligence' refers to information held by a regulated entity that provides reasonable grounds to suspect that a communication, transaction or activity is a scam. This may be received from a scam report, information from regulators or through the entity's own investigation. The information could include email addresses, phone numbers, URLs and information about the suspected scammer.

- The Treasury Minister can delegate the code-making powers to another Minister, the ACCC, or the entity that is to be the SPF sector regulator for the sector. For example, the Treasury Minister may delegate the code making powers for the telecommunications sector to the Minister for Communications. The Treasury Minister intends to delegate code making for the telecommunications sector to the Australian Communications and Media Authority (ACMA).

- Banks, telecommunications providers and digital platform services, initially social media, paid search engine advertising and direct messaging services, will be the initial designated sectors.
  - The Treasury Minister intends to designate these initial sectors under the framework given the prevalence of scams on their services. The designation instrument issued by the Treasury Minister will outline the scope of these sectors designated.
  - Treasury will consult on draft designation instruments before they are formally made.
  - The Government is considering appropriate transition arrangements for penalty provisions across the framework, noting the uplift that is required in capability and infrastructure to adhere to obligations. This must be balanced against the need for immediate and coordinated action to respond to the threat of scam activity and protect SPF consumers.
- The framework may be expanded to additional sectors over time.
  - The Treasury Minister may use the designation mechanism to designate further sectors and the relevant regulator into the framework over time where scam activity shifts. This could include superannuation funds, digital currency exchanges, other payment providers, and transaction-based digital platforms like online marketplaces.
  - The Treasury Minister, before designating other sectors and services under the framework, must take into consideration scam activity, effectiveness of existing industry initiatives, interests of SPF consumers and any consequences (including benefits and risks) of making the designation.
- A multi-regulator approach to enforcement.
  - The tiered regulatory design of the framework will be administered and enforced via a multi-regulator model. This will deliver a whole-of-ecosystem approach to enforcement, and leverage existing regulatory relationships, monitoring and investigation frameworks already established by regulators.
    - The intent is that ACCC will enforce the obligations in the primary law of the framework and the digital platform service provider code; the ACMA will enforce the telecommunications code; and the Australian Securities and Investments Commission (ASIC) will enforce the banking code.
    - The ACCC enforces the *Competition and Consumer Act 2010,* and is the national competition, consumer, fair trading and product safety regulator.
    - The ASIC is established under the *Australian Securities and Investments Commission Act 2001* and its role is to broadly ensure the effective performance of the financial systems.
    - The ACMA regulates communications and media services in Australia, including through the *Broadcasting Services Act 1992* and the *Telecommunications Act 1997.*
  - To ensure a coordinated and effective enforcement approach across the different sectors, the ACCC as the general regulator, will have the ability to delegate its functions and powers to sector code regulators.

- Regulators will be required to enter into one or more arrangements (such as a memorandum of understanding) relating to the regulation and enforcement of the framework. These will be published by regulators to support transparency and provide regulated entities with certainty on the operation of the multi-regulator model.
- As the framework expands to more sectors over time, additional regulators may be brought within the framework to enforce new codes where they have the relevant experience and expertise.

Figure 1. Proposed scams prevention framework



- Regulated entities will be required to have in place an accessible and transparent IDR mechanism to effectively manage consumer complaints about scams.
  - An effective IDR mechanism will be beneficial for both consumers and regulated entities.
  - It would enable consumer complaints to be resolved in a timely and efficient manner and encourage early resolution of complaints.
  - The sector-specific codes may set out additional conditions related to the IDR mechanism, such as timeframes for response.
- Entities that provide a service regulated by the framework must become a member of the prescribed EDR scheme.
  - An EDR scheme is intended to offer an independent, impartial and fair mechanism for consumers to escalate their complaints and seek redress (including compensation) where their complaints are not resolved at the IDR stage, or the IDR outcome is unsatisfactory.
  - The Treasury Minister intends to prescribe the AFCA as the single EDR scheme for the initial sectors designated under the framework (i.e. banks, telecommunication service providers and digital platform services that provide social media, paid search engine advertising and direct messaging services).
  - AFCA will continue to operate its existing EDR jurisdiction for non-scam complaints in financial services, as will the Telecommunications Industry Ombudsman in relation to non-scam complaints about telecommunications service providers.

- The framework sets out a tiered penalty regime (figure 2), with higher penalties applying to more significant and egregious breaches of the framework.

Figure 2. Proposed Tiered penalty regime

	Tier 1 contravention	Tier 2 contravention
	*Breaches of the principles-based obligations in the primary law relating to **preventing, detecting, disrupting and responding** to scams*	*Breaches of the principle-based obligations in the primary law relating to **reporting** and **governance** and any **breaches of the sector codes***
Penalty for an entity	The greater of: • $50 million • three times the value of the benefit obtained, or • 30 per cent of the turnover during the period in breach	The greater of: • $10 million • three times the value of the benefit obtained, or • 10 per cent of the turnover during the period in breach
Penalty for an individual	• $2,500,000	$500,800

Appendix: Consultation questions for stakeholders

Treasury invites stakeholders to consider the following questions in their submissions to the framework. Responses to these questions will assist the Government to finalise the bill and its assessment of the privacy and compliance cost impacts of the proposed framework.

Proposed legislation

1) Does the draft legislation effectively achieve the policy objectives set out in this document?
2) Does the draft legislation include an appropriate level of detail, noting subordinate legislation can provide more prescriptive obligations?
3) Are there provisions in the draft legislation that are better suited to subordinate legislation?
4) Will you face any practical challenges in implementing the obligations in the draft legislation?
5) What would be an appropriate transition period to enable you to implement these changes?

Usage of personal information

6) What kinds of information do relevant entities currently collect from customers (including from internal records), internal investigations and other sources to combat scams?
    a. How do entities use this information to combat fraud and scams both on their service and more broadly across the ecosystem?
    b. How do entities ensure this information is handled and stored securely?
7) What personal information will regulated entities need to comply with their obligations under the framework, particularly to take reasonable steps to prevent, detect, disrupt and respond to scams?
8) Will regulated entities be expecting to collect and store personal information to comply with their obligations under the framework which would not otherwise be collected and stored? (i.e. additional to personal information used for current or planned anti-scam activities)
9) Are there circumstances in which regulated entities may need to publicly publish personal information (e.g. of scammers) to prevent, detect or disrupt a scam?

Expected compliance costs

To support its policy impact analysis, Treasury is seeking views on the expected costs and/or resources (e.g. staffing) to be incurred by regulated entities (as designated) to comply with the framework, including sector codes when made. If possible, please provide your response in dollar terms. Please indicate if you would like such information provided in a submission to be kept confidential. Responses should include only additional costs above those already incurred, that would be attributable to the obligations set out in the framework, and that would not otherwise be incurred. If possible, please include a breakdown of the following including upfront and ongoing impacts:

- uplift in administrative processes (including staff capacity building),
- change management and education support costs,
- governance costs,
- technology uplift, including for data-sharing requirements,
- building and maintaining appropriate mechanisms to meet IDR and EDR requirements,
- additional costs, time, resources or effort for consumers, and
- any other expected compliance impacts.