



Australian Government
The Treasury



Advancing Australia's Scams Prevention Framework through Codes and Rules:

Position paper

November 2025

treasury.gov.au

© Commonwealth of Australia 2025

This publication is available for your use under a [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/legalcode) licence, with the exception of the Commonwealth Coat of Arms, the Treasury logo, photographs, images, third party materials, materials protected by a trademark, signatures and where otherwise stated. The full licence terms are available from creativecommons.org/licenses/by/4.0/legalcode.



Use of Treasury material under a [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/legalcode) licence requires you to attribute the work (but not in any way that suggests that the Treasury endorses you or your use of the work).

Treasury material used 'as supplied'.

Provided you have not modified or transformed Treasury material in any way including, for example, by changing the Treasury text; calculating percentage changes; graphing or charting data; or deriving new statistics from published Treasury statistics – then Treasury prefers the following attribution:

Source: The Commonwealth of Australia.

Derivative material

If you have modified or transformed Treasury material, or derived new material from those of the Treasury in any way, then Treasury prefers the following attribution:

Based on Commonwealth of Australia data.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the Department of the Prime Minister and Cabinet website (see www.pmc.gov.au/government/commonwealth-coat-arms).

Other uses

Enquiries regarding this licence and any other use of this document are welcome at:

Manager
Media and Speeches 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.

Contents

Consultation process.....1

Background.....2

About this position paper3

Next steps.....3

Part 1: Overarching policy considerations4

Reasonable steps and scalability of obligations4

Prescriptiveness.....5

Consumer choice and personal information.....6

Part 2: SPF principles.....7

How actionable scam intelligence supports the Scams Prevention Framework.....7

Principle 1: Governance.....8

Principle 2: Prevent.....9

Principle 3: Detect12

Principle 5: Disrupt15

Principle 6: Respond17

Other issues for the SPF rules23

Definition of a scam23

Definition of SPF consumer24

Designation exceptions.....24

Matters necessary or convenient for carrying out the SPF.....24

Appendix A: List of proposed codes and rules obligations.....26

Appendix B: Consultation questions32

Appendix C: List of matters for SPF codes and SPF rules34



Consultation process

Request for feedback and comments

You must submit your response online through <https://consult.treasury.gov.au/c2025-715201>.

Before you submit

To help you prepare your response, we recommend that you:

- read the supporting documents
- prepare your response in Word (DOCX or RTF) format, you can also upload PDF files as an alternative
- [read our submission guidelines](#)
- [read our privacy policy](#).

You must agree to our privacy collection statement to submit your response.

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

The principles outlined in this paper have not received Government approval and are not yet law. As a consequence, this paper is merely a guide as to how the principles might operate.

Background

The Scams Prevention Framework (SPF) establishes principle-based obligations requiring businesses to take reasonable steps to prevent, detect and disrupt scams. It also sets out new governance, response and reporting requirements.¹ The obligations set under the framework are defined by six overarching principles:

- [Principle 1: Governance](#) – Regulated entities must implement governance policies, procedures, metrics and targets for combatting scams.
- [Principle 2: Prevent](#) – Regulated entities must take reasonable steps to prevent scams connected with, or using their regulated services.
- [Principle 3: Detect](#) – Regulated entities must take reasonable steps to detect scams connected with, or using their regulated services, including investigating activities subject to actionable scam intelligence, and identifying consumers who have been or may be impacted by such activities.
- **Principle 4: Report** – Regulated entities must provide the SPF general regulator with reports of actionable intelligence about activities relating to, connected with or using their regulated services, and give this regulator a report about a scam upon request.
- [Principle 5: Disrupt](#) – Regulated entities must take reasonable steps to disrupt an activity subject to actionable scam activity, prevent losses from that activity, and report to the SPF general regulator about the outcomes of the entity's investigation into that activity.
- [Principle 6: Respond](#) – Regulated entities must have an accessible mechanism for consumers to report activities that may or may not be scams, have a transparent and accessible internal dispute resolution mechanism, and be a member of an authorised external dispute resolution scheme.

Under the SPF, the minister may issue sector-specific codes. These codes would apply to businesses that provide services in sectors that are designated to be regulated under the SPF (designated sectors). The codes will outline the minimum steps that these businesses must take to meet SPF obligations. In some circumstances, businesses may have to do more than is required in the codes to meet the principle-based obligations and what is reasonable for the business in the circumstances.

The minister is also empowered to make rules to prescribe matters outlined in the legislation or that are necessary to give effect to them. These rules may support the operation of codes and ensure clarity, consistency and enforceability across sectors.

The vision is for codes and rules to establish consistent minimum acceptable standards of consumer protections across all businesses from the outset, while ensuring clarity and fairness amongst all designated sectors. As the scams landscape continues to evolve, these instruments will be progressively updated to drive further uplift and improve scam prevention for all Australians.

1 Subsections 58BA – 58BZH of the of the *Competition and Consumer Act 2010*

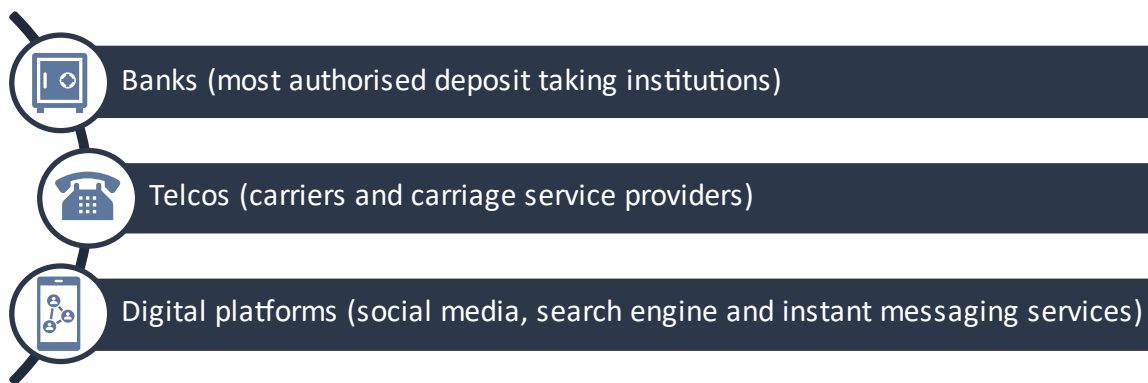
About this position paper

This position paper invites engagement from interested parties, including those responsible for combatting scams, consumers and businesses affected by scam-related harms and other interested persons to help shape the policy outcomes of SPF codes and rules.

The paper sets out preliminary views and poses questions designed to continue building our understanding of Australia's scams landscape. Treasury also welcomes stakeholder views on how SPF codes and rules can be designed to complement existing regulatory frameworks and create regulatory efficiencies.

The preliminary views set out in this paper are indicative only. They describe the potential policy outcomes the codes will support and are not legal instruments. Stakeholders will have an opportunity to comment on exposure draft codes and rules during public consultation in early to mid-2026.

This paper has been released alongside draft sector designation instrument for:



While the draft digital platform sector designation applies to search engine services generally, the digital platforms code is intended to apply obligations only to paid advertising featured on these services, and not to organic (or 'unpaid') search results.

A draft instrument to authorise the Australian Financial Complaints Authority (AFCA) as the external dispute resolution (EDR) scheme for scam complaints for these initial 3 sectors has also been released. For more information related to the designation instruments, please refer to the relevant explanatory statements.

Please note: for simplicity, this paper generally refers to SPF consumers as 'consumers' and regulated entities as 'businesses'. A 'customer' is occasionally referenced throughout this paper, which carries a separate meaning from 'consumer' and is a person with a direct contractual relationship with a business. This paper does not cover SPF rules related to intelligence sharing under the Principle 4: Report. This will be addressed through a separate consultation in 2026.

