
From: s 47F @afca.org.au>
Sent: Wednesday, 16 October 2024 11:36 AM
To: Robertson, Belinda
Cc: s 47F
Subject: AFCA briefing - liability framework s 22
Attachments: 20241014 - Brief to Treasury - SPF - Liability framework.pdf; s 22
s 22

Categories: Maybe

Hi Belinda

Hope you are well.

s 47F mentioned that you recently met with him to discuss the Scams Prevention Framework.

We have recently responded to queries from Treasury on the draft legislation, which may be of interest to you as well. I attach our Brief to Treasury for your information. In our brief we explore how remediation programs (which is a current regulatory tool and has been used previously) may work to resolve scam related matters before they reach EDR.

s 22

Please feel free to reach out if you have any queries.

Kind regards

s 47F

s 47F

s 47F

| Free Call 1800 931 678



AFCA acknowledges the traditional owners of country throughout Australia and their continuing connection to land, culture and community.
We pay our respects to elders past, present and future.

IMPORTANT The contents of this email (including any attachments) are confidential and may contain privileged information. Any unauthorised use of the contents is expressly prohibited. If you have received this email in error, please notify us immediately by Telephone: 1800 931 678 (local call) or by email and then destroy the email and any attachments or documents. Our privacy policy is available on our website.

To	s 47F Scams Taskforce
Cc:	s 47F
From	AFCA
Date	14 October 2024
Subject	Scams Prevention Framework (SPF): Remediation and Redress

Confidential – not for external communication

Purpose

On 9 October, Treasury requested AFCA's views on provisions that deal with proportionate liability in misleading and deceptive conduct in [Part VIA of the Competition and Consumer Act](#), and under [Part 7.10 Division 2A of the Corporations Act](#) as potentially relevant for inclusion in the primary legislation that may also address circumstances where consumer negligence is relevant.

s 22

s 22

Policy outcomes from SPF framework

AFCA has reflected on the policy objectives of the SPF informed by the Minister's comments on 11 October 2024 where he articulated his key priorities and the outcomes he is seeking from the SPF, specifically a:

- focus on prevention and upstream interventions on industrial scam activity
- priority to incentivise the right behaviour by in-scope sector firms
- focus on timeliness, efficiency and accountability

- need for specific and legally binding obligations supported by clear regulatory responsibilities.

Applying this outcomes lens (and informed by feedback offered in submissions), AFCA offers the following observations on the Respond limb of the SPF to ensure these objectives are met when losses have occurred.

Systemic issues and remediation¹

AFCA has deep experience of systemic issues and remediation work over many years. This has resulted in remediation outcomes for consumers at scale.² Critically, for the SPF, this includes outcomes for consumers who may have been affected by a misconduct or other firm failure or breach but who not lodged a complaint.

This work has resulted in many millions of dollars in compensation to consumers (and other remedial activities by firms) in a timely, efficient and cost-effective way that avoids putting *all* affected consumers through a complaints process.

We also note that remediation was a successful regulatory tool used to significant and successful effect after the Hayne Royal Commission to provide \$billions in redress to Australian consumers affected by misconduct. Importantly, it shifts the onus to the firm (not the customer) to provide a simple, accessible pathway to customer redress where misconduct or other failure affecting a group of consumers, is identified.

Under the proposed SPF, the ACCC as the primary regulator will have close to real-time intelligence about scams which they will be sharing with firms to meet their prevent, detect, disrupt and respond obligations, often ahead of consumer complaints.

A directions or consumer redress power

We consider there is an opportunity to materially enhance the SPF—in line with the Minister’s expectations—by empowering the primary regulator to direct firms to remediate where it has formed a view that a firm(s) conduct under the SPF has contributed to losses and where remediation for affected consumers, is appropriate.

Intervening in this way, may circumvent the need for *all* affected consumers to lodge a complaint to IDR or to AFCA, to receive an outcome. It may significantly enhance the efficiency and responsiveness of the SPF and the consumer experience.

[ASIC Regulatory Guide 277: Consumer Remediation](#) (RG 277) provides a streamlined and clear consumer-centred remediation framework for licensees to apply

¹ Note in Row 50 of AFCA’s officer level feedback to Treasury we noted that Court ordered remediations may be appropriate in certain circumstances and suggested consideration of settings in ASIC RG 277.

² For example, in FY 23-24, AFCA investigated and addressed systemic issues, resulting in remediation for **159,051 consumers** and small businesses and secured **\$44,706,897 in remediation and refunds for consumers**.

where they have engaged in *misconduct or other failure* that may have caused consumer loss. This may present a useful remediation model for SPF firms.

Legislative design:

- Include in the primary law—under the Response Principle—a specific obligation that in scope firms have an obligation to remediate where a breach or other failure under the SPF has occurred (e.g. new 58 BZF)
- Introduce a specific power for the ACCC to direct a firm or firms to remediate in appropriate circumstances (e.g. in line with the liability rules or formulas in the Code (or specific rules made by the ACCC as relevant to the fact scenario)
- Provide that Codes include rules / formulas that can be applied in a broad-based remediation (at scale) and at IDR/ AFCA in an individual or class of complaints.

s 22

Scams occur at scale: potential remedial tools to deliver scalable outcomes

Because of the industrial scale of much scam activity, there are limits to the ‘individual complaint’ model of the response limb of the SPF, however, that model remains essential for individual complaints where the wrongdoing is not systemic. In cases, where the misconduct or failure is systemic, the application of a remediation lens supported by appropriate regulatory powers, may more efficiently and effectively deliver the SPF policy outcome.

We note that financial services licensees (future regulated firms under the SPF) have general obligations which include compensation and remediation under ss912A and 912B of the Corporations Act. As noted above, [ASIC Regulatory Guide 277: Consumer Remediation](#) (RG 277) may present a useful remediation model for SPF firms.

In addition to a directions power³, another potential model is the Consumer Redress power used by the Financial Conduct Authority (FCA) in the UK that may warrant consideration in the SPF context.⁴

Provision for proportionate liability rules in the Code

As AFCA understands the policy intent under the SPF, which is to apply across multiple sectors, the ability to apportion liability as and between firms is preferred.

To achieve this outcome for the SPF, the **SPF Bill needs to expressly provide for the apportionment of liability**, which it currently does not.

The decision-making criteria in the AFCA Rules (for non-superannuation complaints) includes having regard to the law, industry codes and standards etc. Each of the limbs of AFCA’s decision-making test informs how we understand and apply our fairness jurisdiction in determining what is *fair in all the circumstances* of a particular complaint. In deciding SPF complaints that may involve apportioning liability as and between different sectors, statutory authority for apportionment in the primary law would be necessary.

In addition to express provision for apportionment in the primary law, further policy options for the development of applicable rules include that the:

³ See for example, ASIC directions powers under the Corporations Act to issue regulatory requirements (including by legislative instrument) to AFCA relating to compliance with the mandatory requirements under s1051 or to direct AFCA to increase limits on the value of claims that may be made or remedies that may be determined etc. See ss 1052C and ss1052B and BA.

⁴ See s404 of the UK Financial Services and Markets Act 2000 which provides that if the regulator identifies that there may have been a widespread or regular failure by relevant firms to comply with requirements applicable to the carrying on by them of any activity; (b) it appears to it that, as a result, consumers have suffered (or may suffer) loss or damage in respect of which, if they brought legal proceedings, a remedy or relief would be available in the proceedings; and (c) it considers that it is desirable to make rules for the purpose of securing that redress is made to the consumers in respect of the failure (having regard to other ways in which consumers may obtain redress). [CONRED 1.8 Imposing a consumer redress scheme on a firm under section 404F\(7\) of the Act - FCA Handbook](#)

- bill could set up the apportionment rules / formulas in their entirety, or
- bill may provide for the development of apportionment rules/ formulas to be contained in the Code(s) to set out the detail as to how they apply in practice
- Code formulas cap liability up to certain caps (see attached slides).

We consider that the models in the Competition and Consumer Act (CCA) and Corporations Act (CA) referenced by Treasury are appropriate models for consideration. We expect Treasury is also engaging with ASIC and the ACCC as to their views as to the operation of these provisions in legislation they administer.

Consistency: Code development

Applying a whole of sector outcomes lens, we consider it essential that:

- the power to determine the liability regime is located in the bill in such a way as to ensure that it applies across all Codes
- relevant codes have **identical settings for apportionable claims under the SPF** so that IDR, AFCA and any remediation process can produce consistent outcomes in making a consumer 'whole' following scam losses.

To be effective, we would expect the liability regime (Code contents) will need to be quite prescriptive as to how liability is adjusted between the parties again so there is consistency, and the regime is workable.

One possible option to ensure such consistency is to have a specific delegated instrument solely for the purposes of setting consistent liability arrangements under the Codes that applies across all Codes. Such an approach will ensure consistency and mean only one instrument relating to liability will need modification where new sectors come on board, supporting the effective future proofing of the SPF.

Attachment B – Policy issues and recommendations

Changes to policy			
Key feature	Issue raised	Treasury recommendation	Minister's decision
s 22			

Changes to policy			
Key feature	Issue raised	Treasury recommendation	Minister's decision
s 22			
Dispute resolution	<p><u>Operation of IDR</u></p> <p>Both consumer and industry stakeholders raised concerns about the lack of clarity on IDR arrangements in primary law, particularly where multiple entities are involved in a scam.</p> <p>Feedback highlighted the importance of co-operation between regulated entities involved in the same scam, in order to support efficient IDR arrangements that avoids the consumer going through multiple IDR processes and inundation of complaints at EDR.</p>	<p>Treasury recommends that sector codes require regulated entities to engage and cooperate with one another to facilitate the resolution of disputes prior to escalation to EDR. Ahead of this, further stakeholder consultation will be undertaken on the operation of dispute resolution arrangements.</p> <p>The explanatory memorandum will set out the policy intent that consumers should not be bounced between multiple IDR processes, and that the sector codes will set out consumer-centric and prescriptive IDR requirements.</p>	<p>Agreed</p> <p>To discuss</p>
	<p><u>Statutory review</u></p> <p>Consumer groups submitted that the dispute resolution arrangements should be subject to statutory review.</p>	<p>Treasury recommends incorporating a requirement for a statutory review of the dispute resolution arrangements under the SPF.</p> <p>Subject to drafting, the provision will provide that the Minister must cause a review within 3 years of the commencement of the first sector code, allowing for flexibility to start the review earlier if there are known issues. The report of the review will be tabled in Parliament.</p>	<p>Agreed</p> <p>To discuss</p>
	<p><u>Proportionate liability and liability guidelines</u></p> <p>Industry stakeholders strongly sought clarity around how liability may be apportioned between regulated entities where regulated entities have breached SPF obligations. This is relevant where multiple regulated entities have breached SPF obligations and have caused or contributed to loss or harm arising from a scam. This could include for example, a sending bank, a receiving bank, a telecommunication service provider, and a digital platform.</p> <p>Many stakeholders (including AFCA) have also sought specific liability apportionment guidelines to be provided in the framework.</p>	<p>Treasury recommends provisions relating to actions for damages to allow for proportionate liability, consistent with those set out in the CCA and Corporations Act, so that a court can apportion liability between regulated entities having regard to the extent to which an entity is responsibility for the damage or loss. In apportioning liability, the court will consider the actions of the consumer and any unregulated entities involved.</p> <p>This means that regulated entities' liability for compensation under the SPF may be less than 100% in circumstances where regulated entities are not fully and wholly causing or contributing to the scam loss (i.e. unregulated entities involved and/or consumer has been contributorily negligent). This approach is consistent with other proportionate liability frameworks.</p> <p>On liability guidelines, Treasury is seeking legal advice on whether some form of liability guidance in relation to IDR and EDR can be provided under subordinate legislation, if desired. This will create flexibility to issue guidelines without mandating it, given the policy intent to date has been that liability is apportioned on a case-by-case basis.</p>	<p>Agreed</p> <p>To discuss</p>
	<p><u>Remediation</u></p> <p>ASIC has suggested that a regulator should have the ability to seek damages for scam losses suffered by consumers in court, consistent with similar provisions in the ASIC Act.</p>	<p>Treasury recommends a regulator having the ability to seek damages on behalf of scam victims, where a regulator is taking legal action against a regulated entity.</p>	<p>Agreed</p> <p>To discuss</p>

Changes to policy			
Key feature	Issue raised	Treasury recommendation	Minister's decision
	<p>AFCA suggested that:</p> <ul style="list-style-type: none">regulated entities should be subject to obligations to actively identify and remediate consumers in line with pre-determined liability rules where a breach in obligations under the SPF is identified that impacts a number of their customers.the ACCC have the specific power to direct a regulated entity to remediate in line with pre-determined liability rules in circumstances where there is evidence that regulated entities have caused harm and not provided sufficient remediation for consumers.	<p>Treasury does not recommend a requirement for regulated entities to remediate where the entities have self-identified a breach that may lead to scam harm for their customers or where the regulator has directed the entity to undertake remediation of this kind, for a number of reasons:</p> <ul style="list-style-type: none">would be difficult to operationalise without pre-determined liability rules (the viability of which is subject to pending legal advice).it is unclear how this will operate in a scam context where multiple regulated entities are involved who may not always be aware if a person was involved in a specific scam, making it difficult for regulated entities to manage and quantify the risk and impose considerable and unknown costs on regulated entities.may have the unintended effect that regulated entities limit information sharing to avoid triggering liability.this would involve a significant change in policy position and would require further consultation with stakeholders so could be considered as part of the statutory review of dispute resolution arrangements.	

s 22

UKScams Prevention Framework Bill 2024

Q&As

Contents

1.	What is the Scams Prevention Framework?	2
2.	Why is this legislation needed?	2
3.	What is the benefit to the Australian community?	3
s 22		
10.	How will the Framework protect consumers?	6
11.	What type of scams will this legislation address?	6
s 22		
14.	Why is AFCA the EDR scheme rather than the TIO or another body?	8
15.	Will consumers get their money back if they are a victim of a scam?	8
16.	How will liability be apportioned between entities?	8
17.	Why hasn't the UK's mandatory bank reimbursement model been adopted in the SPF?	9
18.	If an entity breaches only one obligation under the Framework, will they be penalised?	9
19.	Will victims be compensated for scams that occurred before the SPF come into effect? ...	10
20.	When will more sectors be designated?	10
21.	How will the SPF interact with existing industry codes?	10
s 22		

1. What is the Scams Prevention Framework?

s 22

- The SPF will require regulated entities to have dispute resolution processes in place to deal with consumer complaints. A regulated entity may be responsible for providing compensation to a scam victim where that entity has not met its obligations under the SPF. That responsibility may be shared between multiple regulated entities where more than one entity has not met its obligations in relation to a particular scam.

