PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

PARLIAMENTARY LIBRARY

Bills Digest | 24 January 2025

Scams Prevention Framework Bill 2024

Josh Gibson
Bills Digest No. 33, 2024–25

Key points

- The Scams Prevention Framework Bill 2024 (the Bill) amends the *Competition and Consumer Act 2010* to establish a framework, known as the Scams Prevention Framework (SPF), to prevent and respond to scams impacting the Australian community. The Bill also makes minor consequential amendments to other legislation.
- In particular, the measures in the Bill will:
  - allow the Minister to designate certain sectors as 'regulated sectors', outline persons who are 'regulated entities', and clarify what constitutes 'regulated services' for the purpose of adhering to SPF requirements
  - introduce principles-based obligations, which require regulated entities to take certain actions in relation to scams, including taking reasonable steps to prevent, detect, report, disrupt and respond to scams relating to services the entity provides. Contraventions of obligations may result in civil penalties
  - authorise the Minister to create sector-specific codes and
  - authorise the appointment of inspectors to monitor and investigate compliance with the SPF principles and SPF codes.
- The Bill does **not** mandate compensating victims of scams. However, the Bill does provide redress mechanisms to consumers where a regulated entity has contravened a civil penalty provision. These include internal and external dispute resolution mechanisms and taking legal action against the entity.
- The Bill was considered by the Scrutiny of Bills Committee on 20 November 2024, and has been referred to the Senate Economics Legislation Committee, with the Report due 3 February 2025.

ISSN 1328-8091

Contents

Date of introduction: 7 November 2024

House introduced in: House of Representatives

Portfolio: Treasury

Commencement: The day after Royal Assent

This Bills Digest replaces a preliminary Digest published on 15 November 2024 to assist in early consideration of the Bill.

Links: The links to the Bill, its Explanatory Memorandum and second reading speech can be found on the Bill's home page, or through the Australian Parliament website.

When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the Federal Register of Legislation website.

All hyperlinks in this Bills Digest are correct as of January 2025.

Purpose and structure of the Bill

The Scams Prevention Framework Bill 2024 (the Bill) implements the Scams Prevention Framework (SPF) through amendments to the *Competition and Consumer Act 2010* (*CCA*) and other related legislation. The Bill consists of 1 Schedule with 2 parts which introduce the SPF to prevent and respond to scams that impact the Australian community.

To achieve this, the Bill inserts proposed Part IVF into the *CCA* (Part 1 of the Bill) and makes other technical amendments (Part 2 of the Bill). Part 1 of the Bill:

- allows the Minister to designate 'regulated sectors', which enlivens SPF obligations, and defines 'regulated entities' and 'regulated services' (Division 1)
- introduces principles-based obligations, which require regulated entities to detect, prevent, report and disrupt scams. Additionally, regulated entities will be required to maintain corporate records, report certain information to regulators, and establish dispute resolution frameworks for consumers subject to scams (Division 2)
- allows the Minister to make sector-specific codes which accord with the SPF principles (Division 3)
- allows the Minister to authorise external dispute resolution schemes (Division 4)
- designates the Australian Competition and Consumer Commission (ACCC) as the 'SPF general regulator' and allows for the appointment of other Commonwealth entities as 'sector regulators' (Division 5)
- authorises the appointment of inspectors to monitor and investigate compliance with the SPF principles and SPF codes (Division 6) and
- provides mechanisms for the recovery of damages for scam victims as a result of contravention of civil penalty provisions by a regulated entity, as well as other non-punitive orders (Division 6).

Background

Australians lose billions of dollars to scams each year. Reported financial losses from scams in Australia in 2023 amounted to at least $2.74 billion (p. 1), although the figure is likely higher, as it is understood that many scams are not reported. While this is a decrease from the $3.1 billion lost to scams in 2022, the 2023 losses remain higher than the annual losses in both 2020 and 2021. Moreover, around 601,000 scams were reported during 2023, which reflects an 18.5% increase over the 2022 reporting period. Investment scams, which accounted for approximately $1.3 billion of total scam losses in 2023, are overwhelmingly the largest source of these financial losses (Targeting losses: report of the National Anti-Scam Centre on scams activity 2023, p. 4).

