Australian Government
The Treasury

Guide to Scams Prevention Framework rules and sector codes consultation

How to make a submission

You must submit your response online through https://consult.treasury.gov.au/c2026-765133#documents

Please be aware that Treasury intends to share relevant submissions with the Australian Communications and Media Authority (ACMA), Australian Competition and Consumer Commission (ACCC), Australian Securities and Investments Commission (ASIC) and the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.

If you have any issues submitting your response, you can contact us at scamspolicy@treasury.gov.au

Purpose

Treasury is seeking feedback on exposure drafts of SPF rules and sector codes for the Scams Prevention Framework (SPF). These instruments have been released as early drafts to solicit feedback from stakeholders to help shape the final design of the codes and rules. This guide poses key questions and gives further information on proposed arrangements yet to be drafted. Feedback from this consultation will be used to refine the codes and rules.

General questions

Questions one to three are relevant to both draft rules and codes.

1. Do any of the proposed provisions create conflicting requirements with other elements of the SPF or with other regulations?
2. Are there any transition arrangements required to support industry compliance?
3. Do the draft rules and codes strike the appropriate balance between effective regulation and personal privacy? If not, what changes would you suggest?

SPF Rules

The SPF rules support the effective operation of the SPF by setting out detailed, operational requirements that regulated entities must meet to fulfil their obligations under the SPF. This section includes information and questions on the draft rules and additional rules that are still in development.

Competition and Consumer (Scams Prevention Framework) Rules 2026 – Consultation questions and additional information

The banking, digital platforms and telecommunications sectors have been made regulated sectors under the SPF through a designation instrument.[1] The draft rules include exceptions to the designation instrument; **entities with an exception are not subject to SPF obligations.**

Digital platforms designation exceptions

The designation of the digital platforms sector is limited in scope by the Active Australian User Test (section 1-5) and Revenue Test (section 1-6) set out in the draft rules. It is intended that an entity will be designated as a covered digital platform service where **both** the active Australian user test and the revenue test are satisfied.

4. It is intended that the active Australian user test captures users that accessed the service from within Australia at least once during the relevant month. Does the proposed provision achieve this and does the definition of an 'active Australian user' provide sufficient clarity for stakeholders to assess whether a platform meets the 200,000 monthly average Australian user threshold?
5. Does the proposed revenue test clearly indicate it is intended to apply on a global basis, including to entities that are part of a multinational group with global revenue over $1 billion?

1 For a copy of the SPF designation instrument please visit legislation.gov.au

6. Given that financial reporting periods do not always align with the calendar year, are there any practical challenges with assessing both the active Australian user test and revenue test as at 1 January each year?

Banking designation exceptions

The designation of the banking sector is limited in scope by its application to SPF consumers. The draft rules specify that a person is not an SPF consumer of a covered banking service where they do not have a direct relationship with the regulated entity providing the service (the bank), or they are not making a payment to, or receiving a payment from, the bank (section 3-3). This exception is intended to ensure that business-to-business banking services, such as those providing back-end payment infrastructure, are not captured by the banking designation.

The rules also clarify that providers of purchased payment facilities (PPFs) are not intended to be captured by the banking designation (section 3-2). However, when provided by authorised deposit-taking institutions, PPFs are intended to be 'covered banking services'.

7. Does the proposed definition of an SPF consumer for a covered banking service effectively carve out business-to-business banking services that do not have a direct relationship with SPF consumers?
8. Does the proposed exception of providers of PPFs appropriately capture standalone PPF providers? Are there any inadvertent consequences of this exception?

Statement of compliance

Entities are required to provide consumers who make an internal dispute resolution complaint with a statement of compliance (sections 2-1 to 2-3). The statement of compliance requirements in the draft rules give an option for an entity to provide a simpler statement of compliance where a complaint is resolved in five days. This is intended to support a more streamlined process where a complaint is resolved to a consumers satisfaction quickly and efficiently, such as if an entity voluntarily reimburses a consumer for a scam loss despite not breaching the SPF.

9. How can the statement of compliance requirements in the SPF rules support the efficient and early resolution of complaints where a complaint is resolved quickly to a consumer's satisfaction?

Additional rules in development

There are additional policy settings which government intends to be included in the SPF rules but are not included in the exposure draft as they are still being developed. Information and consultation questions on these settings is below.

Telecommunication sector designation exceptions

The government intends to exclude entities who only operate private lines from designation under the SPF. A private line is a closed, controlled network which scammers would not be able to access.

Definition of scam

The government will make rules to further refine the definition of a scam. The definition will exclude misleading or deceptive conduct by legitimate businesses and Australian Financial Services License (AFSL) holders from being a scam under the SPF. This conduct is already regulated under existing Australian Consumer Law and financial services law. Misleading or deceptive conduct will still be a scam where a person impersonates a legitimate business or AFSL holder.

10. What other conduct, if any, should be excluded from the definition of a scam?

Dispute resolution

The government will make policy settings for internal dispute resolution. These policy settings will be set out in SPF rules and sector codes (see below). Please refer to the *Internal Dispute Resolution under the Scams Prevention Framework* position paper released as part of this consultation for information on what is proposed for future inclusion.

11. Should the internal dispute resolution guidance in the SPF rules enable regulated entities to apply a consumer contribution or excess to scam reimbursements?
12. Does an automatic compensation approach for losses under $3,000, as set out in the Internal Dispute Resolution under the Scams Prevention Framework position paper, provide a sensible approach to handling low-value scam complaints in an efficient and proportionate manner? If not, how else can low-value scam complaints be handled efficiently and proportionately?