2. Why is this legislation needed?

s 22


s 22



- The SPF establishes clear, consistent roles and responsibilities for the private sector to ensure scammers do not exploit vulnerabilities in the ecosystem and also provides scam victims pathways to seek redress.

3. What is the benefit to the Australian community?

s 22



The SPF also mandates dispute resolution arrangements that will improve the way businesses respond to affected consumers and strengthen redress pathways.

s 22



10. How will the Framework protect consumers?

- Consumers can expect regulated businesses that provide services to them to have anti-scam protections in place and provide accessible means to report potential scams, as well as access to adequate support when they are affected by a scam.
- In addition to the obligations under the SPF to prevent, detect and disrupt scams, businesses must also take steps to provide consumers with:
 - information and warnings about observed scam activity and steps consumers can take to minimise the risks of harm using those services,
 - disclosure to consumers that have been affected by a scam in a specified timeframe, including support on how to prevent further harm,
 - accessible mechanisms to provide reports about activity that is or may be a scam that are easy to locate and use,
 - accessible and transparent internal dispute resolution processes and the ability to escalate their complaint to an external dispute resolution (EDR) scheme.

11. What type of scams will this legislation address?

- A scam is defined as conduct that aims to deceive a consumer into facilitating an action, such as providing personal information, or making a payment.
- The legislation will provide protections from scam activity, whether or not it is successful in causing harm to a consumer.

- Scams are distinguished from other types of crime as the interactions between the consumer and the scammer lead to the harm.

s 22



14. Why is AFCA the EDR scheme rather than the TIO or another body?

- Leveraging existing EDR infrastructure and expertise is essential to ensure a single scheme can be in place from the commencement of sector codes under the SPF. This approach is important so that there is a single door for consumers to raise complaints, and have them resolved.
- As scams relate to economic harm and often include financial losses by the consumer, AFCA, the largest existing EDR body among the initial sectors, is the most appropriate single EDR body to address scam complaints regarding banks, telecommunications service providers and certain digital platforms.
- AFCA has experience in resolving scam-related complaints relating to the financial sector, and resolved more than 10,000 scams complaints in 2023-24.
- AFCA will work with the Telecommunications Industry Ombudsman (TIO) to ensure that there is an effective, holistic and consumer-centric complaints-handling system in place.

15. Will consumers get their money back if they are a victim of a scam?

- Entities with SPF obligations may need to compensate scam victims for any loss or damage that those entities are responsible for where they have not met their SPF obligations. A scam victim should lodge a complaint through a regulated entity's internal dispute resolution mechanism in the first instance to seek compensation where an entity has not met its obligations.

16. How will liability be apportioned between entities?

- Liability of regulated entities will be linked to whether there has been a breach of obligations under the SPF, and the extent of those breaches. Given the diverse nature of scams, liability is likely to vary in different circumstances.
- Under the SPF, the Minister has the power to provide guidance on how to apportion liability between multiple regulated entities that have breached their SPF obligations in relation to a particular scam.
- Regulated entities dealing with a complaint at internal dispute resolution must have regard to the any guidelines prescribed for apportioning any liability.

17. Why hasn't the UK's mandatory bank reimbursement model been adopted in the SPF?

- The conduct of a scam can involve interactions between a consumer and a scammer across multiple platforms and services. The multi-sector approach of the SPF recognises the need for stronger actions and interventions to protect consumers by businesses across the entire life cycle of scam activity.
- Under the SPF, businesses in the scams ecosystem each have responsibilities to address scam activity on their platforms and services; and where they do not meet their obligations can be liable for compensation to a consumer. Banks have responsibilities to address scams within the scope of the services they provide to consumers.
- A mandatory presumption of bank reimbursement for scam transactions allocates liabilities for failing to address scams to banks alone. It does not immediately incentivise actions to address the upstream sources of scam activity in the economy. The SPF creates strong incentives at each stage in the scam chain for businesses to take effective action, to minimise the risk of penalties and related liability for consumer compensation.
- Although banks may improve their practices to minimise their liabilities, a reimbursement model does not set specific or proactive standards on how businesses should improve their policies and procedures to address scams.
- The Government will undertake consultation on the design of the dispute resolution model in 2025 to ensure delivery of a consumer-centric complaints process for scams.

18. If an entity breaches only one obligation under the Framework, will they be penalised?

- Regulators have a range of tools to enable them to respond to breaches of SPF obligations in a proportionate way. These include notices, directions, and orders to take appropriate steps remedy loss or harm caused by a breach.
- Breaches of the SPF are subject to a civil penalty regime, where the quantum of any monetary penalties will be proportionate to the nature of the breach.

These include up to a maximum of \$50 million in penalties for breaches of obligations to prevent, detect, disrupt and respond to scams, and \$10 million for a failure to adhere to governance or report obligations or a sector-specific code.

19. Will victims be compensated for scams that occurred before the SPF come into effect?

- The SPF does not introduce avenues for consumers who have been affected by a scam prior to legislation to seek compensation from a regulated business. This is not envisaged as retrospective compensation would penalise entities for actions occurring during a time that legislation was not in force.
- Businesses are entitled to have certainty that they are held by the legal standards of the day when they undertake trade in compliance with the law.

20. When will more sectors be designated?

- The SPF is a flexible framework that allows for additional sectors to be designated in response to new or emerging scam trends. It is important that all sectors which are shown to be used as a key means by which scammers harm consumers play a part in addressing scams on their platforms and services.
- As Government works to develop sector-specific codes for the three initially designated sectors, it will also consider the role of other industry sectors in the scams ecosystem and their potential for designation under the SPF.
- Superannuation, cryptocurrency, online marketplaces and other payment providers have been discussed by stakeholders as the next sectors that could be considered for designation under the SPF.

21. How will the SPF interact with existing industry codes?

- The Government recognises that parts of industry have committed to a range of voluntary measures to address scams, including the Scam-Safe Accord for banks, the Australian Online Scams Code for digital platforms.
- Telecommunications providers are already subject to mandatory requirements under the Reducing Scam Calls and SMS Code, which will be replaced by the SPF telecommunications code.

- The SPF aims to build upon existing industry codes and initiatives in introducing strong enforceable obligations and penalties. The Government will consult extensively with relevant industry sectors in 2025 during the development of designation instruments and sector codes.

s 22



From: s 47F
Sent: Wednesday, 4 December 2024 10:33 AM
To: Jones DLO
Subject: FW: FOR INFO: Treasury/ASIC QA - Treasury Laws Amendment Bill 2024: Scams Prevention Framework - QA by 10:00am Tuesday 5 November 2024
~~[SEC - OFFICIAL: Sensitive, ACCESS - Legislative Secrecy]~~
Attachments: 20241105 - SPF Bill - ASIC QA Documents.pdf
Follow Up Flag: Follow up
Flag Status: Flagged

~~OFFICIAL: Sensitive Legislative Secrecy~~

s 47F
Office of the Hon Stephen Jones MP
Assistant Treasurer and Minister for Financial Services

s 47F

I acknowledge the traditional owners of country throughout Australia, and their continuing connection to land, water, and community. I pay my respects to them and their cultures and to elders past and present.

~~OFFICIAL: Sensitive Legislative Secrecy~~


From: Jones DLO s 47E(d)
Sent: Tuesday, November 5, 2024 11:12 AM
To: s 47F @TREASURY.GOV.AU>
Cc: Jones DLO s 47E(d) Robertson, Belinda s 47F @TREASURY.GOV.AU>
Subject: FOR INFO: Treasury/ASIC QA - Treasury Laws Amendment Bill 2024: Scams Prevention Framework - QA by 10:00am Tuesday 5 November 2024 ~~[SEC - OFFICIAL: Sensitive, ACCESS - Legislative Secrecy]~~

~~OFFICIAL: Sensitive Legislative Secrecy~~

Hi s 47F

Please find attached ASIC's quality assurance advice re the scams leg. They have provided qualified assurance and raised some issues. I have asked Treasury to provide their advice on the attached (this is the standard process).

Cheers,
s 47F

s 47F Departmental Liaison Officer
Office of the Hon Stephen Jones MP
Assistant Treasurer and Minister for Financial Services
s 47F @treasury.gov.au
s 47F Parliament House, Canberra, ACT 2600
 LGBTIQ+ Ally

The Treasury acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, water and community. We pay our respects to them and their cultures and to elders both past and present.

~~OFFICIAL: Sensitive Legislative Secrecy~~

From: s 47F @TREASURY.GOV.AU>

Sent: Tuesday, November 5, 2024 10:38 AM

To: Jones DLO s 47E(d)

Cc: LD Legislation Coordination s 47E(d); s 47F

s 47F @TREASURY.GOV.AU>

Subject: FW: Treasury/ASIC QA - Treasury Laws Amendment Bill 2024: Scams Prevention Framework - QA by 10:00am Tuesday 5 November 2024 [SEC OFFICIAL: Sensitive, ACCESS Legislative Secrecy]

~~OFFICIAL: Sensitive Legislative Secrecy~~

Hi s 47F

It was great to chat this morning.

As requested, please see below confirmation of ASIC's QA that we've received this morning.

Happy to discuss.

Kind regards,

s 47F

Law Division

s 47F

The Treasury acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, water and community. We pay our respects to them and their cultures and to elders both past and present.

~~OFFICIAL: Sensitive Legislative Secrecy~~

From: s 47F @asic.gov.au>

Sent: Tuesday, November 5, 2024 10:01 AM

To: s 47F @TREASURY.GOV.AU>

Cc: LD Legislation Coordination s 47E(d) s 47F

s 47F @treasury.gov.au>; Sykes, Helen s 47F @treasury.gov.au>; White, Kate

s 47F @TREASURY.GOV.AU>; s 47F @TREASURY.GOV.AU>; s 47F

s 47F @TREASURY.GOV.AU>; s 47F @TREASURY.GOV.AU>; s 47F

s 47F @TREASURY.GOV.AU> s 47F @TREASURY.GOV.AU>; s 47F

s 47F @TREASURY.GOV.AU>; s 47F @TREASURY.GOV.AU>; s 47F

s 47F @treasury.gov.au>; s 47F @TREASURY.GOV.AU>; s 47F

s 47F @TREASURY.GOV.AU>; s 47F @TREASURY.GOV.AU>;

s 47F @TREASURY.GOV.AU>; s 47F @TREASURY.GOV.AU>;

s 47F @treasury.gov.au>; s 47F @asic.gov.au>; s 47F

s 47F @asic.gov.au>; s 47F @asic.gov.au>; s 47F

s 47F @asic.gov.au>; s 47F @asic.gov.au>

Subject: Treasury/ASIC QA - Treasury Laws Amendment Bill 2024: Scams Prevention Framework - QA by 10:00am
Tuesday 5 November 2024 [~~SEC-
OFFICIAL: Sensitive, ACCESS-
Legislative Secrecy~~]

You don't often get email from **s 47F** [@asic.gov.au](mailto:s 47F@asic.gov.au). [Learn why this is important](#)

~~OFFICIAL: Sensitive Legislative Secrecy~~

Hi **s 47F**

Please find **attached** ASIC's QA documents for the Treasury Laws Amendment Bill 2024: Scams Prevention Framework.

Kind regards

s 47F

s 47F

Senior Specialist, Scams
Enforcement & Compliance

Australian Securities and Investments Commission

Level 7, 120 Collins Street, Melbourne, 3000

s 47F

s 47F [@asic.gov.au](mailto:s 47F@asic.gov.au)



ASIC acknowledges the Traditional Owners of the lands and waters on which I live and work.
We pay respect to Elders past and present as the custodians of the world's oldest continuing cultures.



~~OFFICIAL: Sensitive Legislative Secrecy~~

From: **s 47F** [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>

Sent: Monday, November 4, 2024 12:08 PM

To: **s 47F** [@asic.gov.au](mailto:s 47F@asic.gov.au)>; **s 47F** [@asic.gov.au](mailto:s 47F@asic.gov.au)>; **s 47F**

s 47F [@asic.gov.au](mailto:s 47F@asic.gov.au)>; **s 47F** [@asic.gov.au](mailto:s 47F@asic.gov.au)>

Cc: LD Legislation Coordination **s 47E(d)** Robinson, Jessica

s 47F [@treasury.gov.au](mailto:s 47F@treasury.gov.au)>; Sykes, Helen **s 47F** [@treasury.gov.au](mailto:s 47F@treasury.gov.au)>; White, Kate

s 47F [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F** [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F**

s 47F [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F** [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F**

s 47F [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F** [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F**

s 47F [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F** [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F**

s 47F [@treasury.gov.au](mailto:s 47F@treasury.gov.au)>; **s 47F** [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F**

s 47F [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F** [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>;

s 47F [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>; **s 47F** [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>;

s 47F [@TREASURY.GOV.AU](mailto:s 47F@TREASURY.GOV.AU)>

Subject: Treasury/ASIC QA - Treasury Laws Amendment Bill 2024: Scams Prevention Framework - QA by 10:00am
Tuesday 5 November 2024 [~~SEC-
OFFICIAL: Sensitive, ACCESS-
Legislative Secrecy~~]

EXTERNAL EMAIL: Do not click any links or open any attachments unless you trust the sender and know the content is safe.