A number of different government and non-government entities currently monitor and regulate scam activity, including the National Anti-Scam Centre (NASC), the Australian Securities and Investments Commission (ASIC), the Australian Financial Complaints Authority (AFCA) and the Australian Financial Crimes Exchange (AFCX). Additionally, a range of government and industry measures have been developed, or are currently in development, to address scam threats. These include the Scam-Safe Accord (a banking sector code), the Australian Online Scams Code (signed by several social media companies), the Reducing Scam Calls and Scam SMs Industry Code (a telecommunications industry code), and the SMS Sender ID Register.

Despite this, the Explanatory Memorandum (EM) for the Bill states that:

> Current scam protections are **piecemeal and inconsistent** across the economy. As a result, Australian consumers face **inconsistent protections** with differing service providers. While some sectors have industry codes to address scam activity, other sectors have no formal scam protection requirements, providing scammers with an avenue to target consumers. [emphasis added] (p. 4)

As Stephen Jones (Minister for Financial Services) has noted, there is currently 'no clear obligation' on banks, telecommunications companies or social media platforms in relation to scam management. Moreover, whilst there has been a 'downward trend' in scam-related financial losses during 2023–24, the ACCC notes 'there still remains much important work to be done' (ACCC annual report 2023–24, p. 8).

The Bill has been developed for the purpose of addressing these concerns. The Treasury undertook public consultation in relation to an Exposure Draft (ED) of the Bill from 13 September 2024 until 4 October 2024. During this period, 85 stakeholder submissions were received. The final form of the Bill was introduced into the House of Representatives on 7 November 2024.

Policy position of non-government parties/independents

In his 2023 Budget Reply speech the Leader of the Opposition, Peter Dutton, stated that a Coalition Government would 'impose more onerous obligations on big digital companies to stop scams and financial fraud'.

Several independent members of Parliament have spoken about scams in the context of the Bill (including the ED). On Wednesday 11 September 2024, Zali Steggall raised the topic of scams as a matter of public importance. Several independent MPs spoke about the growing risk of scams, including Dr Sophie Scamps, Kate Chaney, Kylea Tink, Dr Helen Haines and Zoe Daniel. On another occasion Dai Le spoke about how scams in Australia particularly impact vulnerable persons including non-English speaking migrants.

Several independent MPs, including Dr Monique Ryan and Allegra Spender, have articulated concern that the ED did not contain a scams reimbursement model for consumers, and have shown support for a mandated reimbursement scheme similar to the United Kingdom (UK) reimbursement scheme (discussed in Table 1 below).[1] Senator David Pocock has stated that a scam reimbursement model 'is the most effective means of getting financial institutions to take this seriously and reduce scam losses'.

Members of Parliament who have introduced proposed amendments to the Bill include Dr Sophie Scamps, Allegra Spender, and Zali Steggall.

1 The UK reimbursement scheme is intended to incentivise all businesses involved in payments (p. 6) 'to take more action to prevent scam activity, in part due to the fact that reimbursement costs will be split 50:50 between the bank that sends and the bank that receives the payment'.

Key issues and provisions

What sectors, services and entities will be regulated by the SPF?

The Minister may, by legislative instrument, designate ***regulated sectors***, which would be subject to SPF obligations: **proposed subsection 58AC(1)** of the *CCA* **(item 1** of the Bill constitutes all provisions referred to below unless otherwise specified). Both **individual** businesses and services, and **classes** of businesses and services could be designated.