Next steps

The implementation pathway for the Scams Prevention Framework will be completed in stages. This will ensure that protections are introduced quickly and allow more time for some higher complexity obligations to come into effect. The SPF is intended to commence operation on 1 July 2026 and be fully implemented for the announced 3 sectors by the end of 2027. The implementation stages are proposed as follows:

- The foundations of the SPF will be in place by no later than 30 June 2026, with industry obligations in force and internal dispute resolution available to consumers. These settings will be supported by sector designations and industry codes for the banking, telecommunications, and digital platforms (social media, search engine and instant messaging services) sectors, and supporting operational rules.
- Alongside the supporting instruments for the SPF, the Australian Government will authorise AFCA as the prescribed external dispute resolution scheme for scam complaints. Businesses will be required to be members of AFCA by 1 September 2026. AFCA will be required to accept SPF complaints for EDR from 1 January 2027, though it will take some time for AFCA to build up to full capacity.
- Supplementary rules, including some obligations under Principle 4: Report and [Principle 5: Disrupt](#) of the SPF to report actionable scam intelligence and scam investigation outcomes, will be introduced at a later stage. These rules are necessary to enable intelligence sharing and will be made by 31 March 2027, with industry obligations to commence by the end of 2027.

Part 1: Overarching policy considerations

Overarching policy considerations guide the development of sector codes and rules, and help ensure consistency and effectiveness. They also support broader goals such as encouraging innovation and driving investment in scam prevention efforts that make the biggest difference. This approach is critical to building a trusted, coordinated response to scams, protecting consumers and helping businesses operate confidently in a safer digital environment.


Reasonable steps and scalability of obligations

The SPF establishes a baseline requirement for all businesses to take reasonable steps to prevent, detect and disrupt scams. This supports a consistent and accountable approach to scam prevention across sectors.

Reasonable steps involve businesses taking genuine, proactive and proportionate actions to reduce scam activity on their platforms or services. These actions should reflect the size of the business, its operational complexity and exposure to scam-related threats.

To support a competitive and innovative market, obligations under SPF codes and rules are designed to be scalable and proportionate to capacity, risk and harm:

- Larger businesses or those facing higher scam risks may be expected to go beyond minimum requirements to meet their obligations under the SPF.
- Smaller businesses may find that meeting minimum standards requires initial investment, but these standards help reduce risk over time and strengthen protections for businesses and consumers.



By aligning regulatory expectations with risk, the framework encourages targeted investment in prevention activities that deliver the greatest impact. Sector codes will serve as the primary factor for assessing whether a business has taken reasonable steps.² Other relevant factors include:

- **The size and capacity of the business** – larger businesses may be required to implement more robust measures.
- **The kind of service involved in the scam** – different types of services will need different anti-scam measures.
- **The consumers of the service** – anti-scam measures should be tailored to the service’s customer base.
- **The kind of scam risks those services face** – anti-scam measures should be adaptable to the kinds of scam risks faced by businesses and their customers.

Together, the reasonable steps test and scalability ensure that scam prevention obligations are proportionate, practical, and aligned with the nature and complexity of each business and its services.

Prescriptiveness

To keep pace in the constantly changing scams environment and address the complexity of some scams, the SPF codes will include both prescriptive and principle-based obligations. This balance is important because businesses will sometimes need to use their judgment when assessing how to respond to scam threats, particularly where intelligence is incomplete or ambiguous. Flexibility can also enable better consideration of consumer circumstances and adaptability for various businesses to respond to changing technologies.

If the codes are exclusively prescriptive, they risk becoming rigid and outdated as scammers rapidly adapt their tactics. This could leave businesses and consumers vulnerable to new and unforeseen harms. By incorporating principle-based obligations that require businesses to exercise judgment based on specific context, codes will remain responsive and effective for longer.

There will likely be code obligations that require businesses to make an evaluative judgement on the likelihood that a threat is a scam and the level of risk to consumers posed by a scam. Treasury invites stakeholders to provide feedback on what could be included in codes to assist businesses to make these evaluations, including factors that businesses should consider when assessing the likelihood and level of risk posed by a scam.

Where possible, the codes will include prescriptive obligations to provide as much regulatory certainty as possible. Prescriptive obligations could include or relate to:

- **Timeframes:** Creating a clear benchmark to assess whether a business has acted in a timely manner. This is important in high-risk scenarios where delays can result in significant financial or emotional harm to consumers. Timeframes may also help create minimum standards across sectors, especially where scam response capabilities vary.

² Section 58BB of the of the *Competition and Consumer Act 2010*

- **Standards:** The SPF codes and rules may reference existing industry standards to ensure obligations are in alignment. However, the codes or rules will not introduce duplicative or conflicting obligations.
- **High risk scam threats:** Businesses will need to take specific actions when certain high-risk scams are identified. For example, if a bank is aware that a customer has been scammed, the codes could require the bank to immediately issue a recall request to the receiving bank and require the receiving bank to act on this request.

Consumer choice and personal information

Effective scam prevention requires a balance between protecting consumers and respecting their autonomy.

Measures such as enhanced identity verification or restrictions on messaging introduce friction into digital services but may be necessary in certain circumstances. While these changes may be inconvenient, they can help reduce risk. Businesses should implement protections that are targeted when needed and to empower individuals who are confident in managing their own risk.

This balance is important to accommodate the diverse needs and circumstances of consumers. Some individuals may prefer to opt out of certain protections, while others may benefit from additional support, particularly during periods of increased exposure to scam risks. These may include major life events such as buying a home or planning for retirement, or personal factors such as age, language or digital literacy.

Personal information enables businesses to understand scam risks. Data about suspected scammers and scam victims can help businesses build a stronger evidence base, detect scams in real time or retrospectively and identify affected consumers. It helps businesses tailor protections to individuals who may be more exposed to scam threats. However, data-driven approaches must be implemented responsibly. Risk assessments should not unfairly disadvantage any group of consumers. Additional support should be used to enhance access and safety, not to justify restrictive or exclusionary practices.

Consultation questions

1. Are there other policy considerations that should be taken into account when developing rules and code obligations?
2. What should be included in codes to help businesses evaluate the level of risk posed by scams, and what factors should they consider when making these assessments?
3. Should consumers be able to opt out of scam prevention measures?
4. What safeguards, if any, should be in place to protect consumers with a higher risk of being scammed?

Part 2: SPF principles

This section outlines Treasury's preliminary views on the policy outcomes for each SPF principle (except *Principle 4: Report*). The examples are indicative only: they describe the potential policy outcomes the codes will support and are not legal instruments. For telecommunication providers, the potential obligations build on the existing *Reducing Scam Calls and Scam SMS* industry code.