~~OFFICIAL: Sensitive Legislative Secrecy~~

Hi **s 47F**

As you may be aware we are now progressing with the Treasury Laws Amendment Bill 2024: Scams Prevention Framework for introduction on 7 November 2024 (Week 6 Spring 2024).

Please find attached the Draft Bill and EM. Note that the EM is still subject to a final editorial and formatting review.

Are you please able to review and provide ASIC's quality assurance by **10:00am Tuesday 5 November 2024?**

I apologise in advance for the very short turnaround on this, however please let me know if there are any issues.

Happy to discuss.

Kind regards,

s 47F

Law Division

s 47F

treasury.gov.au

Langton Crescent, Parkes ACT 2600

[Twitter](#) | [LinkedIn](#) | [Facebook](#)

The Treasury acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, water and community. We pay our respects to them and their cultures and to elders both past and present.

Please Note: The information contained in this e-mail message and any attached files may be confidential information and may also be the subject of legal professional privilege. If you are not the intended recipient, any use, disclosure or copying of this e-mail is unauthorised. If you have received this e-mail by error please notify the sender immediately by reply e-mail and delete all copies of this transmission together with any attachments.

~~OFFICIAL: Sensitive Legislative Secrecy~~

Please consider the environment before printing this document.

Information collected by ASIC may contain personal information. Please refer to our [Privacy Policy](#) for information about how we handle your personal information, your rights to seek access to and correct your personal information, and how to complain about breaches of your privacy by ASIC.

This e-mail and any attachments are intended for the addressee(s) only and may be confidential. They may contain legally privileged, copyright material or personal and /or confidential information. You should not read, copy, use or disclose the content without authorisation. If you have received this email in error, please notify the sender as soon as possible, delete the email and destroy any copies. This notice should not be removed.



ASIC
Australian Securities &
Investments Commission

FOI 3784
Document 7A

ASIC Sign Off

Quality assuring legislative proposals

Treasury Laws Amendment Bill 2024: Scams Prevention Framework

5 November 2024

ASIC has undertaken a quality assurance process in relation to the draft legislation and the Senior ASIC Officer provides the following statement:

s 22

2. Identified issues of concern have been raised with Treasury as soon as practicable. Issues that ASIC has raised with Treasury that remain unresolved are outlined in **Attachment A**.

Senior ASIC Officer:

s 47F

Senior Executive Leader, Enforcement & Compliance
ASIC

5 November 2024



ASIC
Australian Securities &
Investments Commission

FOI 3784
Document 7B

Attachment A – Issues Register

Treasury Laws Amendment Bill 2024: Scams Prevention Framework - Issues identified by ASIC

ASIC documented and raised a range of concerns with Treasury. Key unresolved issues are identified in the table below:

Issue	Summary	Resolved	History
s 22			

s 22

Effective dispute resolution under the SPF	<p>The draft Bill does not contain any express provisions regarding how liability for consumer compensation is to be determined, or how liability is to be apportioned where multiple regulated entities are at fault.</p> <p>The draft Bill enables the SPF rules (a legislative instrument to be made by the Minister) to provide for mandatory processes and liability apportionment settings to apply during internal dispute resolution (IDR).</p>	No	<p>Raised by ASIC with Treasury:</p> <ul style="list-style-type: none">- in ASIC's 2 February 2024 submission in response to Treasury's consultation paper <i>Scams – mandatory industry codes</i>;
--	---	----	---

	<p>However, these processes and settings have not yet been developed, and the timing and content of the SPF rules is currently unknown.</p> <p>The absence of liability settings is likely to have material adverse implications for the effectiveness of IDR, as well as for external dispute resolution by AFCA, under the SPF, impacting the ability for consumers to readily access redress where a regulated entity has breached their SPF obligations in line with the policy intent.</p> <p>This may also have implications for ASIC's oversight function in respect of the effective operation of the dispute resolution system for financial firms, which includes financial firms' IDR processes as well as oversight of AFCA.</p>		<ul style="list-style-type: none"> - by email on 22 April, 3 May and 14 August 2024; and - in discussions on 16 August, 5 September, 30 September and 30 October 2024.
s 22			

Assistant Treasurer and Minister for Financial Services – Hot Issues

Contents

s 22



10.	Consumer Affairs – Scams	30
11.	Consumer Affairs – Scams (defensive).....	35

s 22



10. Consumer Affairs – Scams

Key grabs

s 22



- Importantly, our codes will provide **clear pathways for consumers to be compensated** if a bank, telco or digital platform has done the wrong thing.

s 22



If asked – Scams Prevention Framework (SPF)

s 22

- The SPF will impose requirements on industry to have mandatory internal dispute resolution (IDR) process. This will provide consumers with a pathway for mandatory redress where the entity has done the wrong thing.
- In addition, industry will be required to be part of a mandatory external dispute resolution scheme. This will offer an independent, impartial, free and fair mechanism to consumers to resolve complaints.
- The SPF is only the start of a significant uplift in protection laws, prioritising Australian consumers and putting industry on notice.

s 22

If asked – Why isn't Australia replicating the UK model of enforcing mandatory reimbursement.

- Our Framework will focus on prevention. Reimbursement should not be the first line of defence. We do not want to allow criminal scammers to get their hands on Australians' hard-earned money in the first place.
- Our model includes fines and compensation. We will create sector-specific codes that set tough obligations on industry. If a bank, telco or social media company fails to meet these high standards and breaches the code, then the responsible company will need to pay compensation to a victim that loses money.
- Our approach will make Australia the toughest place in the world for scammers to target.

If pushed –

- The mandatory UK scheme has only just commenced (7 October). In early September, the UK Government consulted on (and subsequently decreased) the mandatory payment. There has been concern about the viability of this model and that it creates a moral hazard problem – and this is before the scheme was even made mandatory.
- Further to this, the UK Government released a cost benefit analysis and consultation paper determining that the mandatory payment threshold will be reduced from £415,000 pounds (\$800,000 AUD) to £85,000 pounds (\$165,000 AUD).
- The UK model is also not as extensive as ours. Our approach will hold all of the ecosystem to account – not just the bank, but the telco who allowed the call through, or the social media company that gave a platform to a scam ad.
- Our Framework will ensure that the responsible companies are held liable.
- This lifts consumer protections and helps keep Australians' money safe.

s 22

11. Consumer Affairs – Scams (defensive)

s 22

- They will face fines of up to \$50 million AND be required to compensate victims.

s 22

Dispute resolution

- Our dispute resolution pathway **empowers victims to seek compensation by setting clear guardrails.**
- Without our laws, victims face an uphill battle against these big companies.
- With our laws, redress pathways will be clear and consumer centric.
- It will **not be on the individual victim to determine who pays.** The government will set the criteria of apportionment in the Codes.
- The full process of the IDR and EDR will be designed upon passage of the legislation.
- Breaches are enforceable. Not doing an IDR or EDR correctly will result in penalties.
- **Consumers are at the centre of this legislation** and will be the centre of the design for dispute resolution.

If Asked: Treasury recommended UK model?

- The department has NEVER recommended a UK model.
- They have consistently recommended a model of shared responsibility among the scam's ecosystem – banks, telcos, social media.

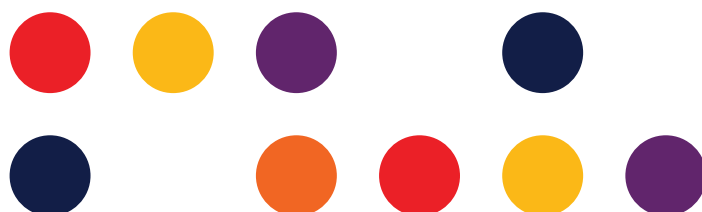
Scams Prevention Framework – exposure draft legislation

TPG Telecom submission

The Treasury

4 October 2024

Confidential



Submission

Thank you for the invitation to provide feedback on the Scam Prevention Framework exposure draft bill (**the Framework**).

About TPG Telecom

TPG Telecom is Australia's third-largest telecommunications provider and home to some of Australia's most-loved brands including Vodafone, TPG, iiNet, AAPT, Internode, Lebara and felix.

We own and operate nationwide mobile and fixed networks that are connecting Australia for the better.

Executive summary

TPG Telecom welcomes the opportunity to contribute to the ongoing work to combat scam activity in Australia. We contributed to the industry association submissions from both the Communications Alliance and the Australian Mobile Telecommunications Association, and support the positions put forward within both submissions.

TPG Telecom is committed to working constructively with industry and Government to leverage our collective expertise and ensure any future approach to scam management meets the Government's intended objectives.

However, TPG Telecom does oppose a generic framework that risks hindering or harming the flexibility and capability required to innovate new solutions in the war against scammers.

We are concerned that the creation of unnecessarily cumbersome and rigid obligations that impose administrative and regulatory burdens will reduce the ability of industry to respond rapidly to the changing operating environment.

In addition, regulators, including the ACMA, should be doing more to enforce existing regulations and prioritise consumer protections. We consider that much more can be achieved under the existing framework to provide the certainty and support required by industry to stop scam communications efficiently, rapidly and in protection of the Australian community. We have provided additional information regarding these issues below.

General comments

TPG Telecom recognises the role we play within the ecosystem to prevent, disrupt and respond to scams and scammers to protect Australians. Our scam reduction activity has resulted in 141,247,156 scam communications blocked in the 2023/2024 financial year (with 33,721,776 calls and 107,525,380 SMSs blocked).

TPG Telecom supports clearer obligations on regulators to ensure the current scam prevention, reduction and disruption instruments are effectively managed and enforced. This includes both current and pending legislative and regulatory instruments:

- Reducing Scam Calls and Scam SMSs Industry Code C661 (**Scam Code**)
- Telecommunications Numbering Plan 2015 (**Numbering Plan**)
- Telecommunications Amendment (SMS Sender ID Register) Act 2024 (**SMS Sender ID Register**)
- Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 (**CID Determination**)
- Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 (**PPV Standard**)
- Digital ID Act 2024
- Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017

The Scam Prevention Framework structure

TPG Telecom recommends the Treasury adopts a more targeted approach, with the Framework setting out the principles and the specific rules for scam prevention housed within the Codes of designated sectors, rather than prescriptive 'one size fits all' obligations as currently contained within the draft Bill.

The use of subordinate instruments drafted with a focus on the operating environment of the designated sectors, enables the principles set out in the Framework to be more effectively achieved and would strengthen the role and enforcement powers of the relevant regulators.

Examples of frameworks following this structure include Security of Critical Infrastructure Act.

Numbering Plan Review and impact on Scams

The principles should include a requirement that the ACMA ensures the Numbering Plan prevents the use of Australian numbers for scam activity. We strongly disagree with the proposition that this issue sits outside the remit of the current framework creation process. The primacy of addressing the misuse of numbers is so fundamental that it rightly sits as a principle in legislation.

The 2024 Numbering Plan Review being conducted by the ACMA provides a critical opportunity to update the Plan to more immediately and efficiently act against the increasing threat of scam traffic to Australian communities.

One of the most effective actions available to reduce scam traffic is for the Plan to clarify how numbers can be used across networks, and to stop and block traffic originating on a network other than its home network, or where there is a valid call case such as call diversion or roaming.

While TPG Telecom embraces competition and innovation, it does not accept numbers should be used without any control over call origination. Using the pretext of anti-competitive action as an excuse to profiteer from scam communications at the expense of the Australian community is unacceptable.

Clear rules for the use of numbers across networks would facilitate tighter control of scam traffic. In accordance with the Scam Code, one of the single most effective actions available to reduce scam traffic is for the Plan to clarify how numbers can be used across networks, and to stop and block traffic originating on a network other than its home network (except for valid call cases such as call diversion and roaming).

Numbers were never intended to be used on multiple networks simultaneously. For example, a number is only identified as being in use on a single network in the Integrated Public Number Database. While the present regulatory environment expects numbers to be used to originate and terminate traffic on a single network, the Plan does not explicitly forbid simultaneous use over multiple networks. However, if a customer wants to use the number issued to them on another network, they can change CSP - which is why we have number portability.

TPG also strongly advocates for the consideration of prohibiting the use of Australian numbers to originate traffic from outside Australia. There are currently no rules for limiting Australian numbers coming into Australia as a local call.

SMS Sender ID Register

As set out in recent submissions on the structure of the Registry, TPG Telecom supports Option 2 - a mandatory Sender ID registry acting as an 'allow-list' for alpha-tagged SMS. Scam Short Messages (SMS) should be prevented from being allowed to be sent in the first place - particularly in the form of alphanumeric Sender ID SMS, which appear to victims as legitimate communication from a trusted organisation.

Without a defined, mandatory model, the general public will remain unable to trust SMS sent by businesses and government services.

Only by developing a mandatory, trusted, closed ecosystem for sending alphanumeric Sender ID SMS will the public, businesses, and the telecommunication industry see a reduction in scam communications, to enable the telecommunication industry to deliver the expected security of SMS communications. In such an environment a clear message can be given to the community that alphanumeric Sender IDs can be trusted.

A voluntary 'block-list' scheme would leave the door open for bad actors to continue to send scam SMS by overstepping, mirroring or impersonating legitimate Sender IDs as they are today – voluntary scheme lists have infinite options available for impersonation. Please see **Attachment A: SMS impersonation scams** for an example of how a voluntary scheme would be unworkable, in a world where non-listed entities could continue to send SMS with alphanumeric Sender IDs.

Opponents of a mandatory scheme do so on the basis that the registration process would be too difficult and onerous. While this may be true for some overseas models it does not have to be the case of an Australian model and the perceived difficulty of mandatory registration needs to be balanced against the real cost to the community of enabling SMS scams to flourish.

Disruption and the risk of blocking legitimate traffic

While the framework contains safe harbour provisions for taking action to disrupt an activity while investigating whether the activity is a scam, TPG Telecom is concerned that heavy handed expectations to respond to scams will result in legitimate traffic being blocked. In some cases, due to the nature of the scams, this may include communications for people in vulnerable circumstances.