The type of businesses or services that may be designated under the Bill are defined non-exhaustively, but are reliant on the Commonwealth's constitutional powers. They may include (**proposed subsection 58AC(2)**):

- banking businesses
- insurance businesses and
- postal, telegraphic, or telephonic services, including carriage, electronic (such as social media services) and broadcasting services.

A banking, insurance or communications business or service of a regulated sector is a ***regulated service***, and a person who is engaged in such a business or service is a ***regulated entity***: **proposed subsection 58AD(1)**. Other businesses or services may also be regulated services, and persons engaged in such businesses or services may be regulated entities: **proposed subsection 58AD(2)**. Complete or partial exceptions to these definitions may be provided under the SPF rules (made pursuant to **proposed section 58GE**), or under an instrument that designates a regulated sector: **proposed subsections 58AD(4)-(5)**).

Before designating a regulated sector, the Minister must consider certain things including scam activity in the sector, the interests of consumers if the sector became a regulated sector, the likely consequences for the public, and any other relevant matters: **proposed section 58AE**.

What constitutes a 'scam'?

The Bill defines ***scam*** as a direct or indirect attempt (whether successful or otherwise) to engage an ***SPF consumer*** of a regulated service in a way that it would be reasonable to conclude involves deception (an attempt that involves deception is explained in **proposed subsection 58AG(2)**) and, if successful, would cause loss or harm: **proposed section 58AG**. As stated in the EM (p. 15), the definition of scam 'is deliberately broad to capture the wide range of activities scammers engage in and their ability to adapt and to adopt evolving behaviours over time.'

Meaning of 'SPF consumer'

An 'SPF consumer' is defined as a natural person or small business operator who is provided a service in Australia, or a natural person who is ordinarily resident in Australia but is provided a service outside of Australia by a regulated entity that meets certain taxation-related residency requirements: **proposed section 58AH**.

Who are SPF regulators?

There are 2 types of SPF regulators established in the Bill:

(1) SPF general regulator

The ACCC is the regulator (referred to as the ***SPF general regulator***) for all provisions except for SPF codes (discussed below): **proposed section 58EB**. The ACCC's functions and powers for the purposes of the SPF include:

- reviewing and advising the Minister about the operation of SPF provisions
- exercising existing functions outlined in section 155 of the *CCA* (power to obtain information, documents and evidence) to the extent it relates to SPF provisions and
- developing and publishing non-binding guidance material relating to SPF provisions.

(2) SPF sector regulators

The Minister may, by legislative instrument, designate a Commonwealth entity to be the ***SPF sector regulator*** for a particular regulated sector: **proposed section 58ED**. For instance, it is expected that the Australian Communications and Media Authority (ACMA) will be designated as the sector regulator for the media and telecommunications sector, and ASIC as the banking sector regulator. Other agencies may also be designated SPF sector regulators (EM, p. 81).

If ACMA is authorised as an SPF sector regulator, then Part 26 (Investigations) and Part 27 (ACMA's information-gathering powers) of the *Telecommunications Act 1997* apply for SPF purposes: **proposed section 58FG**.

If ASIC is authorised as an SPF sector regulator, then certain provisions of the *Australian Securities and Investments Commission Act 2001* (being Divisions 1, 2, 3 (other than sections 30A, 30B and 39A), 7, 9 and 10 of Part 3, which relates to investigation and information gathering) apply for SPF purposes: **proposed section 58FH**.

Ministerial powers to make sector specific SPF codes

To regulate specific sectors the Minister may, by legislative instrument, make a code (***SPF code***) for each regulated sector: **proposed section 58CB**. Each SPF code must be consistent with SPF principles: **proposed section 58CC**. Specific functions and powers of SPF sector regulators may be contained within an SPF code.