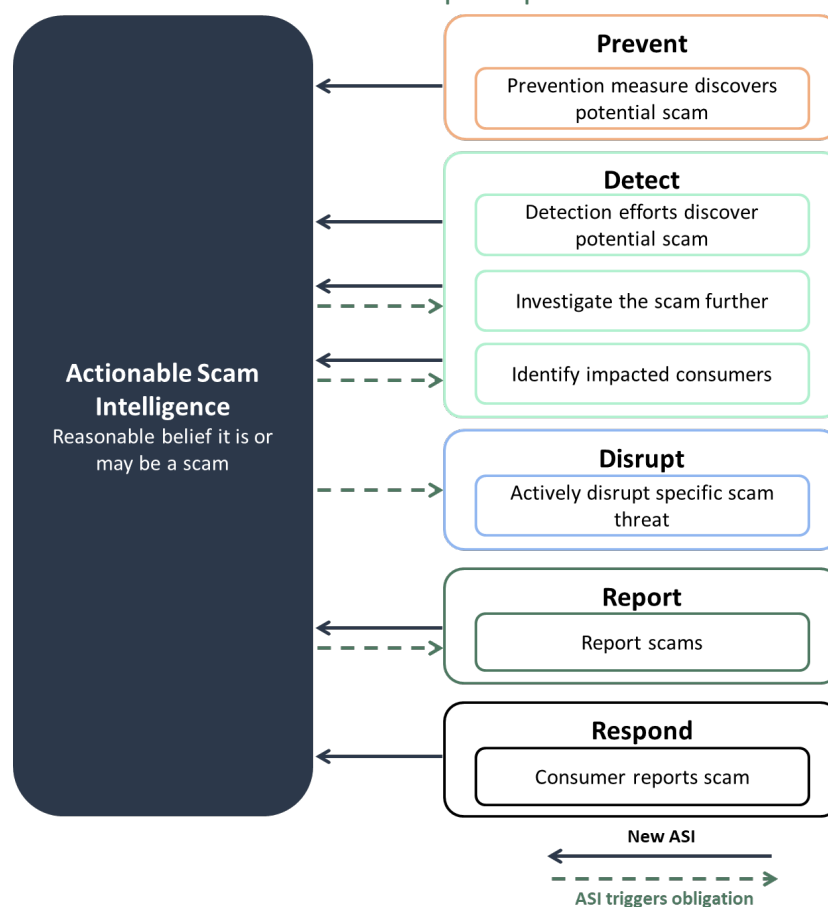
Stakeholders will have an opportunity to comment on exposure draft codes and rules during public consultation in 2026.

How actionable scam intelligence supports the Scams Prevention Framework

Actionable scam intelligence is central to the principles-based operation of the SPF. It arises when a business has reasonable grounds to suspect that a communication, transaction or other activity related to the entity's regulated services is a scam. Businesses can receive actionable scam intelligence from multiple sources, and the legislation is agnostic as to how it is received. For example, a business might receive actionable scam intelligence from a consumer report, through its detection activities or from the Australian Competition and Consumer Commission (ACCC) or another entity. Once it has actionable scam intelligence, the business must take reasonable steps to:

- investigate the scam further (detect)
- to identify impacted consumers (detect)
- to disrupt the scam, and
- if required by the SPF rules, report the scam to the ACCC.

Figure 1: Actionable scam intelligence interacts with different Scams Prevention Framework principles



Principle 1: Governance

Governance measures the effectiveness of policies, procedures, metrics and targets to drive a strong anti-scam posture. For the SPF, businesses will be required to have clear and accountable governance structures that support continuous improvement in scam prevention practices.³

We propose that governance obligations support proactive scam prevention and an appropriate level of strategic oversight for senior executives or managers responsible for a business's effort to reduce scam harms on their platforms or services.⁴ The governance obligations will be designed to complement and work cohesively with existing broader corporate governance frameworks.

Complementing the obligations in the SPF, the codes and rules will also support the following policy outcomes for 'Governance':

³ Subsections 58BC – 58BH of the of the Competition and Consumer Act 2010

⁴ Some of the proposed obligations in Governance may sit under other principles in law but have been grouped together to improve readability as they are related to governance arrangements that will support the SPF's operation.

- **Transparency and accountability.** Businesses embed scam prevention within leadership and governance structures, ensuring senior management oversight and clear lines of accountability. This includes assessing whether appropriate actions are being taken to mitigate scam harms.
- **Data-driven continuous improvement.** Businesses maintain robust policies, procedures, and systems to collect and analyse relevant datasets. This enables ongoing learning and refinement of strategies to address scam threats. Regular reviews of policies, complaints, outcomes, and other insights support adaptive responses and operational transparency.
- **Evidence-based risk management.** Maintaining comprehensive records of scam-related complaints and outcomes allows businesses to consider whether interventions are effective.
- **Assurance mechanisms.** Businesses implement internal controls and assurance processes to monitor performance and outcomes. Mechanisms such as audits, compliance reviews, and performance monitoring enable organisations to evaluate the effectiveness of scam prevention and ensure governance standards are upheld.

Principle 1: Governance – Potential code and rules obligations

All sectors

Businesses must embed responsibility for scam prevention within their governance frameworks including strategic risk management and oversight.

Consultation questions

5. What oversight and reporting mechanisms are in place to keep senior executives informed of scam-related risks and incidents?
6. What data, including complaints data, is useful to help develop and maintain policies and procedures?
7. Should other governance obligations be considered for inclusion in sector codes?

Principle 2: Prevent

A central part of the SPF is the requirement for businesses to take reasonable steps to prevent scams on their services.⁵

In most cases, preventative actions are informed by overarching developments in scam activities, including scam trends and responses, rather than in direct response to specific items of actionable scam intelligence.

Sector codes will support the following policy outcomes for ‘Prevent’:

⁵ Subsections 58BH – 58BK of the of the *Competition and Consumer Act 2010*

- **Businesses have appropriate capabilities to meet their SPF requirements and prevent scams.** This includes ensuring third parties who act on their behalf meet SPF requirements and have sufficient resources and arrangements to support their obligations.
- **Businesses proactively identify and assess current and emerging scam threats.** This will help businesses to take a proactive and evidence-based approach to scam prevention. It will also support targeted interventions for high-risk activities, products, services, delivery channels, counterparty jurisdictions, accounts, advertisements and content.
- **New users of regulated services are identified and verified.** User verification checks should be proportionate to the risk of the service and updated in response to emerging scam threats and consistent with existing regulatory requirements such as 'know you customer' obligations. Businesses may need to re-verify customers who are at a high risk of providing scammers with access to their accounts (for example, to confirm consumers are still controlling their accounts).
- **Businesses impose risk-based controls to prevent scams from occurring on their platforms.** Businesses should impose measures that make it more difficult for scammers to leverage their services. These measures should be proportionate to the scam risk and balance additional friction and broader economic costs with increased consumer protections. This could involve imposing additional verification requirements for digital platforms around advertising services with a high scam risk (such as financial advice); or requiring banks to provide additional warnings before completing higher-risk transactions, such as new transfers to overseas accounts.
- **Consumers are educated about scam risks.** Awareness empowers consumers to recognise and avoid scams. Businesses should tailor their education efforts to different cohorts, including consumers at a higher risk of being scammed. When warnings are not tailored, there is a high risk they are ignored. Businesses should use multiple channels to reach consumers, including customer service interactions and public awareness campaigns.
- **Businesses take reasonable steps to prevent brand impersonation.** This should make it harder for scammers to impersonate a businesses' brand or personal profile. For example, businesses taking steps to prevent their number being spoofed by scammers.
- **Additional protections are provided for consumers at a higher risk of being scammed.** Tailored protections make sure people at a higher risk of being scammed have additional protections that are proportionate and effective. Businesses should consider how vulnerability may change over time and in different contexts, noting the intent is not to create exclusionary risks for those consumers in need of additional support.
- **Staff education and training.** Targeted training equips frontline and compliance staff with the knowledge to identify and respond to scams effectively, to support consumers who may be victims of a scam and to minimise consumer harm. Training should be tailored to role-specific responsibilities and updated in response to emerging threats and improved practices.

Principle 2: Prevent – Potential code obligations

All sectors

- Businesses must have systems in place to identify vulnerabilities that are being or could be exploited by scammers on their services.
- Businesses must require multi-factor authentication for log in attempts from new devices.
- Businesses must provide accessible information to consumers about scam risks on their services, including a scam awareness webpage. This should include easy referral to public resources, such as scamwatch.com.au.
- Businesses must take effective steps to protect their brand from being used in scams, including on other communication platforms, such as social media and online search services.
- Businesses must provide scam prevention training to relevant staff, tailored to their roles. For scam response roles or customer-facing roles, businesses must have processes in place to ensure staff understand emerging scam trends.