This concern comes from the nature of the 'Hey Mum/Dad' scam, which can be very targeted, complex to identify, and reflect legitimate scenarios of individuals seeking support in a moment of need (**Attachment C: 'Hey Mum/Dad' scam** outlines how the scam operates today). The choice will come for telecommunications providers to either block a child from seeking assistance or a scammer seeking to take advantage.

While telecommunications companies may be able to avail themselves of the safe harbour legal protections in the Framework, it will do nothing for the affected members of the public who were unable to contact their loved ones in a moment of need, nor the reputation of the telco who blocked that contact.

Liability

There has been significant effort and activity by TPG Telecom and the telecommunications sector to address scam activity – often for the benefit of other sectors and industries. The rise of government and businesses using links within SMS and SMS one-time passcodes (**OTP**) as part of multi-factor authentication (**MFA**) has created an environment where our services are utilised to perpetuate fraud.

We have acted to prevent, disrupt, and stop scam activity, often to the detriment of accessibility and ease of management of a customer's account. Consideration is needed to the trade-off between customer experience and the impact of scams. Customer friendly can be fraud friendly – but it is rarely fraud conducted on our customer's account that we are protecting them from, but fraud on their bank account or government services.

We particularly wish to call out the reluctance of banking services to participate in solutions that would have protected their customers from SIM swap and porting associated fraud through the Jersey Telecom scheme: <https://www.itglobal.com/jersey/it-protects-australian-consumers-from-fraud/>, <https://international.itglobal.com/mobile-intelligence/know-your-customer/>. Telecommunications providers have for years have sought to support the Australian public from the risks of their telecommunications services being hijacked to perpetuate banking fraud. We have many regulatory instruments, such as the CID Determination and the PPV Standard, that create regulatory burden and liability on our sector, for the protection of other sectors customers. The framework should serve to require that all players in the ecosystem must, to the extent practicable, involve themselves in joint efforts to combat scam activity.

On the liability for individual consumer scam losses under the Framework, TPG Telecom submits it should be limited to the losses experienced due to scams directly associated with the customer's account with telecommunications providers, not the use of telecommunications services for a scam perpetrated for another regulated industry.

Additionally, TPG Telecom supports the Government's intention to make Australia one of the least attractive countries in the world for scammers. To achieve this aim, TPG Telecom submits the Framework should include rules that mirror the UK compensation scheme's use of excess per claim

and a cap on claims, to ensure the compensation scheme is protected from 'no risk' scam activity
s 47G(1)(a)

<https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf>).

External dispute resolution scheme

TPG Telecom supports the Australian Financial Complaints Authority (AFCA) being authorised as the operator of the SPF EDR scheme.

Given the financial impact of scams on consumers, it is our view that it is appropriate for AFCA to manage scam-related complaints where the incident falls under the Framework.

We strongly support a 'no wrong door' referral process, to ensure the public can seek assistance from any EDR scheme they approach. In this proposal, it would be a pathway from other EDR schemes (such as the Telecommunications Industry Ombudsman) to refer consumer complaints to AFCA.

Specific clauses

Clause	Text	Comments
58AE	Minister must consider matters before designating a sector (b) the effectiveness of existing industry initiatives to address scams in the sector;	As outlined above, the telecommunications sector has a significant collection of enforceable direct and co-designed regulatory instruments. TPG Telecom submits that following a review of the current Scam Code to ensure it meets the principles set out the Framework, in conjunction with analysis of how the current review of the Numbering Plan, SMS ID register, and know your customer activity under the Digital ID, there is effective industry initiatives for the prevention of scam.
58AG	Meaning of scam (1) A scam is a direct or indirect attempt to engage an SPF consumer of a regulated service that: (a) involves deception (see subsection (2)); and (b) would, if successful, cause loss or harm including obtaining personal information of, or a benefit (such as a financial benefit) from, the SPF consumer or the SPF consumer's associates. (2) The attempt involves deception if the attempt:	There must be a way to differentiate between scam events using telecommunications services and scam events against telecommunication's customers' services. The mechanism for reasonable processes and systems should be based on the nature of the scam event, as it will not be appropriate to require the same actions for volume events as there is for individual events. What is the role of customer-assisted fraud (such as the example outlined in Attachment A). Customers, for a potential benefit for their participation, do today perpetrate fraud on their telecommunications account. This issue is not captured in the current definition, which is focused on scammers seeking to take advantage.

	<p>(a) deceptively represents something to be (or to be related to) the regulated service; or</p> <p>(b) deceptively impersonates a regulated entity in connection with the regulated service; or</p> <p>(c) is an attempt to deceive the SPF consumer into facilitating an action using the regulated service; or</p> <p>(d) is an attempt to deceive the SPF consumer that is made using the regulated service.</p> <p>(3) However, the attempt is not a <i>scam</i> if the attempt is of a kind prescribed by the SPF rules.</p>	<p>Finally, what reasonable steps should be considered where the customer is not aware that their service has been hijacked and the transactions/interactions look legitimate to us (for example, where the scammer has collected the required intelligence about the individual to effectively impersonate them and pass authentication processes. This can include the use of compromised emails to pass MFA.</p>
58AI	<p>Meaning of <i>actionable scam intelligence (ASI)</i></p> <p>A regulated entity identifies, or has, actionable scam intelligence if (and when) there are reasonable grounds for the entity to suspect that a communication, transaction or other activity on, or relating to, a regulated service of the entity is a scam.</p> <p>Note 2: Gathering and reporting this information will minimise the harm from scams.</p>	<p>The ASI definition must be limited to ASI that is meaningful to be shared to other parties, not merely the existence of data. Given the extraordinary amount of data produced in anti-scam activity, it would be of limited value to push all data into the portal.</p> <p>Under the Scam Code, TPG Telecom currently sends scam intelligence to the ACMA and ACCC as part of our daily processes.</p> <p>We receive actionable intelligence from the AFCX loop a few times a week. We also provide actionable intelligence to a partner in the banking sector every weekday.</p> <p>TPG Telecom has also been engaged with the NASC on the development of a partner sharing portal. The fast sharing of ASI envisioned under the Framework should be achieved using this portal, to enable a single point of input for ASI.</p>
58BB	<p>Each regulated entity must develop and implement governance policies, procedures, metrics and targets for combatting scams.</p> <p>These must be reviewed, and certified by a senior officer of the entity, at least annually.</p> <p>The entity must publish information</p>	<p>We strongly encourage the detail of 'must publish information about how the entity is protecting its consumers from scams, and about the rights of its consumers in relation to scams' be reconsidered or softened, in an environment where scammers are using this knowledge to bypass our processes and systems.</p> <p>Regulated sectors will need to be very careful about the information that is shared online with the</p>

	<p>about how the entity is protecting its consumers from scams, and about the rights of its consumers in relation to scams.</p> <p>The entity must keep records and give reports about its compliance with this principle.</p>	<p>public. We don't want to let the scammers know about what we are doing to detect and disrupt scams.</p> <p>Currently, the Scam Code requires CSPs to publish education information about Scam Calls and Scam SMS. For example, Vodafone publishes the following:</p> <ul style="list-style-type: none"> - https://www.vodafone.com.au/support/notify/scams - https://www.vodafone.com.au/support/notify/fraud - https://www.vodafone.com.au/support/notify/security <p>We submit that these rules and our current obligations under the Scam Code are sufficient and get the balance right between informing the public and tipping off scammers.</p>
58BC	<p>Developing and implementing governance policies and procedures—civil penalty provision</p> <p>(c) develop and implement performance metrics and targets that:</p> <p>(i) are for measuring the effectiveness of those policies and procedures; and</p> <p>(ii) comply with any requirements for those metrics and targets that are prescribed by the SPF rules.</p>	<p>While TPG Telecom understands the need for metrics and data to understand the performance of designated sectors, we are concerned with the use of the term 'targets'. Scam activity is in constant flux – as several years of Scam Call and SM data provided to the ACMA demonstrate.</p> <p>As a volume-based scam event is detected and shut down, we may see a flattening in our data; however, this will change, as scammers alter their modus operandi and reattempt. We cannot envision circumstances where targets make sense in the context of scams.</p> <p>We strongly support the continuation of volume-based metrics under the current Scam Code.</p>
58BD	<p>Content of governance policies, procedures, metrics and targets</p> <p>(d) meet performance metrics and targets developed for these policies and procedures; and</p>	<p>As above in response to 58BC, the concept of 'targets' should be removed.</p>
58BF	<p>Publishing information about protecting SPF consumers from scams—civil penalty provision</p> <p>(a) the measures the entity has in place to protect SPF consumers of the entity's regulated services from scams;</p>	<p>As above, in response to 58BB, there should not be requirements to publish information that would be detrimental to our anti-scam activity.</p>

58BI	<p>Each regulated entity for a regulated sector must take reasonable steps to prevent scams. This includes:</p> <p>(a) making resources accessible to its consumers to assist these consumers to identify scams and to minimise the risk of harm from scams; and</p> <p>(b) identifying its consumers that have a higher risk of being targeted by a scam and providing warnings to those consumers.</p>	<p>Clause 58BI(b) stipulates 'identifying its consumers that have a higher risk of being targeted by a scam and providing warnings to those consumers'.</p> <p>There is no mechanism that enables TPG Telecom to profile and identify if a customer may have a higher risk of being targeted. There is no consumer data that we hold that would identify if that individual's circumstances may place them in a position of higher risk.</p> <p>Given the sheer volume of scam SMS and calls that are identified, it would be unworkable in practice to inform every customer who may be impacted, beyond general education requirements.</p> <p>We do update the scams page online for any major new scam trends that occur, that may meet these criteria (see details in response to 58BB).</p>
58BJ	<p>Taking reasonable steps to prevent scams from being committed—civil penalty provision</p> <p>A regulated entity contravenes this subsection if the entity fails to take reasonable steps to prevent another person from committing a scam relating to a regulated service of the entity.</p>	<p>Clarification will be needed on what 'reasonable steps' means.</p> <p>Further, this clause will be complex to achieve without the changes requested under the Numbering Plan review and a mandatory SMS Sender ID register (as outlined above).</p>
58BK	<p>Giving resources and warnings to SPF consumers—civil penalty provision</p> <p>(2) A regulated entity contravenes this subsection if the entity fails to take reasonable steps to:</p> <p>(a) identify the classes of SPF consumers (if any) of a regulated service of the entity who have a higher risk of being targeted by a scam relating to the regulated service; or</p> <p>(b) provide warnings about such a scam to each SPF consumer belonging to such a class.</p>	<p>As above, in response to 58BI. We have no way of profiling customers that may receive a scam.</p> <p>It is unclear how this requirement would operate in practice due to the sheer volume of scam SMS and calls that are identified. There needs to be a difference between scam impacting telecommunications accounts and scams perpetrated over telecommunications services.</p>
58BW	Taking reasonable steps to disrupt	TPG Telecom is concerned about what would

	<p>scams—civil penalty provision.</p> <p>1) A regulated entity contravenes this subsection if the entity fails to take reasonable steps within a reasonable time to:</p> <p>(a) disrupt a scam, or suspected scam, relating to actionable scam intelligence that the entity has; or</p> <p>(b) prevent loss or harm (including further loss or harm) arising from such a scam or suspected scam.</p>	<p>constitute reasonable steps, timeframes and intel.</p> <p>Scammers will evolve content to slip through cracks. Once a scam has been identified and blocked, if a similar scam is created, will the telecommunications provider be liable for interim scams sent between identifying and blocking?</p> <p>Once a scam has been delivered, would there be an expectation that a notification is sent to the recipient therefore “preventing loss”?</p> <p>What requirements would there be from a telecommunications provider to prevent loss or harm where our customer’s accounts are not impacted?</p>
58BZB	<p>Enabling SPF consumers to easily report scams—civil penalty provision</p> <p>(1) A regulated entity contravenes this subsection if the entity does not have an accessible mechanism for SPF consumers of the entity’s regulated services to report scams relating to those services to the entity.</p>	<p>It is unclear if this rule is intended to create an obligation for 2-way communications to report scams, or simply a mechanism for consumers to provide information about scams with no expectation for a response, similar to the service offered by Scam Watch.</p>
58BM	<p>Each regulated entity for a regulated sector must take reasonable steps to detect scams. This includes identifying, in a timely way, its consumers that are or could be impacted by a scam.</p> <p>The SPF code for the sector may include sector specific provisions for this principle.</p>	<p>While TPG Telecom has processes in place to identify someone attempting to transact using another person or organisation’s identity without consent, this is limited to scams seeking to be perpetrated against us in relation to the services we provide.</p> <p>This needs clarification for how it could be applied to telecommunication providers in relation to the use of telecommunication services. We detect thousands of scam SMS and calls per day. There are thousands of potentially impacted consumers everyday.</p> <p>Would telecommunications providers be expected to contact the potentially thousands of customers that have received a scam SMS or call? Are there going to be proposed thresholds with regards to when we should contact our customers?</p> <p>For some sectors, this may make sense, as it may be one customer who has fallen victim to a scam, potentially making it easier for them to identify and communicating with that customer.</p>