Stakeholder comments on interactions between primary legislation and codes

Some stakeholders, through submissions to the Senate Economics Committee, noted that the SPF legislation contained complexities and detailed information which may be more appropriate to be included in codes. For instance, the Digital Industry Group Inc (DIGI) (pp. 2–3) recommended that some of the complexity should be removed from the legislation and inserted into codes. Similarly, the Internet Association of Australia (IAA) (p. 2) is 'concerned that [the SPF] is too prescriptive and will be difficult to comply with', and may cause undue burdens on industry and smaller entities. Google (p. 10) notes that having overlapping obligations in legislation and codes makes the Scams Framework 'highly complex to

navigate', which could lead to adverse consequences including risk of duplication of obligations, inconsistent obligations, and an increased burden on industry.

Information sharing between regulators

An SPF regulator may disclose information or documents to another SPF regulator if doing so is relevant to the operation (including enforcement) of the SPF provisions: **proposed section 58EG**. An SPF regulator that discloses information or documents is not required to notify any person of its disclosure actions or intentions: **proposed section 58EI**.

The SPF general regulator is required to enter an arrangement with each SPF sector regulator relating to the regulation and enforcement of SPF provisions: **proposed section 58EF**. These arrangements can include, for example, when disclosures should be made between SPF regulators (see the Note in **proposed section 58EH**).

Regulated entity obligations: what are entities required to do?

Division 2 of **proposed Part IVF** requires entities to comply with principles-based obligations. Regulated entities are required to implement appropriate governance arrangements, report certain information to SPF regulators, and have accessible forums for consumers to report scams. Additionally, an entity must take ***reasonable steps*** (defined in **proposed section 58BB**) to prevent, detect, disrupt and respond to scams.

The Tech Council of Australia (p. 5) welcomes the definition of 'reasonable steps' contained in the legislation, but notes it 'should be further clarified in the codes, with specific reference to what it means for the designated businesses.'

(1) Governance requirements

Regulated entities are required to establish governance policies about how they will prevent, detect, disrupt, respond to and report scams: **proposed paragraph 58BD(1)(a)**. Once established, entities are required to implement their governance policies and create performance metrics and targets assessing the effectiveness of their policies: **proposed paragraphs 58BD(1)(b)–(c)**. Entities must keep records relating to their governance policies for 6 years: **proposed subsection 58BF**. If an entity fails to comply with these requirements, it may be liable for civil penalties.

Governance policies (and associated documents) must be certified annually by a senior officer (defined in **item 5**): **proposed subsection 58BE(1)**. If a senior officer does not certify governance policy compliance within the required timeframes, the entity may be liable for civil penalties: **proposed subsection 58BE(2)**.

(2) Prevention requirements

Regulated entities must take reasonable steps to prevent scam activity from occurring. Taking reasonable steps for the purpose of preventing scam activity requires more than merely acting on ***actionable scam intelligence*** (defined in **proposed section 58AI**) which the entity has received: **proposed subsection 58BK(1)**. If an entity fails to comply with these requirements, it may be liable for civil penalties.

(3) Detection requirements

Regulated entities must take reasonable steps to detect scams related to regulated services they offer. This includes, but is not limited to, taking reasonable steps to detect a scam as it happens or after it happens: **proposed subsection 58BM(3)**. Failure to take reasonable steps to detect scams may result in civil penalties.

Additionally, an entity contravenes requirements if it has in its possession actionable scam intelligence relating to a regulated service, and it fails to take reasonable steps to investigate (within 28 days) whether the activity is a scam: **proposed section 58BN**. Failure to take reasonable steps to investigate may result in civil penalties. Regulated entities may also be liable for civil penalties if they fail to take reasonable steps to identify impacted SPF consumers impacted by scams: **proposed section 58BO**.

(4) Reporting requirements

An entity must report any actionable intelligence it has about scams to the SPF general regulator: **proposed section 58BR**. Failure to report this information may result in civil penalties.

The SPF general regulator may disclose information relating to scams to prescribed entities including Commonwealth agencies, law enforcement agencies, and relevant agencies of foreign countries (being law enforcement or regulatory agencies responsible for scam prevention): **proposed section 58BV**. Information may only be shared with prescribed foreign agencies if the SPF general regulator is satisfied that certain conditions have been met, relating to the storage and use of such information, and that it is appropriate to disclose the information to the foreign agency: **proposed subsection 58BV(3)**.