Banks

- Banks must provide targeted warnings about scam risks to customers before they make high-risk payments.
- Banks must use name-checking technology to confirm a payee's details match those provided by the payer.
- Banks must have systems in place to verify the identity of their customers and to understand the nature of their transactions.

Digital platforms

- Digital platforms must verify advertisers hold licences necessary to provide high-risk products, such as financial services and healthcare products.
- Digital platforms must provide warnings to users in high-risk circumstances, such as receiving messages from unconnected accounts, or messages requesting financial details.
- Digital platforms must have authentication processes to ensure accounts are legitimate, including comparing new account details against previously banned accounts, and requiring business users and advertisers to provide appropriate identification.

Telcos

- Carriage service providers must verify a customer has a legitimate use case before offering certain services. This includes confirming a customer has a legitimate use case to originate calls using a number not allocated to the originating carriage service provider.

Consultation questions

8. Would codes benefit from specific consumer verification requirements?
9. How can businesses ensure scam education efforts are inclusive and accessible to diverse consumer groups, including those with limited digital literacy or language barriers?
10. What additional protections should be in place for consumers who may be at higher risk of being scammed, in a way that is proportionate, effective and non-exclusionary?

Principle 3: Detect

Active detection of scams goes beyond consumer reporting. Businesses will be required to actively search for scams across all designated services and platforms.⁶ Detection obligations generate critical intelligence to support businesses in taking reasonable steps to disrupt scams and respond effectively.

Proactive detection enables swift disruption, protecting consumers and significantly reducing harm. Once actionable scam intelligence is identified, businesses must act promptly to investigate the activity and identify consumers who may have been impacted.⁷

Meeting detection obligations does not mean businesses are expected to identify every scam in real time. Scammers often mimic legitimate business or consumer behaviour, making detection challenging. This is why a reasonable steps test applies.

Obligations under this principle interact closely with all other areas of the SPF, and may be linked to or, in some cases overlap, to ensure detection leads to disruption where necessary.


Sector codes will support the following policy outcomes for 'Detect':

- **Businesses proactively detect scams on their services.** This enables earlier intervention and reduces consumer harm. It supports consistency in detection practices across sectors and provides a foundation for timely disruption. This will involve businesses monitoring their own services for scam activity, including information provided in customer reports, suspicious transactions, communications, content, advertisements or account behaviours that may indicate a scam is occurring or has occurred. Monitoring should be tailored to the nature of the service and informed by scam risks relevant to the sector.
- **Businesses investigate actionable scam intelligence in a timely manner.** This will help determine whether the activity is a scam and the level of risk it poses to consumers. This will then help determine the steps needed to disrupt the scam. Investigations should be risk-based and proportionate, with high-risk cases prioritised for urgent action. Businesses may be required to gather specific data, such as the suspected scammer's phone number, account number or social media account and details about how the consumer was contacted.

This provides valuable actionable scam intelligence to support disruption efforts, and will help support reporting arrangements, noting Treasury will consult on these separately. Businesses may need to take steps to disrupt a potential scam while they investigate the threat (see

⁶ Subsections 58BL – 58BP of the *Competition and Consumer Act 2010*

⁷ Subsection 58BO of the *Competition and Consumer Act 2010*



Principle 5: Disrupt) and take steps to consider the information provided from consumer reports of scams or suspected scams (see [Principle 6: Respond](#)).

- **Businesses identify the overall impact of the scam and the consumers impacted.** Identifying the impact of the scam will involve assessing financial and non-financial impacts and understanding the nature of the scam so the entity can provide appropriate support (such as targeted disruption, consumer notification and referrals to external support services). For businesses that hold personal information, this will likely also mean investigating whether an SPF consumer is at risk of identity theft.

Principle 3: Detect – Potential code obligations

All sectors

- Businesses must investigate actionable scam intelligence, including systems or processes in place to gather specific data to assist potential disruption activities.
- Businesses must have systems in place to identify consumers impacted or potentially impacted by a scam.

Banks

- Banks must have systems in place to monitor all transactions for suspicious activity that might be a scam and identify actionable scam intelligence.
- Banks must have systems in place identify consumers that have made a payment to a known scam account. This includes identifying customers at another bank where the bank identifies a home account that is suspected of receiving scam proceeds.

Digital platforms

- Digital platforms must have systems in place to proactively detect accounts, content, messages and advertisements suspected of being associated with scams.
- Digital platforms must identify, notify and warn:
 - owners of accounts exhibiting behaviour associated with account compromise,
 - consumers who have communicated with accounts associated with scam activity or interacted with content or advertisements associated with scam activity.

Telcos

- Telcos must have processes and systems in place to analyse traffic (calls and messages) for patterns or indicators of a scam. These could include a combination of:
 - calls or messages from numbers already under investigation,
 - patterns of behaviours such as sending mass communications from a new number or IMEI,
 - unusual increases in calls for a number,
 - repeated short call durations,
 - calls from invalid numbers or numbers on do not originate lists.
- Telcos must have systems in place to identify consumers who received scam calls or short messages, with a focus on consumers who have engaged with the suspected scammer via returning a text message or speaking with them on the phone.

Consultation questions

11. What challenges do businesses face when investigating scams, particularly in verifying intelligence or assessing risk levels, and how might these challenges be accommodated in setting SPF code obligations?

Principle 5: Disrupt

The disrupt principle works together with the detect principle to ensure businesses take steps to remove or reduce scam activity when identified on their platform or services. Disruption is intended to eliminate or minimise further harm to consumers and limit the ability of scammers to continue operating. A business will be required to take reasonable steps to disrupt scam activity once it has actionable scam intelligence.⁸ A business can obtain actionable scam intelligence from several sources, including internal detection efforts (see Principle 3: Detect), consumer reports (see [Principle 6: Respond](#)) or intelligence shared by regulators or other businesses.⁹

Disruption actions should be timely and proportionate. While some scams require immediate and decisive action, others warrant a measured response to avoid unintended consequences, such as disrupting legitimate consumer activity or business operations.

Under the *Scams Prevention Framework Act 2025* (SPF), businesses are provided with temporary safe harbour from liability for the impact of any disruption activity while they investigate the scam, provided the action is taken in good faith and is proportionate to the risk of the scam.¹⁰ It is important to recognise that some disruption measures, such as freezing a bank account, can have serious consequences for consumers, potentially cutting off access to essential funds and services. Businesses must carefully balance the need to prevent harm from scams with the potential impact on consumers when implementing disruption measures.

Codes and rules will support the following policy outcomes for ‘Disrupt’:

- **Scams and scammers are removed from the relevant service.** This is critical to prevent further harm to consumers by stopping the continuation of scam activity. This will involve removing scam advertisements, disabling fraudulent accounts and blocking phone numbers or domains used by scammers.
- **Possible scam activity is disrupted while it is investigated.** This will help protect consumers from harm while businesses determine if a threat is a confirmed scam. This may include reversing the scam transaction where possible, such as recalling a payment from a scam account.

8 Sections 58BW – 58BZA of the *Competition and Consumer Act 2010*

9 Consultation for supplementary rules, including those for obligations under Principle 4: Report and [Principle 5: Disrupt](#) to report actionable scam intelligence and scam investigation outcomes, will be published in 2026–27.

10 Subsections 58BZA(1) and (2) of the *Competition and Consumer Act 2010*

- **Services are restored where it is not a scam.** Where disruption actions have been taken and investigation confirms that the activity was not a scam, it is critical businesses promptly restore access to affected services to prevent further harm to the impacted customer. This includes unfreezing and unblocking accounts, removing flags or restrictions and notifying consumers of the outcome. The safe harbour for disruptive actions will only apply if such services are restored when reasonably practicable.¹¹
- **Consumers are notified of disruption actions that affect them.** This will ensure consumers understand the reasons for the action, expected timeframes for resolution and have guidance on next steps.¹² Where appropriate, consumers should be given an opportunity to respond or clarify their circumstances, enabling the business to determine if they have mistakenly identified a consumer as being involved in scam activity.
- **Consumers are warned about specific scam threats.** Providing proactive alerts to consumers who may be impacted by specific scams enables consumers to take action to limit harm. Alerts may include warnings about suspicious transactions, scam-related content or impersonation attempts. They should be timely, accessible and tailored to the consumer's risk profile and the risk profile of their proposed transactions. These warnings should go beyond general consumer education about scams. They are not intended to cover every possible scam but should be communicated by businesses in response to specific threats that could impact their customers.