		In a volume based scam event for a telecommunications provider, this may be hundreds of thousands of individuals, who did nothing more than answer a call.
58BN	<p>Taking reasonable steps to detect scams—civil penalty provision</p> <p>Without limiting subsection (1), the regulated entity fails to take reasonable steps to detect a scam relating to a regulated service of the entity if the entity fails to take reasonable steps to:</p> <p>(a) detect such a scam as it happens; or</p> <p>(b) detect such a scam after it happens; or</p>	<p>Scams can be multi-platform. Often scammers can start the scam process on a digital platform. By the time the scam conversation shifts to a telecommunications service, it has all the hallmarks of a normal, legitimate communication, as the scammer has now established a relationship with the potential victim. Telecommunications providers will have no way to detect if a scam is or has happened in such scenarios.</p> <p>Further, the Framework should consider the technical realities of the telecommunications network – there is often not only one provider involved in the transmission of a call or SMS. Calls will have an originating, transiting, and terminating carrier.</p> <p>What would occur in the instance where another carrier (Carrier B) floods Carrier A's network with scam calls and one of Carrier A customers falls victim and loses money.</p> <p>Are both Carrier A and Carrier B liable? Who is more liable, the carrier that originated the traffic or the carrier that it goes to? How would that liability be calculated?</p> <p>Again, these issues would be best dealt with under the subordinate legislation, to ensure the technical needs of each designated sector is consider and effectively dealt with.</p>
58BV	<p>Each regulated entity for a regulated sector must take reasonable steps to disrupt scams and prevent losses from scams.</p> <p>If the entity has actionable intelligence about a suspected scam, the entity must:</p> <p>(a) disclose sufficient information to its consumers to enable them to act in relation to the suspected scam; and</p> <p>(b) share that intelligence with the SPF general regulator.</p>	<p>Consideration should be given to the benefits of immediate disruption versus timely reporting to and action by law enforcement. Disruption activities may lead to the compromise of legal enforcement opportunities for criminal prosecution.</p>

	<p>The entity is not liable for damages etc. in taking certain actions to disrupt a suspected scam.</p> <p>The SPF code for the sector may include sector specific provisions for this principle.</p>	
58BO	<p>Identifying impacted SPF consumers in a timely way—civil penalty provision</p> <p>(b) fails to take reasonable steps within a reasonable time to identify each SPF consumer of that service who is or could be impacted by the suspected scam.</p>	As above, for 58BM.
58BR	<p>Reporting information to SPF regulators—civil penalty provisions</p> <p>(1) A regulated entity contravenes this subsection if the entity fails to give the SPF general regulator, in accordance with subsection 58BS(1), a report of actionable scam intelligence the entity has about a suspected scam relating to a regulated service of the entity.</p>	<p>Under the Scam Code, TPG Telecom sends actionable scam intelligence to other carriers every day as part of traceback requests. If we identify scams coming in from other carriers, these are reported as part of the scam code. Would this current activity cover this clause?</p> <p>We would need confirmation of what exactly is expected of us to report, bearing in mind that privacy is important.</p>
58BV	<p>Each regulated entity for a regulated sector must take reasonable steps to disrupt scams and prevent losses from scams.</p> <p>If the entity has actionable intelligence about a suspected scam, the entity must:</p> <p>(a) disclose sufficient information to its consumers to enable them to act in relation to the suspected scam;</p>	<p>There must be a differentiation between disclosing sufficient information if a consumer has received a suspected scam call or SMS, compared to the customer's telecommunications service having been impacted by a suspected scam.</p> <p>On the former, such communications has the potential to simply create 'noise' about scams, with very little practical impact, as the community beings to ignore the communication due to sheer volume. For the latter, this would be workable where we know the individual (for example, we hold their contact details), compared to fraud events where we do not have the personal details of the individuals impacted.</p> <p>This clause would be best housed in an industry specific Code, given the complexity behind</p>

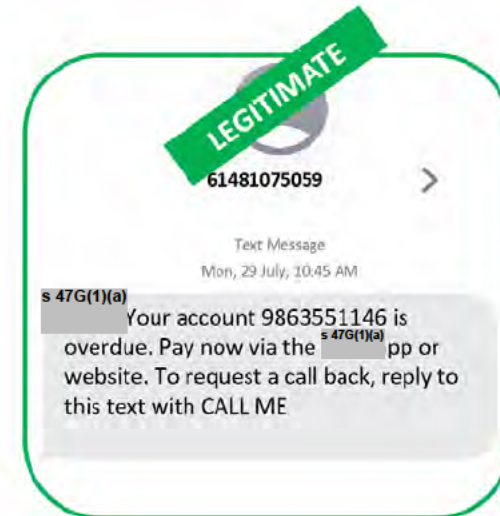
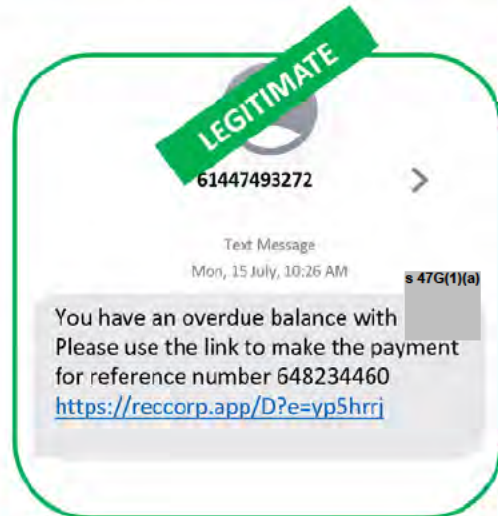
		operationalising the objective of the rule.
58BX	<p>Sharing information about scams—civil penalty provision</p> <p>(1) A regulated entity contravenes this subsection if the entity:</p> <p>(a) has actionable scam intelligence about a suspected scam relating to a regulated service of the entity; and</p> <p>(b) fails to take reasonable steps within a reasonable time to disclose to SPF consumers of the regulated service sufficient information to enable those consumers to act in relation to the suspected scam.</p>	<p>As above in response to 58BV. The detail of this obligation is best held in subordinate legislation, as the complexity of how communications to the public for volume scams, targeted scams, scam-attempts using telecommunications service, and scam-attempts about an individual telecommunications account all require very different approaches and various level of practicality and effectiveness.</p>
58DB	Minister may authorise external dispute resolution schemes for a regulated sector	<p>As noted above, TPG Telecom supports the Australian Financial Complaints Authority (AFCA) being authorised as the operator of the SPF EDR scheme.</p>

Attachment A: SMS impersonation scams

SMS campaigns *Scammers are ever evolving. Differentiating legitimate and scam SMS is becoming increasingly difficult.*

Campaign comparison	Scammer	Legitimate company
Sends from alphanumeric tag or mobile number	✓	✓
Asks customers to pay via link	✓	✓
Threatens action if payment not made	✓	✓
Outbound call campaign requesting PI or payment details	✓	✓
Sends both bulk and single campaigns	✓	✓

An SMS Sender ID Register would allow companies to send SMS using a trusted alpha tag. Only a **mandatory** model would provide consumers with 100% confidence.



s 47G(1)(a)



Attachment C: 'Hi Mum/Dad' scam

Hi Mum/Dad Scam

What is the scam?

- Scammer purporting to be a child in need
- Broken/lost device
- Need money for new phone
- Often offer to pay back once they regain access

Why it is successful

- No links
- Purely conversational
- Very little red flags
- Kids lose things, regularly

Telco challenges

- Low volume campaigns (sometimes sent to a single recipient)
- Requires reading stored content
- Lost in legitimate medium volume campaigns such as birthdays, weddings, etc.

Successful Hi Dad scam

Hey dad hope you're well, I'm letting you know I damaged my phone earlier today and it couldn't read my sim so save this temporary number for now x

Victim Responds

I'm looking at replacement phones online I can't choose between the iPhone 15 or the plus with the bigger screen

I'm looking at the new iPhone's at the moment. I should be able to keep all my data as it's saved on the cloud.

Victim Responds

When I tried ordering the phone it's saying I need a code sent to my old number which I can't get to

Victim Responds

Is it okay if I can use your card to pay for the phone

Victim Responds

Ok I'm gonna order it now I'll let you know how it goes xx

ABC Afternoon Briefing (Pre-record)

Interviewer: Melissa Clarke

Topics:

s 22

2. AFCA Scams complaints

s 22

4. Qantas

MEDIA RELEASE

s 22

AFCA SCAMS DATA (2023-23)

Key points

- AFCA resolved more than 10,000 scams complaints in 2023-24
- 70% of scams complaints were resolved within 60 days
- Monthly average of scams complaints to AFCA turned downwards

Government scams crackdown TPs

- For the last decade scams have been doubling every year. It wasn't treated as a serious problem by the Coalition. For the first time this has changed.
- The focus of our new law is prevention - stopping the losses before they occur. We will do this by placing new obligations on companies to protect their customers. Liability, and compensation, arises when there is a breach of obligation.
- The law will establish new dispute resolution pathways where currently there are none. It will create new grounds for compensation where currently there are few.
- Once the framework is legislated Australia will have the toughest prevention system in the world.
- It would be a tragedy if politics got in the way of introducing these new protections. The Government will be seeking bipartisanship on this. It's in the national interest.

Additional background:

The Government has provided over \$168 million in the 2024-25 and 2023-24 Budgets to tackle scam activity across the economy.

Questions about delays in resolutions timing:

This is why we have invested \$14.7 million over two years to equip AFCA with the resources it needs to effectively implement and operate the single EDR

CROSSBENCH BRIEF

SCAMS PREVENTION FRAMEWORK BILL 2024

**ASSISTANT TREASURER AND MINISTER FOR
FINANCIAL SERVICES
THE HON STEPHEN JONES MP**

TUESDAY 5 NOVEMBER 2024

SCAMS PREVENTION FRAMEWORK BILL 2024

Overview

The Scams Prevention Framework (SPF) is an economy-wide reform that will make Australia a tougher target for scammers. This Bill establishes a whole-of-economy approach to prevent scams in Australia by placing new obligations on key businesses through the *Competition and Consumer Act 2010*.

Designated business will be required to take steps to prevent, detect, disrupt, report and respond to scam threats in their networks. The SPF will be overseen and enforced by regulators who are provided with enforcement powers and the ability to apply significant penalties for non-compliance. Under the SPF, consumers will be eligible for compensation for loss or damage when a designated business has not complied with the law.

It introduces principles-based obligations for regulated sectors and enables the development of sector-specific codes. Internal and External Dispute Resolution processes for consumers are also mandated and regulated entities may be responsible for providing compensation if they have not met their SPF obligations.

Who does it affect?

Banks, telecommunication providers and certain digital platforms (social media, paid search engine advertising and direct messaging services) are the initial sectors being designated as they are key vectors of scam activity.

The SPF protects individuals and small businesses in Australia, and Australian residents using the services of a regulated entity based in Australia while overseas.

Financial impact

\$51.9 million has been allocated to enable regulators to administer and enforce the SPF, and provide funding for AFCA to establish external dispute resolution for the SPF. ASIC, ACMA and AFCA will be subject to industry funding arrangements.

All figures in this table represent amounts in \$m, rounded to the nearest \$0.1m.

	2024-25	2025-26	2026-27	2027-28

Payments	16.5	18.5	8.3	8.6
Receipts (cost recovery)	-	8.0	5.2	4.5
Total	16.5	10.5	3.1	4.1

Timing and further processes

The law will take effect from passage. Designation instruments will be consulted on and made in 2025, with entities to comply from the designation date subject to any transitional arrangements. Sector-specific codes will be developed in 2025.

ADDITIONAL INFORMATION

- The Government has committed over \$180 million to combat scams and online fraud. There have been positive signs from Government and industry efforts to combat scams, but scam losses remain high with \$2.7 billion stolen from Australians in 2023 and continue to inflict psychological and emotional harms.
- Current scam protections are piecemeal and inconsistent across the economy and consumers face inconsistent protections across different service providers.
- The consistent and enforceable approach of the SPF will ensure that incentives and obligations are in place across key sectors where scammers take advantage to cause harm in the community. The SPF will ensure that all points of the ecosystem are held to account, as it is common for scammers to use multiple platforms and services to steal from consumers.
- Regulated entities will be required to take reasonable steps to prevent, detect, disrupt, report, report to scams and have governance arrangements in place relating to how entities will protect consumers from scams.
- Banks, telecommunication providers and certain digital platforms will initially be designated as they represent key vectors of harms for consumers.
 - Bank transfer was the most reported payment method used by scammers with \$212.9 million in reported losses in 2023 (Source: Scamwatch).

- Phone calls and social media were the contact methods associated with the highest value of losses, \$116 million and \$93.5 million respectively in 2023 (Source: Scamwatch).
- Other sectors may be designated under the SPF in future, such as online marketplaces, superannuation, cryptocurrency, and other payment providers.
- A multi-regulator model led by the ACCC with the support of ASIC and ACMA will capitalise on existing expertise and ensure a single regulator will not be spread too thin as the SPF continues to expand to additional sectors.
- Regulators have access to civil penalties of up to \$50 million for the most egregious breaches. This should incentivise compliance and deter regulated entities who may foresee higher possible gains from breaching the SPF. Regulators will be able to take a proportionate approach with other compliance tools such as infringement notices, enforceable undertakings, injunctions, public warnings and remedial directions also available.
- As scams are a global challenge, this legislation will support the Government and industry in international engagement and collaboration, and the sharing of monitoring and intelligence across regulated entities in Australia and support international enforcement action to disrupt illicit scam activities.
- The Minister is required to commission a statutory review to examine the operation of the SPF 3 years after the commencement of the first SPF code. This will provide an opportunity to ensure the object of the SPF is being met.

Mandatory codes

- The SPF aims to build upon existing industry codes and initiatives in introducing strong enforceable obligations and penalties for designated sectors/services. The Government will consult extensively with all stakeholders during the development of designation instruments and sector codes.
- The codes will provide industry specific, prescriptive obligations for each sector that are consistent with the principles of the SPF. However, they do not relieve a business from their obligations to take reasonable steps in all circumstances

recognising that scams are constantly evolving, so businesses must be evolving in their response as well.

- An SPF code may also set out timeframes for responding to a complaint as a condition for an IDR mechanism. It could include different timeframes reflecting complexity of a complaint or the particular sector.

SPF Rules

- Under the enabling legislation, the Minister has the power to design SPF Rules that will prescribe processes and guidelines to accompany the codes. The SPF Rules will set out additional detail in relation to industry requirements to address discrepancies in entity size and functionality, as well as clear expectations for reporting and dispute resolution.
- These rules will include mandated requirements for fit and proper IDR processes and for those processes to include liability apportionment for cross sector complaints.