(5) Disruption requirements

Entities that possess actionable scam intelligence are required to take reasonable steps to disrupt the scam activity or prevent any loss or harm arising from the activity: **proposed section 58BX**. Failure to take reasonable steps may result in civil penalties. The word 'disrupt' is not defined in the Bill or the *CCA*. However, the Bill notes that the reasonable steps taken to disrupt 'should be proportionate to the actionable scam intelligence': **proposed subsection 58BX(3)**. Within this subsection, the Bill provides the example (Note 1) of a bank receiving a substantial number of similar reports of suspicious activities, noting in those circumstances it may be appropriate to pause or delay authorised payments while the bank investigates (satisfying the disruption requirements).

Safe harbour for taking action to disrupt a scam activity

A regulated entity will be provided safe harbour (meaning the entity will not be liable in civil action or civil proceedings) for taking action to disrupt a scam activity, subject to certain requirements: **proposed section 58BZA**. Safe harbour will be provided for action taken during a maximum period of 28 days from when the intelligence became actionable scam intelligence, so long as the actions of the regulated entity are undertaken in good faith, in compliance with the SPF provisions, and are reasonably proportionate to the scam activity: **proposed subsection 58BZA(2)**. To come within the safe harbour, action taken by the entity

must be 'promptly reversed' if the entity identifies that the activity is not a scam and it is reasonably practicable to reverse the action: **proposed paragraph 58BZA(2)(c)**.

(6) Response requirements

Each regulated entity is required to have an accessible mechanism for consumers to report scam-related activities to the entity: **proposed section 58BZC**. Failure to have this mechanism may result in civil penalties.

Internal dispute resolution

A regulated entity must have an accessible and transparent internal dispute resolution (IDR) mechanism to deal with a person's complaint about a scam or scam related activity: **proposed section 58BZD**. SPF consumers will be able to bring complaints about scams relating to an entity's regulated services and about the entity's conduct relating to such scams. If an entity does not have an IDR mechanism it may be liable for civil penalties.

External dispute resolution

Where complaints are not resolved at the IDR stage, or if the IDR outcome is unsatisfactory, consumers can escalate their complaints to an independent and impartial external dispute resolution (EDR) mechanism. The Minister may, by legislative instrument, authorise an EDR scheme (***SPF EDR scheme***): **proposed section 58DB**.

There are two possible types of SPF EDRs that can be established. Firstly, the SPF EDR scheme can be a scheme that is already authorised under Commonwealth law: **proposed paragraph 58DB(1)(a)**. For example, AFCA could be designated: Note 1 to **proposed subsection 58DB(1)**. A Treasury officer stated in Senate Estimates on 6 November 2024 (p. 113) that it was the Government's intention that AFCA, as an SPF EDR, would be 'a one-stop shop' for consumers who have been scammed. Authorising AFCA would enliven ASIC's functions and powers relating to the AFCA scheme for the purposes of the SPF (see: Note 1 of **proposed subsection 58DB(1)**).

Secondly, the Minister may, by legislative instrument, authorise an SPF EDR scheme (that is not currently authorised by Commonwealth law), so long as the Minister is satisfied that certain requirements prescribed in the SPF rules are satisfied: **proposed paragraph 58DB(1)(b)**. If the Minister authorises a scheme, then the SPF rules may prescribe certain requirements which are to be met: **proposed section 58DC**. If an SPF EDR scheme becomes aware of certain contraventions in relation to SPF requirements, then the SPF EDR operator must give particulars to the relevant SPF regulator: **proposed section 58DD**.

A regulated entity must not provide a service if it is not a member of an SPF EDR scheme: **proposed section 58BZG**.