Principle 5: Disrupt – Potential code obligations

All sectors

- Businesses must alert customers as soon as practicable where there is a risk they are involved in an ongoing scam.¹³
- Businesses must issue targeted scam alerts to consumers where there is a reasonable suspicion a specific scam threat may impact them.
 - Scam alerts must include information on how to report the scam and access support services.
- Businesses restore disrupted services where investigations found that the relevant activity was not a scam.
- Businesses must notify consumers impacted by disruption activities, including how the disruption affects them.

11 Paragraph 58BZA(2)(e) of the of the *Competition and Consumer Act 2010*

12 Businesses subject to obligations under *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* will need to consider interactions with that regime

13 Businesses subject to obligations under *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* will need to consider interactions with that regime

Banks

- Banks must close – and block payments to and from – accounts controlled by scammers (where the account owner is either the scammer or complicit in the scam) or freeze the account and return it to the account owner (where the account access was stolen from an innocent party).
- Banks must take reasonable and proportionate measures to disrupt potential scam activity. This may include interim or permanent disrupt actions, such as:
 - issuing a payment recall request where it has reasonable that a payment may have been made to a scammer. Banks must immediately act upon payment recall requests made by other banks,
 - suspending or freezing an account suspected of being used by a scammer while the bank investigates,
 - enabling customers to instantly freeze accounts to block outgoing payments when they are concerned they have been compromised by scammers, such as through an in-app function or a dedicated priority call centre.

Digital platforms

- Digital platforms must permanently ban users and advertisers found to have been operating scams on their services and prevent them from creating new accounts.
- Digital platforms must permanently remove or delist content (for example, social media posts or videos) and advertising linked to a scam and prevent future distribution.
- Digital platforms must notify users they identify as having been potentially impacted by a scam (for example, users who have interacted with content since removed for scams) and warn users in real time if they are contacted by accounts under investigation for scam activity.
- Digital platforms must take reasonable and proportionate measures to disrupt potential scam activity under investigation. This may include interim measures to:
 - limit visibility of content and advertising being investigated for scam activity,
 - publicly flagging content and messages being investigated for scam activity,
 - suspending all display of advertising being investigated for scam activity.

Telcos

- Carriage service providers must block calls and messages from or to calling line identifiers (CLI) confirmed to be a scam following investigation of actionable scam intelligence.
 - Carriage service providers must temporarily withdraw CLI from calls and messages from or to phone numbers which are subject of an investigation of actionable scam intelligence.

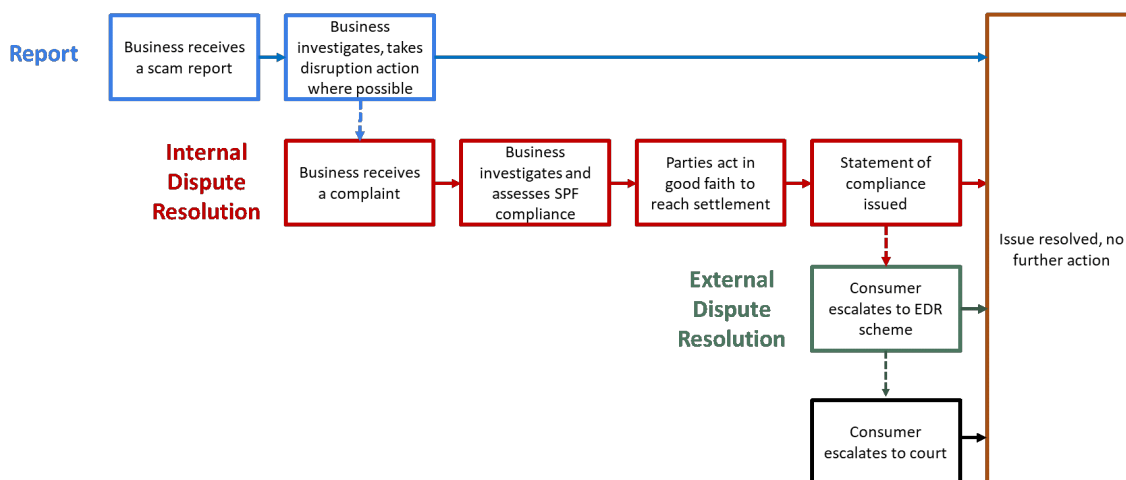
Consultation questions

12. What criteria should be used to determine when disruption actions are deemed necessary (for example, freezing accounts, removing content)?
13. What safeguards should be in place to ensure disruption actions do not disproportionately impact legitimate users, particularly vulnerable cohorts and small business users?
14. What is the most effective and practical way for businesses to alert customers as soon as practicable when there is a risk they are involved in an ongoing scam?

Principle 6: Respond

How businesses respond to consumers who may have been scammed can significantly influence a scam's financial and emotional impacts. Minimum standards will ensure businesses respond appropriately to consumers making a **report** of a possible scam or a **complaint** about how a scam has been handled (to either a business or the authorised SPF EDR scheme).¹⁴ A consumer journey through these processes is illustrated in Figure 2.

Figure 2: Scams Prevention Framework – consumer journey



Due to the multi-layered approach to scam response set out in the SPF, this section of the paper sets out the intention and proposed policy settings for:

- reporting a scam under s 58BZC
- making complaint about how a scam was handled by a business for internal dispute resolution (IDR) under s 58BZD
- the statement of compliance required under s 58BZDA, and
- guidance for businesses working together and apportioning liability in multi-party disputes under subparagraph 58BZE(1)(b)(ii).

¹⁴ Subsections 58BZB – 58BZH of the *Competition and Consumer Act 2010*

Consumers making a report of a scam or possible scam

The 'Respond' principle works together with the 'Detect' and 'Disrupt' principles to allow consumers to alert businesses to possible scams on their services. SPF codes will include settings aimed at ensuring all regulated entities accept a scam report from a consumer, businesses' communications with consumers are timely and helpful, and businesses triage consumer reports to allow scam disruption or quick resolution.

Potential code obligations for reporting a scam

In addition to the obligations set out in the primary law, all sectors must:

- publish information on how to make an urgent report about a scam that may be in progress.
- accept scam reports 24/7 and free of charge.
- provide an acknowledgement of a scam report as soon as practicable but within 24 hours of receiving the report. The acknowledgement must provide information about how to escalate the report to a complaint for IDR if the consumer is dissatisfied with how the report is handled.

Consumers making a complaint to businesses about how scams are handled


Consumers must be able to make a complaint and seek compensation and/or other remedies through a business' accessible and transparent internal dispute resolution process.

Since a consumer's right to compensation under the SPF emanates from non-compliance by businesses, businesses must consider whether they have met their SPF obligations relevant to the scam when a complaint is received. The SPF is different in this regard to frameworks that link compensation to the actions of the consumer, like the ePayments Code or the mandatory Authorised Push Payment Reimbursement Policy in the United Kingdom, which both presume the consumer will receive reimbursement unless the consumer is negligent or careless. Under the SPF, if a consumer suffers harm as a result of a scam, it is the business' conduct that is key to determining compensation, not the consumer's.

Accessible and transparent internal dispute resolution

All businesses must have the capacity to accept complaints for IDR, respond quickly when a complaint is made, work together to support consumers in multi-party disputes and provide reasonable redress if they have breached relevant SPF obligations.