Dispute resolution process

- Consumers will have access to free and transparent internal and external dispute resolution processes if they are the victim of a scam and one or more regulated entity has not met its obligations.
 - With ‘no wrong door’ intended for internal dispute processes, consumers can approach any regulated entity connected to a scam.
- The Government will authorise the Australian Financial Complaints Authority (AFCA) as the external dispute resolution scheme for initial sectors. This ‘single door’ means consumers have one body to escalate their scam complaint (which may involve multiple regulated entities) with.
 - Leveraging existing EDR infrastructure and expertise is essential to ensure a single scheme can be in place from the commencement of sector codes under the SPF.
 - As scams relate to economic harm and often include financial losses by the consumer, AFCA, the largest existing EDR body among the initial

sectors, is the most appropriate single EDR body to address scam complaints regarding banks, telecommunications service providers and certain digital platforms.

- AFCA has experience in resolving scam-related complaints relating to the financial sector and resolved more than 10,000 scam complaints in 2023-24.
- The consumer's right to compensation is provided for in Section 58FZC. A victim may seek to recover the compensation through internal or external dispute resolution or through the courts and regulators are also able to take action on behalf of consumers against regulated sectors/services.
- Further, it is intended to set out in the dispute resolution rules that a regulated entity/service will be required to provide the consumer who has lodged a complaint/dispute with written confirmation (manner and form to be specified in the rules) of their compliance to the SPF related to their specific claim.
- The Government will consult on the SPF dispute resolution model in 2025 to ensure that alternative dispute resolution operates effectively and ensure delivery of a consumer-centric complaints process for scams.
 - AFCA has commenced work on experimental test cases that will assist with setting lead decisions for various iterations of failures in the scam ecosystem. These test cases will build on AFCA's existing complaints-handling system, ensuring a quick and effective consumer experience.

Reimbursement

- The Government has not taken a mandatory presumption of reimbursement approach (like the UK) to ensure the SPF incentivises actions to address scam activity across the ecosystem - from the point of inception through to the end of the scam activity chain.
- An ecosystem approach ensures each entity is liable if they have not met their obligations. This will force an ecosystem uplift, and not provide scammers another avenue to thrive while the focus is on a single sector.

- Comments that the Government received recommendations to adopt a bank only reimbursement model are inaccurate.

Consultation

- Treasury publicly consulted on the exposure draft legislation from 13 September to 4 October 2024. They received 85 submissions and held 9 roundtables across industry. The Assistant Treasurer personally met with all consumer advocacy groups, digital platforms, telcos, and members of the Australian banking system, as well as future sectors.
 - Stakeholders welcomed the Government’s whole-of-ecosystem approach and intent to introduce legislation to better protect the community from scam activity.
 - They supported the designation of the three initial sectors of banks, telecommunication providers and certain digital platforms (social media, paid search engine advertising and direct messaging services) and encouraged the rapid inclusion of other sectors, such as superannuation, cryptocurrency, other payment providers and online marketplaces.

From: s 47F
Sent: Tuesday, 3 September 2024 11:27 AM
To: s 47F
Cc: s 47F
Subject: FW: s 34(3)
Framework [SEC=OFFICIAL]
Attachments: PM SIGNED - MC24-113500 - Scams Code Framework.pdf
Categories: Check

OFFICIAL

s 47F

As discussed, to assist with your follow up conversations, below is the email where TSY reached out to the TO indicating we may seek to offset the EDR proposal with the revenue Sub.

Cheers,

s 47F

s 47F

Scams Taskforce
Consumer Branch
Market Conduct and Consumer Division

s 47F

treasury.gov.au
Langton Crescent, Parkes ACT 2600
[Twitter](#) | [LinkedIn](#) | [Facebook](#)

The Treasury acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, water and community. We pay our respects to them and their cultures and to elders both past and present.

OFFICIAL

From: s 47F @TREASURY.GOV.AU>
Sent: Saturday, August 31, 2024 10:04 AM
To: s 47F @TREASURY.GOV.AU>; s 47F @TREASURY.GOV.AU>
Cc: s 47F @TREASURY.GOV.AU>; Storer, Aidan
s 47F @TREASURY.GOV.AU>; s 47F
@TREASURY.GOV.AU>; s 47F @TREASURY.GOV.AU>; s 47F
@TREASURY.GOV.AU>; CFOB Budgets and Portfolio Coordination
Unit s 47E(d)

Subject: s 34(3)

[SEC=OFFICIAL]

OFFICIAL

Dear s 47F

s 34(3)

Key points in the proposal

s 47C, s 47E(d)

Context

s 34(3)

s 47C, s 47E(d)

We would be very happy to run you through more detail and discuss the offsets situation early next week if helpful. Please do not hesitate to reach out to s 47F or I.

best,

s 47F

s 47F

The Treasury acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, water and community. We pay our respects to them and their cultures and to elders both past and present.

OFFICIAL



Australian Government
The Treasury

Ministerial Submission

MS24-001681

FOR ACTION - Approval of exposure draft legislation establishing the scams protection framework

TO: Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP
CC: Treasurer - The Hon Jim Chalmers MP

TIMING

URGENT – By 11 September 2024, to enable the Communications Minister to review and approve the legislative package ahead of planned three week consultation period opening on 13 September 2024.

RECOMMENDATION

- That you approve the release of the scams protection framework exposure draft legislation at Attachment A, explanatory memorandum at Attachment B for public consultation (subject to any minor editorial changes).

Approved / Not approved

- That you agree that the exposure draft legislative consultation package will include document outlining the vision of the reforms , to be finalised with your Office.

Agreed / Not agreed

- That you agree the public consultation will be conducted over a three week period from 13 September to 4 October 2024 with the intent to meet the Spring A introduction timetable.

Agreed / Not agreed

- That you sign the letter at Attachment C to the Communications Minister, the Hon Michelle Rowland MP, seeking her agreement to release exposure draft legislative consultation package.

Signed / Not signed

Signature

Date: 11/9/2024

KEY POINTS

- Treasury seeks your approval to release an exposure draft legislative package establishing the scams protection framework (the framework) for public consultation.
 - The package consists of a draft bill (Attachment A) accompanied by a draft explanatory memorandum (Attachment B). ✓
 - The package will also include a paper outlining the vision of the reforms, which Treasury will finalise with your Office ahead of release.
 - A summary of the key policy outcomes in the draft bill and expected stakeholder reactions is at Attachment D, and a draft media release is at Attachment E.
 - Following discussions with you and your Office, the draft bill has been revised to reflect the changes you have agreed, particularly in relation to definitions, as outlined at Attachment F. ✓
 - As co-sponsor of the bill, Treasury recommends you seek the Minister for Communications' agreement to release the exposure draft legislative package for consultation. Treasury has engaged the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) as the draft bill was developed and is supporting them to brief Minister Rowland. A letter to Minister Rowland is provided at Attachment C.
 - Treasury understands your Office has engaged with Minister Rowland's Office on the changes you agreed to the draft bill (outlined at Attachment F). Treasury has liaised with DITRDCA officials on the revisions.
 - Following approval from you and the Minister for Communications, the package will be made available on the Treasury website, with consultation open to the public for a three week period commencing 13 September.
 - A three week consultation period is marginally shorter than the standard consultation time for draft legislation in the Treasury portfolio and may attract some criticism from stakeholders.
- Noted* – The compressed consultation timeframe is required to enable analysis and advice on stakeholder feedback, finalise the bill and obtain all relevant ministerial text approvals to support introduction in the week commencing 18 November 2024.
- Treasury continues to manage risks to support introduction of the bill on 21 November, including potentially extensive stakeholder feedback over the consultation period, competing legislative priorities, and limited OPC drafting resources.

- The framework complements the Government’s broader effort to modernise Australia's laws for the digital age, including reforms to Australia’s privacy, money laundering and cyber settings, modernisation of the payment system, enhancing online safety, as well as and the rollout of Digital ID and eInvoicing infrastructure for businesses.

s 34(3)



Risks and sensitivities

- s 22



- s 22



- s 22



s 22

ADDITIONAL INFORMATION

Summary of the package

s 34(3)

- The principles-based approach for the design of obligations under the framework, the elements of the definition of scam, and the penalties regime are consistent with what you have previously agreed.
- The designation power has been expanded to provide flexibility to the Treasury Minister to delegate additional functions in relation to the development of a sector code to another Minister or Commonwealth agency, including the power to designate a sector.
- Aspects of the multi-regulator model have been refined to manage the risks associated with an inconsistent regulatory approach. This includes introducing a default set of investigative powers to ensure that appropriate powers are immediately available to any regulator brought within the framework. The bill offers flexibility by providing the Minister with discretion to enable regulators to access their existing powers, where appropriate.
- Regulated entities will be required to be a member of a prescribed EDR scheme as a condition to providing a service regulated by the framework in Australia. The EDR scheme relevant to each sector will be prescribed in a legislative instrument. The draft bill will enable a single EDR scheme for the framework, to be administered by AFCA s 34(3)
- The Prime Minister has agreed to vary the existing authority to enable the development of the telecommunications sector-specific code via an approach consistent with the sector-specific codes for banks and digital platforms (MS24-113500 refers).

- Treasury met with you and your Office over the week of 2 September to discuss the policy features reflected in the draft bill. Following these discussions, you requested changes to certain aspects of the bill, particularly in relation to definitions. Treasury provided advice to you and your Office on 6 September in relation to policy considerations and risks associated with these changes and seeking your agreement to proceed. The draft bill has been revised and reflects the changes you have agreed and as set out in Table 1 of Attachment F, being:
 - The definition of scam has been simplified without impacting the policy outcome in relation to the scope of harms captured. ✓
 - The definition of consumer has been extended to provide protections to persons present in Australia and Australian citizens or permanent residents ordinarily overseas. ✓
 - The draft bill no longer includes requirements in relation to an annual review and revision of policies and procedures under the governance principle; and to enable sector codes to provide additional detail on governance obligations. ✓
 - Prescribed timeframes for information sharing with the SPF general regulator have been removed from the report principle, and providing for a more flexible approach by requiring that information is either shared within a period prescribed by rules, or as soon as reasonably practicable. ✓
- Treasury understands there are several areas in the draft bill that you consider may be more appropriate for inclusion in subordinate legislation and areas that you would like to consider transition arrangements.
 - Treasury is preparing a paper outlining the vision of the reforms, which will draw stakeholder attention to these areas for feedback during consultation, particularly in relation to the level of detail in the draft bill under the governance and report principles. *Good*
 - The paper will also indicate that the Government is considering appropriate transition arrangements for the application of penalty provisions and information sharing requirements, recognising that the framework represents significant change for entities across the ecosystem.

Stakeholder consultation plan

- Treasury has worked with industry, consumer groups and other stakeholders throughout development of the proposed reforms and we will continue to engage with them during the consultation period.
- Treasury intends to hold an information session, industry roundtables and issue specific workshops to gather direct feedback from stakeholders on the legislative package. Treasury will engage DITRDCA on their participation in the consultation sessions.
- Stakeholders are likely to have strong interest across several areas of the bill, and some may wish to put their views to you directly.

- Stakeholders may raise that the definitions of ‘scam’ and ‘consumer’ are overly broad (this remains the case following the revisions that were made to the draft bill following discussion with you) and may result in unintended consequences. In relation to the definition of ‘scam’, aspects of this risk can be managed through the use of a legislative instrument to exclude harms that are not intended to be regulated by this framework. However, a broad definition is reflective of policy objective for comprehensive protections against methods used by scammers.
- Stakeholders may comment that the design of the principles-based obligations are not detailed enough and seek more certainty for compliance purposes. Additional detail on principles-based obligations will be set out in sector codes, enabling tailoring for each sector.
- Stakeholders are likely to seek additional clarity on the scope of information sharing requirements and how this will intersect with privacy obligations. Treasury has engaged AGS to undertake a privacy impact assessment, which will further inform the design of these requirements ahead of the finalisation of the bill.
- Regulators have expressed concerns in relation to the design of the multi-regulator model. Treasury has worked closely with each of the regulators in the design of the current approach and has sought to manage concerns where possible, without compromising the effective operation of the model.
- Telecommunication providers and digital platform service providers will express concern and pushback on the requirement to be a member of a AFCA as a condition to providing a service regulated by the framework in Australia.
- Stakeholders are likely to ask for more detail on consumer redress arrangements, including on liability apportionment of the EDR scheme.

Next steps

- Subject to both your and the Minister for Communication’s agreement, Treasury will publish the draft legislative package on its website on 13 September, with consultation to be open until 4 October.
- At the conclusion of consultation, Treasury will provide you with a summary of stakeholder feedback and advice on issues raised in feedback for your consideration. It is likely that you will also be required to finalise the policy design in consultation with the Prime Minister and other relevant ministers.
- Subject to OPC resourcing availability, and the extent of changes in response to feedback, Treasury will finalise the legislative package following stakeholder feedback and will provide you with a final package for approval in early November.

Clearance Officer

s 47F

Head of the Scams Taskforce
Market Conduct Division
11 September 2024

Contact Officer

s 47F

Director

Ph: **s 47F**

Mob: **s 47F**

CONSULTATION

Law Division, DITRDCA

ATTACHMENTS

- A: Exposure Draft Legislation
- B: Draft Explanatory Memorandum
- C: Letter to Minister Rowland MP
- D: Summary of policy outcomes and expected stakeholder views
- E: Media release
- F: Changes to draft bill – scams protection framework

Scams

FOI 3784
Document 17

KEY MESSAGE

- The Government is taking action and implementing an ambitious anti-scam agenda to combat scams and protect Australians.