Intelligence sharing/Reporting

Regulated entities are required to report actionable scam intelligence to the ACCC, which can share the intelligence with other impacted entities so they can disrupt scams. However, the obligation to share intelligence with the ACCC does not take effect until the SPF rules specify what information must be shared and how entities must share it. The government has announced that it intends to make information sharing rules at a later stage so that it takes effect by the end of 2027.

The National Anti-Scam Centre (NASC) is currently leading a collaborative process to develop proposed systems and settings for actionable scam intelligence sharing. This proposal will inform the development of SPF Rules for reporting. The government will consult on these rules at a later date.

SPF Sector Codes

The SPF sector codes will be consolidated into a single legislative instrument. The consultation includes two exposure draft code instruments because it is expected that parts of the code will be made by different ministers. The two instruments are:

- *Competition and Consumer (Scams Prevention Framework – SPF Codes) Instrument 2026*. This includes banking specific, digital platform specific and common obligations and will be made first by the Assistant Treasurer.
- *Competition and Consumer Amendment (Scams Prevention Framework – Telecommunications Code) Instrument 2026*. This includes telecommunications sector specific obligations and will be made by the Minister for Communications.

Development processes for the two instruments occurred in parallel. Differences or overlapping/duplicative provisions between instruments will be resolved post consultation.

Competition and Consumer (Scams Prevention Framework – SPF Codes) Instrument 2026 – Consultation Questions

Common Provisions

13. The draft common code provisions are intended to require regulated entities to work together effectively to resolve multi-party scam complaints through internal dispute resolution

(section 2.26). This reflects that a single scam event will often involve several entities. Does the draft code effectively require cooperation between entities during internal dispute resolution to support consumers making complaints involving more than one entity?

Banking Provisions

14. The draft code requires banks to verify the identity of consumers of their services, to prevent any misuse or manipulation by scammers (section 3-3). Is it clear how banks would implement these verification requirements? What further specific actions are appropriate for verification?
    i. For example, how should this obligation interact with existing Know-Your-Customer obligations under Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) law? Should this interaction be made explicit in the legislation?
15. The draft code requires banks to identify transactions or activities that are a high-risk of being used to facilitate scams and take proportionate preventative action to limit scam losses before funds leave the system and it is impossible to recover them (sections 3-4 to 3-7). Is it clear what is meant by transactions and activities that 'have a high risk of being, or facilitating, a scam' (section 3-4)?
16. Does the draft code make it sufficiently clear what steps are expected of banks who identify the transactions or activities referred to in section 3-4?
17. Does the draft code include sufficient obligations on sending banks to disrupt scam activity (division 4), and is it clear that the disrupt obligations extend to both sending and receiving banks?
18. Do the payment recall request obligations accurately reflect industry practice around payment recalls (section 3-11)? Is there a more appropriate way to frame this obligation?

Digital Platform Provisions

19. The draft code provisions for digital platforms are intended to be scalable and workable across different types and sizes of platforms. Do the proposed provisions appropriately address scams across all digital platforms? Do the provisions provide sufficient flexibility to support compliance by smaller digital platforms?
20. The draft code requires digital platforms to verify the details of new users and advertisers (sections 5-3 and 5-4). Is it clear how digital platforms would implement these verification requirements? What further specific actions are appropriate for verification?
21. It is intended that digital platforms undertake ongoing re-verification of users and advertisers where the platform detects a change in the identity and/or contact information of the account holder to address potential account takeover (sections 5-3 and 5-4). Does the draft code achieve this objective?
22. Should verification of an advertiser's licence be confined to verification of an applicable Australian Financial Services Licence, Australian Credit Licence and Australian Deposit-taking Institution (ADI) Licence (section 5-4)? What other Australian licences, if any, should be captured?
23. The draft code requires digital platforms to check advertisements before they are published and engage in ongoing monitoring of advertisements (section 5-5). How could the provisions minimise any unintended consequences, particularly for small businesses?

24. It is intended that a digital platform operating multiple regulated services be required to have collective processes for monitoring and detecting scam risks across its multiple services (section 5-7). Do the proposed obligations achieve this objective?
25. Do the draft code provisions to disrupt suspected and confirmed scam content and advertising (section 5-9 and section 5-11) strike the right balance of proportionate action while minimising unintended consequences?
26. Are additional safeguards needed to limit potential negative impacts on small businesses who rely on digital platforms for advertising and communication to customers?

Competition and Consumer Amendment (Scams Prevention Framework – Telecommunications Code) Instrument 2026 – Consultation Questions

27. Do the definitions in the draft code correctly reflect the sector and the positions of telecommunications services?
28. Do the obligations match the role of the entity in the telecommunications ecosystem?
29. The draft provisions consider high-risk services as using Australian numbers from overseas, multiple service practice and sending of bulk SMS, as these services can obscure scam traffic. Are there any other services which should be considered high-risk in the context of scams?
30. Could any of the obligations impede a telecommunications providers' ability to deliver legitimate, including critical, traffic?
31. Are there additional checks that should be undertaken before providing higher risk services, such as the overseas use of numbers or sending of bulk messages?
32. Are there any other scam related reasons a regulated entity should not carry a call or message that should be added to clause 8?
33. Are overseas messages using Australian numbers common? Should clause 8(3), clause 9 and clause 10 apply to messages using Australian numbers?
34. In your experience with identifying scams, are there any additional scam indicators commonly found in the content of messages that would help with detection?
35. Are there other ways telecommunications services can quickly share scam information on calls and messages they have detected and if so, what regulatory arrangements are needed to support them?
36. Are the proposed requirements sufficient to assist in resolving disputes where traffic is being disrupted?