When a business receives a complaint about a scam it will be required to provide a **statement of compliance** and resolve the complaint (including issuing any proposed remedy) within specified timeframes. The purpose of the statement of compliance is to reduce information asymmetries between consumers and businesses in relation to the business' actions related to the scam.



Given the likelihood that more consumers will approach their bank first when they suspect they have been scammed, the proposed timeframes and other IDR obligations aim to align with the Australian Securities and Investment Commission (ASIC) Regulatory Guide 271 (RG271) on Internal Dispute Resolution for the banking sector where possible.

Potential code and rule obligations for IDR

In addition to the obligations set out in the primary law, all sectors must:

- make information about how to make complaints publicly available and offer accessible communication options that recognise consumer circumstances.
- accept scam complaints 24/7 and free of charge.
- provide an acknowledgement of the complaint within 24 hours or as soon as practicable.
- facilitate a no wrong door approach to complaints (allowing a consumer to make a complaint to any business involved in the scam chain).
- issue any proposed remedy within 30 calendar days of receiving an SPF complaint.
- respond to requests for information from other regulated entities assisting a consumer with the same scam complaint in a timely way.

Statements of compliance must:

- be provided to a consumer in writing no later than 30 calendar days after the business receives a scam complaint.
- set out what specific steps the business took to comply with the SPF in relation to the consumer's scam.
- describe the remedy provided to the consumer or the reasons why a remedy has not been offered.
- explain the consumer's rights and processes for escalating the matter to EDR if they are dissatisfied with the IDR outcome.
- be signed off by a manager with responsibility and oversight of the matters contained in the complaint, as identified in the business' governance policy and procedures.

If a business resolves the complaint to the consumer's satisfaction within 5 calendar days of receiving the complaint, no statement of compliance will be required.

Guidelines for IDR

The SPF allows the minister to make rules to guide the way businesses undertake IDR, how they work together to resolve complaints at IDR and how they should apportion compensation payments between them. The SPF rules will contain guidance to support the requirement for cooperation that will be in SPF codes and the timely and effective resolution of complaints involving more than one business. Businesses will be required to have regard to these guidelines.

Since any settlement reached and offered through IDR requires mutual agreement, the SPF can encourage businesses to work together and to offer a joint resolution but cannot mandate outcomes.

Potential guidance in rules for businesses working together and apportioning compensation

- Businesses assisting the same customer with the same scam complaint should work together to resolve the complaint in a manner that minimises the burden of the complaints process on the consumer (for example, by facilitating a single front door for complaints) (see the next section).
- Where more than one business provides a statement of compliance to the effect that it has not complied with a relevant SPF obligation, the businesses should collectively offer redress that reasonably represents the consumer's losses.
- As a default, each entity offering to compensate a consumer for a multi-party scam loss should pay an equal share of compensation. Where one entity is clearly more or less culpable for the loss and agreement is reached between businesses within IDR timeframes, other apportionment arrangements may be agreed.

Optimising cooperation at IDR – a business-led solution

The expectation under the SPF that regulated entities work together to compensate consumers, in recognition of the fact that scammers often exploit vulnerabilities across several sectors to perpetrate a single scam, is ambitious. Guidance for multi-party disputes is aimed at encouraging businesses to cooperate with one another and make timely decisions. Any settlement reached and offered through IDR needs mutual agreement, so while the SPF rules can require businesses to find ways to work together, they can't compel them to offer a joint resolution.

This feature of IDR does not preclude the generation of business-led solutions. For example, businesses across regulated sectors may agree to invest in a third-party administered IDR solution that can coordinate multi-party disputes and act as a one-stop-shop for consumers. Treasury would welcome an initiative of this nature from industry. Proposals should comply with the primary law; ensuring consumers are appropriately compensated by the IDR process and retain their right to escalate dissatisfaction with the IDR result to EDR. To support this, Treasury would welcome feedback on any ways the IDR settings could be amended to better facilitate an industry-led solution.

The EDR scheme to assist with complaints

If a complaint is not resolved at the IDR stage, or the IDR outcome is unsatisfactory, consumers may escalate the complaint to the SPF EDR scheme. The Australian Government intends to authorise the Australian Financial Complaints Authority (AFCA) to be the SPF EDR scheme operator for the 3 sectors it has announced will be subject to the SPF.

AFCA will be required to publicly consult on the changes to its rules needed to implement the EDR arrangements. The AFCA rules will clarify:

- who is eligible to make a complaint,
- what scam complaints are eligible to be considered by AFCA,
- what changes to jurisdiction and processes will be required to allow it to expand its membership to SPF businesses and effectively deal with complaints.¹⁵

In accordance with its usual process, AFCA will provide accessible information on:

- how to make an EDR complaint,
- the complaint process,
- how a consumer should expect SPF complaints to be handled at EDR.

The SPF can include code obligations for businesses regarding the EDR scheme. Given the comprehensive primary law obligations related to EDR in the SPF, which will be supported by changes to AFCA's rules, Treasury's initial view is that further EDR-related obligations in the subordinate legislation are not necessary. Treasury would welcome stakeholder feedback on whether any additional EDR code obligations should be considered.

Consultation questions

15. How can SPF rules and codes encourage cooperation and timeliness in multi-party disputes?
16. How should the SPF rules and codes relating to IDR manage or reflect disparate industry standards?
17. If SPF codes allow consumers to opt out of certain frictions for certain transactions, how should that impact their right to redress?
18. Should any additional information or evidence be included in the statement of compliance?
19. What roles should non-financial remedies or compensation for non-financial harm play in determining appropriate redress?
20. Should the proposed SPF rules and code obligations better facilitate industry developing innovative approaches to fast-track resolution of high-volume, low-value scam losses?
21. Should any code obligations be made to help ensure the external dispute resolution scheme operates effectively?

15 The AFCA Rules are available at <https://www.afca.org.au/about-afca/rules-and-guidelines>.

Other issues for the SPF rules

SPF rules can be made to support the effective operation of the SPF and assist businesses to meet their obligations. This section outlines Treasury's initial positions on SPF rules that are considered necessary to support the effective implementation of the SPF from the time of commencement. Other SPF rules may be added over time and as needed.

This section does not discuss SPF rules relating to redress (discussed in relation to Principle 6: Respond) or intelligence sharing under the Principle 4: Report (which will be addressed through a separate consultation in 2026).

Definition of a scam

The definition of a scam in the SPF is broad to enable a range of conduct to be captured and provide flexibility as scammers evolve their practices. The definition of a scam requires several key elements, including:

- there is a direct or indirect attempt (whether or not successful)¹⁶ to engage an SPF consumer of a regulated service,
- where it would be reasonable to conclude that the attempt involves deception, and
- would cause loss or harm to the SPF consumer or their associates.

The definition is not intended to capture circumstances that do not involve deceiving a consumer into performing an action that results in loss or harm.


The SPF rules may prescribe attempts to engage an SPF consumer that are not 'scams' for the purposes of the SPF. Such limits on the definition of a scam may improve clarity for businesses and SPF consumers. In some cases, it may be appropriate to apply exclusions where other laws would be better placed to address activity. The rules could be used to exclude the following activities, that in isolation, would not meet the definition of a scam:

- Certain types of cybercrime that do not involve consumer interaction, such as identity theft or using information obtained as part of a data breach or hack for criminal purposes.
- Certain criminal conduct regulated under anti-money laundering and counter-terrorism financing (AML/CTF) legislation, such as disguising illicit funds to enable serious crimes like terrorism, drug trafficking and child exploitation.
- Misleading and deceptive conduct in trade or commerce where disputes relate to the buying and selling of goods and services.¹⁷

Submissions to previous consultations suggested clarifying that specific scam types are captured within the definition (such as scams enabled by artificial intelligence and phishing scams). Treasury considers that the current definition, which is technology-neutral, remains capable of capturing both established and emerging scam typologies, provided the definition is met.