KEY FACTS AND FIGURES

- Australians lost \$2.7 billion to scams in 2023. The Government is providing \$67.5 million over four years in the 2024-25 Budget to continue its action to combat scams and online fraud, including to:
 - Develop and introduce legislation for a Scams Prevention Framework (Framework) as a priority, that outlines principles-based obligations and clear consequences for non-compliance on regulated businesses.
 - Establish and provide ongoing funding to administer and enforce new mandatory industry codes under the Framework, initially targeting telecommunications providers, banks, and digital platform services (social media, paid search engine advertising and direct messaging services).
 - Continue the Australian Taxation Office’s oversight and operation of the secure eInvoicing network to disrupt payment redirection scams; and
 - Improve public awareness of the threat of scams and prompt them toward better information to identify and report scams.
- Exposure Draft legislation for establishing the Framework was released on 13 September for a three-week consultation and is now closed. The government will consider feedback in finalising the Framework.
 - The Framework is an economy-wide reform to protect the Australian community from scams. It takes a whole-of-ecosystem approach to reduce gaps which scammers can exploit.
- The Framework will build upon the Royal Assent of the *Telecommunications Amendment (SMS Sender ID Register) Act 2024* on 5 September 2024, which gives the Australian Communications and Media Authority (ACMA) powers to establish and maintain a SMS Sender ID Registry, to stop scammers from spoofing trusted brand names.

Office Responsible	Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP	Adviser	s 47F
Contact Officer	s 47F	Contact Number	s 47F
Division responsible	Market Conduct and Digital Division		
Date of Update	08 October 2024		

Scams

- The Government’s crackdown on scams is already showing early signs of success.
 - In 2023, Australians’ losses to scams were \$400 million lower than in 2022, or a reduction of 13 per cent. Annual scam losses declined in 2023 for the first time since aggregate data reporting commenced in 2015.
 - The reduction in financial losses in 2023 occurred despite scam reports increasing by 19 per cent, showing that protections are helping to disrupt scammers, and the public is more alert to how to avoid losses from the scam threat.
- The Government continues to support the adoption of eInvoicing to disrupt payment redirection scams, improve cash flow and boost productivity for small businesses.
 - As of 30 June 2024, 132,188 businesses were registered for eInvoicing - approximately 5 per cent of Australia’s 2.5 million businesses.

Office Responsible	Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP	Adviser	s 47F
Contact Officer	s 47F	Contact Number	(s 47F
Division responsible	Market Conduct and Digital Division		
Date of Update	08 October 2024		

Scams

BACKGROUND

- The Government made an election commitment to introduce measures to combat scams and online fraud, including establishing a National Anti-Scam Centre and introducing mandatory industry codes to protect consumers.
- The Government has provided over \$154 million across the 2024-25 and 2023-24 Budgets to tackle scam activity across the economy.

National Anti-Scam Centre (NASC)

- Launched on 1 July 2023, the NASC is an initiative to make Australia a harder target for scammers. It co-ordinates efforts to prevent scams by improving intelligence sharing across Government and the private sector as well as coordinating a series of time-limited taskforces known as ‘fusion cells’ to support industry action on specific scam activity.
 - The first fusion cell focused on disrupting investment scams. Investment scams losses reported to Scamwatch in the March quarter 2024 declined by around 47% from the same quarter in 2023.
 - The second fusion cell focusses on jobs and employment scams and commenced in September 2024.

ASIC anti-scams activities

- The Government provided \$17.6 million in the 2023-24 Budget to enhance ASIC’s website takedown service, with over 7,300 phishing and investment scam websites taken down since July 2023.
- ASIC launched an investor alert list in November 2023 to provide warnings to about scam businesses and websites.
- In August 2024, ASIC published a second report banks’ anti-scam practices (covering non-major banks). It found variation in the maturity of practices, including gaps in support for scam victims and narrow approaches in determining the bank’s liability for scam losses.

Office Responsible	Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP	Adviser	s 47F
Contact Officer	s 47F	Contact Number	s 47F
Division responsible	Market Conduct and Digital Division		
Date of Update	08 October 2024		

Scams

SMS Sender ID Registry

- The Government provided the ACMA \$10 million to launch and maintain an SMS Sender ID Registry, to prevent spoofing of trusted brand names.
 - The *Telecommunications Amendment (SMS Sender ID Register) Act 2024* received Royal Assent on 5 September. A decision on whether the Register will be voluntary, or mandatory is expected by the end of 2024.
- Under the *Reducing Scam Calls and Scam SMS Code*, telecommunications providers reported blocking over 156.8 million scam calls and over 134.6 million scam SMS in the second quarter of 2024.

Scams Prevention Framework

- In the 2024-25 Budget the Government announced it will legislate the Framework. The legislation will impose robust and mandatory obligations to:
 - prevent, detect, disrupt, report, and respond to scams, complemented by regulator enforcement action and strong penalties for non-compliance; and to establish governance systems accordingly, and
 - provide consumers clear pathways of support and dispute resolution with access to redress, such as compensation for scam losses.
- : Entities that provide a service that is regulated by the framework must become a member of an authorised external dispute resolution (EDR) scheme. The Government intends to prescribe the Australian Financial Complaints Authority (AFCA) as the single EDR scheme for the three initial sectors designated under the framework.
- Consultation on the Exposure Draft legislation was open from 13 September to 4 October 2024. During consultation Treasury held 9 roundtables to hear feedback on the draft Framework.

eInvoicing

- In 2024-25 Budget, the Government committed \$23.3 million to support increased eInvoicing.

Office Responsible	Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP	Adviser	s 47F
Contact Officer	s 47F	Contact Number	s 47F
Division responsible	Market Conduct and Digital Division		
Date of Update	08 October 2024		

Scams

- Benefits of eInvoicing include increased protection from invoice scams, digitising and automating manual invoice processes, and reducing payment delays.
- Payment redirection (invoice) scams were reported by the ACCC’s *Targeting Scams* publication as the 5th most common scams in 2023, with \$91.6m in losses (a reduction from \$224.9m in 2022).
- As of 30 June 2024, 132,188 businesses were registered for eInvoicing - approximately 5 per cent of Australia’s 2.5 million businesses.

Office Responsible	Assistant Treasurer and Minister for Financial Services - The Hon Stephen Jones MP	Adviser	s 47F
Contact Officer	s 47F	Contact Number	s 47F
Division responsible	Market Conduct and Digital Division		
Date of Update	08 October 2024		

Areas raised in SPF roundtables and next steps (23 September – 27 September)

Issue	Feedback Roundtables (23 September – 27 September)	Feedback Roundtables (30 September – 4 October)	Next steps
Interaction between code obligations and principles and 'reasonable steps' test	Banking and digital platform sectors have expressed concern that a breach of the principles may occur in the absence of a code breach. Banking stakeholders raised the concern that consumers may bring forward court action against a breach of the principles, and there is currently no direct relationship with the code obligations, meaning it will be up to the Court to determine what constitutes reasonable without any regard to sector codes.	Telecommunication providers had concerns about the gap between the codes and framework and how the term reasonable would apply to their sector, considered guidance was needed. Payment providers were concerned that a lack of clarity between the codes and principles would create uncertainty for banks and support risk averse behaviour that would negatively impact interactions. Community banks were concerned about the gap between the framework and codes. Preferred more detail to be in place when designations are made either in the primary law or by having codes in place	We are working with LD to look at opportunities to establish clearer parameters for reasonable steps in the law or through explanatory material. This could include introducing a clearer nexus between the sector codes and principles to provide assurance to industry that compliance with the principles will not be considered in complete isolation of compliance with sector codes.
Actionable scam intelligence and reporting obligations	Stakeholders across the superannuation, banking, and digital platform sectors have expressed concerns with the volume of information that may be captured by the current definition of actionable scam intelligence and have commented that the definition captures information that would not be useful to support the disruption of scam activity.	Telecommunication providers, community banks and AFCX echoed previously heard concerns about the volume and usability of reports. View that providers would overreport where unclear due to high penalty risk. Community banks expressed concerns that the requirement may present a high burden for smaller entities due to lower systematisation and automation.	The policy intent is for actionable scam intelligence to be limited to information that is useful to support disruptive action being taken. We are working on how this can be more clearly defined in the bill – and will consider whether additional targeted engagement is required with industry specialists to workshop this definition and scope. We are also cognisant of the need for appropriate transition arrangements to reflect the uplift that will be required by some smaller entities.
Approach to consumer warnings	Stakeholders across digital platform and banking sectors raised concerns in relation to the number of obligations that require warnings or engagement with consumers.	Large telecommunication providers, community banks and AFCX were concerned about appropriateness of warnings in certain circumstances. Large telecommunication providers also considered warnings could drive consumer anxiety that would be difficult to appropriately manage and warnings were at high risk of being mimicked by scammers. Transit intermediaries noted these obligations would not be appropriate for their services given they do not have a direct consumer relationship (and given the broad definition of SPF consumer linked to these obligations).	We are looking at opportunities to streamline these requirements and make clearer the distinction between making information available to assist with prevention, and direct warnings to support disruption. Given the differences between how various sectors interact with consumers, we are also considering whether it is more appropriate to address these obligations through sector codes.
Definition of consumer	Banking stakeholders have raised concerns that the definition is overly broad, resulting in certain obligations (such as those relating to warnings) being impractical.	Telecommunication providers commented that the definition of consumer is overly broad, particularly as it relates to the obligations imposed on carriage service intermediaries who typically do not have a direct relationship with consumers. ASBFEO supported the definition of consumer, particularly as it relates to small business.	We have identified opportunities to make amendments to clarify the scope of obligations in the context of the broad definition of consumer.
Interaction with other legislative frameworks	Superannuation and banking stakeholders have raised concerns that the reporting regime overlaps with existing requirements in the AML/CTF space. Stakeholders have also raised interactions with privacy laws, the ePayments code, the Spam Act and other legislative frameworks.	Payment providers were concerned about negative interactions with PSP scheme rules and considered other mechanisms should be used in the payment space to better define system rails (as is currently done). Community banks noted duplication between reporting requirements introduced by the framework, and similar reporting requirements under the AML/CTF regime.	This is an area we will further consider upon receiving submissions to understand where the interactions lie, and the extent to which entities are restricted from complying with their obligations under the framework. In relation to AML/CTF interactions, we are looking to engage with AGD to better understand the reporting regime under the AML/CTF laws, however, note that these serve different purposes and that we are trying to introduce a whole-of-ecosystem approach.
Designation	Stakeholders have raised the importance of a consultation period before designation instruments are made and suggested this should be enshrined in the primary law.	It was suggested that it may not be appropriate to designate carriage service intermediaries given their unique position in the sector and their inability to take action to prevent and detect scams in many circumstances.	We are considering whether there is an opportunity to introduce a requirement that a designation instrument be consulted on, without setting a minimum timeframe for consultation, to still enable quick action to be taken to designate a sector. We understand that carriage service intermediaries do play a significant role in facilitating telecommunication services and the obligations are not intended to require entities to take action that is not practical or possible – rather are intended to require what is reasonable in the circumstances. We will consider the next steps further upon reviewing telecommunication industry submissions.

Liability apportionment	Where more than one regulated entity has not met its obligations under the SPF, banks have expressed concern about lack of clarity about how liability should be apportioned between entities at both IDR and EDR stage?	<p>Consumer groups strongly advocated for a presumption of reimbursement framework, with banks compensating consumers unless gross negligence is shown, and then chasing other sectors to apportion liability. Payment providers had a strong preference against the reimbursement approach.</p> <p>Telecommunication providers, payment providers, community banks and AFCA all raised concerns about the lack of clarity on liability. Concerns seemed to be driven by a view that a regulated entity would still be held liable when it felt it had taken reasonable steps in context or that other parties would not receive the relevant focus. ASBFEO raised the concern that redress is not adequately linked to not meeting obligations in the primary legislation.</p>	<p>There has been a clear policy decision not to pursue a reimbursement-based framework. We will consider incentives to promote positive IDR outcomes for consumers.</p> <p>We intend to seek legal advice to confirm if liability guidance could be introduced if desired:</p> <ul style="list-style-type: none"> • in primary legislation, • when authorising the EDR scheme, • in sector codes, or • SPF rules <p>However, we understand that the Minister’s preference is to consider liability apportionment on a case-by-case basis. This would then rely on AFCA case law to provide guidance.</p> <p>We will be consulting broadly over the next 6 months to ensure a workable dispute resolution model can be implemented. We will consider how that model may work as per the current policy intent, and will keep the Minister in the loop on developments and stakeholder-feedback.</p> <p>We are also considering further whether the primary legislation should explicitly state that regulated entities that do not meet their obligations will be liable for all or a proportion of the loss incurred by the consumer as a result of the scam, and that where multiple regulated entities have not met their obligations, those regulated entities would need to apportion loss between them.</p>
Participation in IDR	Banks raised concerns about how we can ensure that there are adequate provisions in the SPF to compel all regulated entities to engage in settling disputes at the IDR stage. Consumer groups raised concerns that victims may be bounced between IDR of various regulated entities.	Community banks were concerned that IDR is not clearly regulated in other sectors and there is no clear path for joining parties at the IDR stage. Considered multiple IDR could lead to a poor consumer experience. Consumer groups also expressed concern about how IDR would work where there are multiple parties involved.	Policy intent is that consumers are not bounced between IDR schemes – i.e. that there is a one door approach. In the draft legislation, IDR is currently required to be accessible and transparent. We could add an additional requirement for regulated entities to engage with the IDR processes of other regulated entities (to encourage quick resolution of the majority of complaints at IDR stage). However, our view is that this is not necessary or appropriate to add at this late stage. Mechanics of how this will work will be consulted on further and could be reinforced in sector codes if needed.
Interaction with criminal enforcement processes	The superannuation sector raised the point that there may be an opportunity to manage the interaction between the SPF and criminal enforcement processes to improve dispute resolution at the EDR.		In developing a dispute resolution model, consideration will be given to how best to manage customer journey to pursue rights under the SPF and broader criminal enforcement pathways in parallel. We consider that changes to the draft legislation are not needed to address this but are considering whether changes to the explanatory memorandum could be appropriate.
Capacity for AFCA to handle complaints/ AFCA decision making	Digital platforms raised concerns about the capacity of AFCA to handle complaints.	Community banks raised concerns that AFCA’s current approach looks at best in field, and are concerned AFCA would require significant change to move to an assessment that took account of a lower bar to meet the ‘reasonable steps’ threshold.	<p>We note that we are working to ensure that AFCA has funding to establish the capacity to provide EDR for SPF complaints. Ensuring AFCA is adequately funded to commence work is a priority to enable it to commence implementation work to expand its jurisdiction/capacity.</p> <p>We will be working to address this issue when providing further guidance/codes/rules around IDR/EDR to ensure that regulated entities are incentivised to resolve disputes prior to EDR, to limit the proportion of disputes that are escalated to AFCA.</p> <p>Further engagement with AFCA on operationalising the framework as intended is anticipated. Best in field vs reasonable issue will need to be addressed when providing further guidance/codes/rules/authorisation around EDR.</p>

Information asymmetry in dispute resolution		Consumer groups argued information asymmetry between victims and entities will lead to poor consumer outcomes due to a lack of proof. Community banks also concerned about clear evidence requirements.	This will need to be addressed when providing further guidance/codes around IDR and EDR.
Management of vulnerable consumers		Consumer groups were concerned that the framework does not adequately consider how regulated entities should support vulnerable consumers.	No action for primary law. The sector codes could set out specific requirements if appropriate.
Penalty risk		Telecommunication providers raised the issue of quadruple jeopardy – multiple potential penalties from the framework, codes, EDR and consumer civil action. Telcos and payment providers wanted a test based on systems, processes and controls rather than individual failures. Concerned about unintended consequences of high-risk aversion due to penalties.	We understand that this is not novel and is consistent with other legislative regimes applying to telecommunication providers. We will consider providing more certainty in the application of the ‘reasonable steps’ test to make it clear that obligations are not envisaged to prevent every individual scam, rather they are intended to require what is reasonable and practical in the circumstances.
Detail in codes, framework and guidance		Telecommunication providers and community banks are concerned about the level of detail in the framework and potential gap with the codes. Seeking clear and regularly updated guidance to support certainty. Payment providers suggested a new safe harbour where a third party provides assurance a business’s actions are reasonable in current context.	We are reviewing how to provide clarity on interaction between the framework and codes in the primary legislation.
Safe harbour		Payment providers and ASBFEO expressed concern that safe harbour provisions presented serious risk to impacted businesses revenue and potentially extending to existence.	Awaiting further guidance through submissions, particularly in relation to reasonable timeframes.
Consumer responsibility		Community banks considered that consumer responsibility in relation to scams needs to be clearly set out to avoid a push to EDR on all cases.	We don’t anticipate that this will be addressed through the primary legislation. Will need to be considered in context of further development of dispute resolution requirements.

What will this legislation do?

Amending the *Competition and Consumer Act 2010*, the Scams Protection Framework (the Framework), is a whole of ecosystem reform that will protect consumers from scammers while providing confidence in the efficiency and convenience of the digital economy. The Framework will require service providers to comply with the overarching principles to prevent, detect, disrupt, report and respond to scams. Non-compliance will result in civil penalties, including fines of up to \$50 million.

The Framework will establish a sophisticated network for sharing and reporting actionable scam intelligence across Government and industry.

The Framework will also mandate internal and external dispute resolution mechanisms, including enabling a single external dispute resolution mechanism for cross sector investigation and redress.

The Framework will be introduced as part of the Governments broader work to uplift and modernise Australian laws, maintaining pace with the evolution of the digital age.

When will the code be in effect?

Once the Framework legislation passes, and the Minister designates sectors, the codes will be designed with buy in from industry experts. At this stage, we aim for the codes to be in effect by 2026.

What penalties will telcos, social media companies and banks face under the code?

The Framework will provide regulators with powers to monitor, investigate and enforce compliance. Broadly, the powers of the regulators align with existing powers of the ACCC under the CCA or otherwise incorporate by reference Parts of the Regulatory Powers Act.

The amendments set out the maximum penalties for contravention of the civil penalty provisions by the regulated entity. There are two tiers of contraventions, of which tier 1 will attract a higher maximum penalty than tier 2. This approach reflects that higher penalties will be imposed on obligations where breaches would be the most egregious and result in significant impact on consumers.

Who will administer the code?

Oversight of the Framework will be undertaken by ACCC as the general regulator. The sector regulators will be ACCC for digital platforms, ACMA for telcos and ASIC for banks.

Where/how will disputes be managed under the regime?

Disputes will be managed via mandated internal dispute resolution schemes in the first instance and then escalated to the single external dispute resolution scheme where required.

Can you provide examples of obligations for each sector?

Prescriptive obligations for each sector will be further defined by sector specific codes. However, the Framework sets out overarching principles that regulated entities must adhere to.

Governance

- Regulated entities will be required to have strict arrangements in place to develop, implement and review governance policies, procedures, metrics and targets to combat scams.

Prevent

- Regulated entities will be required to undertake reasonable steps to prevent scams, including assisting consumers to identify and minimise risk of harm. This includes preempting scams that may have not yet impacted a consumer.

Detect

- Regulated entities will be required to take reasonable steps to detect scams within the sector as well as identify consumers that are or could be impacted by a scam in a timely way. This includes financial and non-financial harm, such as the loss of personal information.

Report

- Regulated entities must give the general regulator reports of any actionable scam intelligence the entities hold and report on an instance when requested by the general or sector regulator.

Disrupt

- Regulated entities will be required to take reasonable steps to disrupt scams and prevent losses or harm from scams. This principle includes the provision of actionable scam intelligence to the general regulator, and the consumer, enabling them to take appropriate steps to disrupt the scam.

Respond

- Regulated entities must have accessible mechanisms for consumers to report scams and an accessible and transparent internal dispute mechanism in place for consumers to complain about scams.
- To provide a regulated service in Australia regulated entities must be a member of an external dispute resolution scheme.

SCAMS

Headline Statement

- The Government is delivering its election commitment to combat scams through an economy-wide reform to introduce strong enforceable obligations on industry through its Scam Prevention Framework; and to improve scam awareness and support for consumers and businesses.

Key Points

- Scam losses remain unacceptably high, with \$2.7 billion reported losses in 2023. However, anti-scam measures of government and industry have started to show signs of success in stabilising the upward scams trend, with losses in 2023 being 13 per cent lower than in 2022 (or \$0.4 billion).

Policy Commitments

Scams Prevention Framework

- The Government consulted on Exposure Draft legislation to establish the Scams Prevention Framework (the Framework) from 13 September to 4 October 2024.
 - The Framework will establish high-level scam prevention principles, which will be complemented by codes outlining industry-specific mandatory obligations for designated sectors. The Framework design will allow flexibility to tailor obligations for each sector, and enable responsiveness to make changes as scam trends evolve.
 - The Framework principles will establish obligations to prevent, detect, report, disrupt, and respond to scams, and to require businesses to have governance systems.
 - The Government is considering consultation feedback to inform finalisation of the bill for introduction to Parliament this year.
- The Government has announced it intends to designate three initial sectors to be subject to the Framework: banks, telecommunications providers and digital platforms providing social media, paid search advertising and direct messaging.

Contact Officer:

Name: **s 47F**
Division: Market Conduct Division
Telephone: **s 47F**
Last updated: 22/10/2024 8:40:00 PM

- The Government has also announced its intention to authorise the Australian Financial Complaints Authority (AFCA) as the single external dispute resolution (EDR) scheme for scams complaints in the first three designated sectors.
 - The single EDR scheme will provide scam victims with a clear pathway for redress where one or more regulated entities has done the wrong thing, and the consumer is unable to reach a satisfactory outcome through internal dispute resolution.
 - The Telecommunication Industry Ombudsman and AFCA will continue to operate to consider non-scam complaints for their relevant industry members.

2024-25 Budget measures

- The Government provided \$67.5 million over four years in the 2024-25 Budget to continue its action to combat scams and online fraud, including:
 - \$1.6 million for the Treasury to develop and legislate the overarching framework legislation.
 - \$37.3 million (and \$8.6 million ongoing) for Australian Competition and Consumer Commission (ACCC), Australian Securities and Investments Commission (ASIC) and Australian Communications and Media Authority (ACMA) to administer and enforce the framework.
 - \$6.3 million for the ACCC to deliver a consumer education media campaign, to improve public awareness of the threat of scams and Australians toward better information to identify and report scams.
 - \$23.3 million to support adoption of eInvoicing to disrupt payment redirection scams, improve cash flow and boost productivity for small businesses.

SMS Sender ID Registry

- The Government provided the ACMA \$10 million to launch and maintain an SMS Sender ID Registry, to prevent spoofing of trusted brand names.
- The *Telecommunications Amendment (SMS Sender ID Register) Act 2024* received Royal Assent on 5 September. A decision on whether the Register will be voluntary, or mandatory is expected by the end of 2024.

Background

- The Government made an election commitment to introduce measures to combat scams and online fraud, including establishing the National Anti-Scam Centre (NASC) and establish new mandatory industry codes to clearly define responsibilities for industry to protect consumers from scams.

Scam losses

- In April 2024, the NASC published the Targeting Scams report which shows:
 - 602,000 scam reports, a 19 per cent increase compared to the preceding year.
 - the greatest losses were associated with scams relating to investment (\$1.3 billion), remote access (\$256 million), romance (\$201 million), phishing (\$137 million) and payment redirection (\$92 million).
 - financial losses decreased in the second half of 2023 by 21 per cent compared to the first half of the year.

Anti-scam responses in key sectors

- On 24 November 2023, the Australian Banking Association and Community Owned Banking Association launched the 'Scam-Safe Accord' as a sector-wide agreement for members to implement measures that disrupt, detect, and respond to scams over 2024 to 2025.
- On 26 July 2024, the Digital Industry Group Inc. (DIGI), the industry association for digital platform service providers launched the 'Australian Online Scams Code'. The code applies to social media, peer-to-peer marketplaces, email, messaging, video sharing and paid advertising on digital platforms.
- The *Reducing Scam Calls and Scam SMS Code* in the telecommunications sector was initially introduced in 2020 (and updated in 2022). Under the code, telecommunications providers have reported blocking over 156.8 million scam calls and over 134.6 million scam SMS in the second quarter of 2024.
- Since the Government's announcement of ASIC's website takedown service in July 2023, ASIC have taken down over 7300 investment scam websites. The NASC is using intelligence gathered from industry and the public to coordinate takedown activity with ASIC.

Consultation on the Scams Prevention Framework

- The Government's consultation on Exposure Draft legislation for the Scams Prevention Framework involved:
 - a virtual information session, with around 200 attendees.
 - Treasury and DITRDCA holding nine roundtables and bilateral meetings with key sectors covering banking, payments, telecommunications, digital platforms, consumer groups and regulators.

- feedback received through over 80 formal submissions, including around a dozen confidential submissions.
- The Framework is proposed to be set out in the *Competition and Consumer Act 2010*, to:
 - Enable the Minister to designate sectors and establish sector-specific codes. The Codes will impose mandatory obligations on designated sectors to combat scams.
 - Mandate designated sectors to have internal dispute resolution mechanisms that are accessible and transparent for customers.
 - Enable an EDR scheme to be nominated for all scam complaints made under the Framework.
 - Build a coordinated intelligence sharing ecosystem by mandating timely reporting and information sharing across industry and government.
- The design of the Framework has been informed by consultation on a proposed model, which was undertaken between 30 November 2023 to 29 January 2024.

Dispute resolution under the Scams Prevention Framework

- The Framework will establish obligations on regulated businesses in related to internal and external dispute resolution for consumers.
- The Government’s intention to nominate AFCA as the single EDR scheme will expand AFCA’s jurisdiction to telecommunications service providers and certain digital platforms in relation to scams. This represents a significant expansion to AFCA’s existing complaints remit.
 - Leveraging AFCA’s existing EDR infrastructure and expertise is essential to ensure a single scheme can be in place from commencement of sector codes under the SPF.
 - AFCA has significant experience in managing and resolving complaints, receiving more than 100,000 complaints about financial firms each year. In 2023-24, approximately 11,000 of these were scam-related complaints.
 - AFCA would be expected to:
 - : consult on and make updates to its rules and processes,
 - : update public facing guidance and information,
 - : develop and update its funding model, and
 - : engage with other relevant EDR bodies such as the Telecommunications Industry Ombudsman to ensure effective referral mechanisms or other arrangements.
 - Once AFCA has established the capacity to handle scam complaints, the EDR scheme will be industry funded through fees and membership charges.

The National Anti-Scam Centre

- The NASC, launched on 1 July 2023, is coordinating efforts to address scams by improving intelligence sharing across Government and the private sector, and raising public awareness.
- The NASC is coordinating a series of time-limited taskforces known as ‘fusion cells’ to explore proof of concepts and solutions to disrupt scams.
 - The first fusion cell focused on disrupting investment scams and concluded in early 2024. A key achievement was an initiative that successfully diverted 113 calls from confirmed investment scams numbers, potentially saving millions of dollars in scam losses (around \$264,000 per person on average).
 - The second fusion cell focusses on jobs and employment scams and commenced in September 2024.

eInvoicing

- eInvoicing is the digital exchange of invoice information between the software of a supplier and a business customer’s software, via a secure network, using an internationally accepted standard (the Peppol Framework).
- Standardisation allows eInvoicing to work even if the software used between parties is different, as long as it is eInvoicing enabled.
 - eInvoicing is not sending an invoice via email with a pdf attachment, which may be vulnerable to scammers.
 - In the ACCC 2023 Targeting Scams report, it was reported payment redirection (invoice) scams were the 5th most prominent type of scam reported with \$92 million in losses over 2023. This is down from \$225 million in 2022.
- As of 30 August 2024, 135,582 businesses were registered for eInvoicing - approximately 5 per cent of Australia’s 2.5 million businesses.
- Greater use of eInvoicing would significantly increase businesses protection from invoice scams, improve productivity by digitising and automating manual invoice processes, and reduce payment delays.

2023-24 Budget anti-scam measures

- The Fighting Scams 2023-24 Budget package included \$86.5 million to establish the NASC to enhance public-private collaboration on scams, fund ASIC to take down investment scam websites and to ACMA to develop a SMS sender ID registry to help prevent scammers imitating key brand names in text message headers.