16 As noted in the [Revised Explanatory Memorandum](#) of the Scams Prevention Framework Bill 2025, the meaning of scam in the SPF captures both successful scams which have caused loss or harm to an SPF consumer and scam attempts which have not yet resulted in loss or harm to an SPF consumer (para 1.62).

17 For example, see the [Revised Explanatory Memorandum](#) of the Scams Prevention Framework Bill 2025 (para 1.81).



Where appropriate, future regulatory guidance could provide further clarity and support consistent application.

Definition of SPF consumer

The definition of a 'SPF consumer' of a regulated service includes:¹⁸

- A natural person or small business operator who is provided or purportedly provided the service in Australia, or a natural person who is ordinarily resident in Australia and is/may be provided the service outside of Australia by a regulated entity that satisfies residency requirements.
- A small business operator under the SPF has less than 100 employees, has annual turnover less than \$10 million and has a principal place of business in Australia.

Previous stakeholder feedback to earlier consultations raised concerns with the small business definition. Treasury welcomes stakeholder views and supporting information on whether the definition of 'small business operator' meets the objectives of the SPF, as well as what other exceptions to the definition are required.

Designation exceptions

The SPF rules can also operate to exclude the application of specified SPF provisions for certain businesses or services within a designated sector.¹⁹ Draft designation instruments for the banking, telecommunications and digital platform sectors have been released to accompany this paper. Stakeholder feedback on the draft designation instruments will help inform whether designation exceptions are required to ensure the designation instruments operate as intended.

Matters necessary or convenient for carrying out the SPF

The SPF also provides the ability to make rules necessary or convenient for carrying out the SPF.²⁰ Treasury proposes to make rules requiring all businesses to keep records in Australia (such as those records stipulated under [Principle 1: Governance](#) and any other additional record keeping requirements). Keeping records locally will help ensure relevant information is accessible to regulators and will assist with compliance and enforcement efforts.

18 Section 58A of the of the Competition and Consumer Act 2010

19 Subsection s58AD(4) of the of the Competition and Consumer Act 2010

20 Section s58GE of the of the Competition and Consumer Act 2010



Consultation questions

22. What guardrails, if any, are needed in considering potential exceptions to the definition of a scam?
23. What other exceptions to the definition of a scam would be appropriate to consider? In your response, please provide supporting evidence.
24. What other exceptions to the definition of a SPF consumer should be considered? In your response, please provide supporting evidence.
25. What other SPF rules should be considered and developed as a priority to support the effective operation of the SPF and provide clarity for stakeholders?

Appendix A: List of proposed codes and rules obligations

Tables A to C list indicative code obligations for regulated entities in the 3 initial industry sectors to meet the principles and anticipated policy outcomes under the Scams Prevention Framework. As stated in the Introduction, these reflect preliminary views. Obligations for Principle 5: Report will be developed with consultation at a later date.

Table A: Proposed obligations for all regulated sectors

Governance	<ul style="list-style-type: none"> Businesses must embed responsibility for scam prevention within their governance frameworks including strategic risk management and oversight.
Prevent	<ul style="list-style-type: none"> Businesses must have systems in place to identify vulnerabilities that are being or could be exploited by scammers on their services. Businesses must require multi-factor authentication for log in attempts from new devices. Businesses must provide accessible information to consumers about scam risks on their services, including a scam awareness webpage. This should include easy referral to public resources, such as scamwatch.com.au. Businesses must take effective steps to protect their brand from being used in scams, including on other communication platforms, such as social media and online search services. Businesses must provide scam prevention training to relevant staff, tailored to their roles. For scam response roles or customer-facing roles, businesses must have processes in place to ensure staff understand emerging scam trends.
Detect	<ul style="list-style-type: none"> Businesses must investigate actionable scam intelligence, including systems or processes in place to gather specific data to assist potential disruption activities. Businesses must have systems in place to identify consumers impacted or potentially impacted by a scam.

Disrupt	<ul style="list-style-type: none"> • Businesses must alert customers as soon as practicable where there is a risk they are involved in an ongoing scam.²¹ • Businesses must issue targeted scam alerts to consumers where there is a reasonable suspicion a specific scam threat may impact them. <ul style="list-style-type: none"> – Scam alerts must include information on how to report the scam and access support services. • Businesses restore disrupted services where investigations found that the relevant activity was not a scam. • Businesses must notify consumers impacted by disruption activities, including how the disruption affects them.
Respond	<p>Reporting a scam</p> <ul style="list-style-type: none"> • In addition to the obligations set out in the primary law, all sectors must: <ul style="list-style-type: none"> – publish information on how to make an urgent report about a scam that may be in progress. – accept scam reports 24/7 and free of charge. – provide an acknowledgement of a scam report as soon as practicable but within 24 hours of receiving the report. The acknowledgement must provide information about how to escalate the report to a complaint for IDR if the consumer is dissatisfied with how the report is handled. <p>IDR</p> <ul style="list-style-type: none"> • In addition to the obligations set out in the primary law, all sectors must: <ul style="list-style-type: none"> – make information about how to make complaints publicly available and offer accessible communication options that recognise consumer circumstances. – accept scam complaints 24/7 and free of charge. – provide an acknowledgement of the complaint within 24 hours or as soon as practicable. – facilitate a no wrong door approach to complaints (allowing a consumer to make a complaint to any business involved in the scam chain). – issue any proposed remedy within 30 calendar days of receiving an SPF complaint. – respond to requests for information from other regulated entities assisting a consumer with the same scam complaint in a timely way.

²¹ Businesses subject to obligations under Anti-Money Laundering and Counter-Terrorism Financing Act 2006 will need to consider interactions with that regime.

Respond

- Statements of compliance must:
 - be provided to a consumer in writing no later than 30 calendar days after the business receives a scam complaint.
 - set out what specific steps the business took to comply with the SPF in relation to the consumer's scam.
 - describe the remedy provided to the consumer or the reasons why a remedy has not been offered.
 - explain the consumer's rights and processes for escalating the matter to EDR if they are dissatisfied with the IDR outcome.
 - be signed off by a manager with responsibility and oversight of the matters contained in the complaint, as identified in the business' governance policy and procedures.
- If a business resolves the complaint to the consumer's satisfaction within 5 calendar days of receiving the complaint, no statement of compliance will be required.

Guidance in rules for businesses working together and apportioning compensation

- Businesses assisting the same customer with the same scam complaint should work together to resolve the complaint in a manner that minimises the burden of the complaints process on the consumer (for example, by facilitating a single front door for complaints) (see the next section).
- Where more than one business provides a statement of compliance to the effect that it has not complied with a relevant SPF obligation, the businesses should collectively offer redress that reasonably represents the consumer's losses.
- As a default, each entity offering to compensate a consumer for a multi-party scam loss should pay an equal share of compensation. Where one entity is clearly more or less culpable for the loss and agreement is reached between businesses within IDR timeframes, other apportionment arrangements may be agreed.

Table B: Proposed obligations for the banking sector

Prevent	<ul style="list-style-type: none"> • Banks must provide targeted warnings about scam risks to customers before they make high-risk payments. • Banks must use name-checking technology to confirm a payee's details match those provided by the payer. • Banks must have systems in place to verify the identity of their customers and to understand the nature of their transactions.
Detect	<ul style="list-style-type: none"> • Banks must have systems in place to monitor all transactions for suspicious activity that might be a scam and identify actionable scam intelligence. • Banks must have systems in place identify consumers that have made a payment to a known scam account. This includes identifying customers at another bank where the bank identifies a home account that is suspected of receiving scam proceeds.
Disrupt	<ul style="list-style-type: none"> • Banks must close – and block payments to and from – accounts controlled by scammers (where the account owner is either the scammer or complicit in the scam) or freeze the account and return it to the account owner (where the account access was stolen from an innocent party). • Banks must take reasonable and proportionate measures to disrupt potential scam activity. This may include interim or permanent disrupt actions, such as: <ul style="list-style-type: none"> – issuing a payment recall request where it has reasonable that a payment may have been made to a scammer. Banks must immediately act upon payment recall requests made by other banks, – suspending or freezing an account suspected of being used by a scammer while the bank investigates, – enabling customers to instantly freeze accounts to block outgoing payments when they are concerned they have been compromised by scammers, such as through an in-app function or a dedicated priority call centre.

Table C: Proposed obligations for the telecommunications sector

Prevent	<ul style="list-style-type: none"> • Carriage service providers must verify a customer has a legitimate use case before offering certain services. This includes confirming a customer has a legitimate use case to originate calls using a number not allocated to the originating carriage service provider.
Detect	<ul style="list-style-type: none"> • Telcos must have processes and systems in place to analyse traffic (calls and messages) for patterns or indicators of a scam. These could include a combination of: <ul style="list-style-type: none"> – calls or messages from numbers already under investigation, – patterns of behaviours such as sending mass communications from a new number or IMEI, – unusual increases in calls for a number, – repeated short call durations, – calls from invalid numbers or numbers on do not originate lists. • Telcos must have systems in place to identify consumers who received scam calls or short messages, with a focus on consumers who have engaged with the suspected scammer via returning a text message or speaking with them on the phone.
Disrupt	<ul style="list-style-type: none"> • Carriage service providers must block calls and messages from or to calling line identifiers (CLI) confirmed to be a scam following investigation of actionable scam intelligence. • Carriage service providers must temporarily withdraw CLI from calls and messages from or to phone numbers which are subject of an investigation of actionable scam intelligence.

Table D: Proposed obligations for the digital platforms (social media, search engine and instant messaging) sector

Prevent	<ul style="list-style-type: none"> • Digital platforms must verify advertisers hold appropriate licences to advertise high-risk products, such as financial services and healthcare products. • Digital platforms must provide warnings to users in high-risk circumstances, such as receiving messages from unconnected accounts, or messages requesting financial details. • Digital platforms must have authentication processes to ensure accounts are legitimate, including comparing new account details against previously banned accounts, and requiring business users and advertisers to provide appropriate identification.
Detect	<ul style="list-style-type: none"> • Digital platforms must have systems in place to proactively detect accounts, content, messages and advertisements suspected of being associated with scams. • Digital platforms must identify, notify and warn: <ul style="list-style-type: none"> – owners of accounts exhibiting behaviour associated with account compromise, – consumers who have communicated with accounts associated with scam activity or interacted with content or advertisements associated with scam activity.
Disrupt	<ul style="list-style-type: none"> • Digital platforms must permanently ban users and advertisers found to have been operating scams on their services and prevent them from creating new accounts. • Digital platforms must permanently remove or delist content (for example, social media posts or videos) and advertising linked to a scam and prevent future distribution. • Digital platforms must notify users they identify as having been potentially impacted by a scam (for example, users who have interacted with content since removed for scams) and warn users in real time if they are contacted by accounts under investigation for scam activity. • Digital platforms must take reasonable and proportionate measures to disrupt potential scam activity under investigation. This may include interim measures to: <ul style="list-style-type: none"> – limit visibility of content and advertising being investigated for scam activity, – publicly flagging content and messages being investigated for scam activity, – suspending all display of advertising being investigated for scam activity.

Appendix B: Consultation questions

Overarching policy considerations

1. Are there other policy considerations that should be taken into account when developing rules and code obligations?
2. What should be included in codes to help businesses evaluate the level of risk posed by scams, and what factors should they consider when making these assessments?
3. Should consumers be able to opt out of scam prevention measures?
4. What safeguards, if any, should be in place to protect consumers with a higher risk of being scammed?

Principle 1: Governance

5. What oversight and reporting mechanisms are in place to keep the board or senior executives informed of scam-related risks and incidents?
6. What data, including complaints data, is useful to help develop and maintain policies and procedures?
7. Should other governance obligations be considered for inclusion in sector codes?

Principle 2: Prevent

8. Would codes benefit from specific consumer verification requirements?
9. How can businesses ensure scam education efforts are inclusive and accessible to diverse consumer groups, including those with limited digital literacy or language barriers?
10. What additional protections should be in place for consumers who may be at higher risk of being scammed, in a way that is proportionate, effective and non-exclusionary?

Principle 3: Detect

11. What challenges do businesses face when investigating scams, particularly in verifying intelligence or assessing risk levels, and how might these challenges be accommodated in setting SPF code obligations?

Principle 5: Disrupt

12. What criteria should be used to determine when disruption actions are deemed necessary (for example, freezing accounts, removing content)?
13. What safeguards should be in place to ensure disruption actions do not disproportionately impact legitimate users, particularly vulnerable cohorts and small business users?
14. What is the most effective and practical way for businesses to alert customers as soon as practicable when there is a risk they are involved in an ongoing scam?

Principle 6: Respond

15. How can SPF rules and codes encourage cooperation and timeliness in multi-party disputes?
16. How should the SPF rules and codes relating to IDR manage or reflect disparate industry standards?
17. If SPF codes allow consumers to opt out of certain frictions for certain transactions, how should that impact their right to redress?
18. Should any additional information or evidence be included in the statement of compliance?
19. What roles should non-financial remedies or compensation for non-financial harm play in determining appropriate redress?
20. Should the proposed SPF rules and code obligations better facilitate industry developing innovative approaches to fast-track resolution of high-volume, low-value scam losses?
21. Should any code obligations be made to help ensure the external dispute resolution scheme operates effectively?

Issues for the SPF Rules

22. What guardrails, if any, are needed in considering potential exceptions to the definition of a scam?
23. What other exceptions to the definition of a scam would be appropriate to consider? In your response, please provide supporting evidence.
24. What other exceptions to the definition of a SPF consumer should be considered? In your response, please provide supporting evidence.
25. What other SPF rules should be considered and developed as a priority to support the effective operation of the SPF and provide clarity for stakeholders?

Compliance costs

26. What additional compliance costs will businesses in designated sectors incur to meet the indicative code obligations proposed in this paper?

What is the type and quantum of these costs for individual businesses where estimable, and are they one-off or ongoing? Is additional expenditure beyond delivery of these obligations expected, such as for staffing, system upgrades or training to achieve readiness for the SPF?

Appendix C: List of matters for SPF codes and SPF rules

Matters that can be included in the SPF sector codes:

- *Governance* – Matters for inclusion in and factors to consider in development of policies and procedures
- *Prevent* – Describing reasonable steps for prevent obligations, requirements to identify SPF consumers at risk or with a higher risk of being targeted and requirements to give information to at risk consumers
- *Detect* – Describing reasonable steps and time for detect obligations
- *Disrupt* – Describing reasonable steps or time to disrupt and requirements to provide information to consumers about disruption activities
- *Respond* – Conditions for a consumer reporting mechanism, conditions for an IDR mechanism and obligations that must be met to an EDR scheme
- Related or incidental matters.

Matters that can be included in SPF rules:

- Exceptions to sector designations
- Exceptions to the definition of a scam or consumer
- *Governance* – Performance metrics and targets, and additional activities for record keeping
- *Report* – Reporting of actionable scam intelligence and prescription of a scheme to authorise third parties
- *Disrupt* – Reporting of investigation outcomes
- *Respond* – Details for the statement of compliance and internal dispute resolution
- SPF regulator arrangements and information SPF regulators are not required to disclose
- Other matters necessary or convenient for carrying out the SPF.