Stakeholder comments

Optus (p. 4) raised concern with the 'scenario of dual liability' between obligations outlined in Division 2 (overarching principles of the SPF) and 3 (sector-specific codes), specifically as applied to the telecommunications industry:

> This duality of liability across Division 2 and Division 3, combined with the drafting of reasonable steps under s. 58BB, leads to regulatory uncertainty and implementation complexity given the highly technical nature of providing telecommunications services and implementing scam detection, prevention and disruption measures across the whole telecommunications ecosystem.

To resolve this, Optus (p. 4) recommends removing the civil liability elements in Division 2 and instead relying on civil liability through industry codes under Division 3 (discussed below).

Enforcing the SPF

Contraventions of the SPF may be enforced by:

- civil penalties
- infringement notices
- enforceable undertakings
- injunctions
- actions for damages
- public warning notices
- remedial directions
- adverse publicity orders and
- other orders (**subdivisions C-L** in **Division 6** of **proposed Part IVF**).

An SPF regulator may appoint an employee of the regulator who holds or performs the duties of an Executive Level 1 position or higher, or a member of the Australian Federal Police as an ***inspector*** (**proposed subsection 58FB(1)**), if they have 'appropriate qualifications, training, skills or experience' to perform the role: **proposed subsection 58FB(2)** (EM, pp. 80–81). An inspector will have specified powers with respect to monitoring and investigating compliance with the SPF. If an SPF regulator has not appointed an inspector, the regulator itself is taken to be the inspector: **proposed subsection 58FB(4)**.

Default monitoring and investigation powers under the *Regulatory Powers (Standard Provisions) Act 2014* apply to an SPF code for a regulated sector, unless:

- the regulator is ACMA, ASIC, or the ACCC (as these entities have existing monitoring and investigation powers under their own respective legislation) or
- the Minister has declared (under **proposed subsection 58(FI)(2)**) that alternative monitoring and investigation powers apply to an SPF sector regulator in relation to specified provisions of the SPF code (**proposed sections 58FE** and **58FF**).

Civil penalties

Regulated entities that fail to comply with obligations in the SPF may be liable for civil penalties: **proposed section 58FJ**. For civil penalties relating to SPF principles outlined in the Bill, the authorised applicant is the ACCC: **proposed paragraph 58FJ(2)(a)**. For civil penalties relating to SPF codes, the authorised applicant is the SPF regulator for the regulated sector:

proposed paragraph 58FJ(2)(b). Civil penalties vary, being either tier 1 contraventions (**proposed section 58FK**) or tier 2 contraventions (**proposed section 58FL**).

Tier 1 civil penalties

A tier 1 contravention is a contravention of a civil penalty provision located in **Subdivisions C (Prevent)**, **D (Detect)**, **F (Disrupt)** or **G (Respond)** of **Division 2** of **proposed Part IVF**. The maximum penalty for a tier 1 contravention for a body corporate is the greater of:

- 159,745 penalty units (currently equivalent to $52,715,850)
- three times the value of the benefit obtained from the contravention or
- if the value of the benefit cannot be determined, 30% of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

The maximum penalty amount for individuals is 7,990 penalty units (currently equivalent to $2,636,700).

Tier 2 civil penalties

A tier 2 contravention is a contravention of a civil penalty provision located in **Subdivisions B (Governance)** or **E (Report)** of **Division 2** of **proposed Part IVF**. The maximum amount for a tier 2 contravention for a body corporate is the greater of:

- 31,950 penalty units (currently equivalent to $10,543,500)
- three times the value of the benefit obtained from the contravention or
- if the value of the benefit cannot be determined, 10% of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

The maximum penalty amount for individuals is 1,600 penalty units (currently equivalent to $528,000).

Infringement notices

Infringement notices can be issued as an alternative to civil penalty proceedings for an alleged contravention of a tier 2 civil penalty provision, or a civil penalty provision of an SPF code: **proposed subsection 58FN(1)**.

To issue an infringement notice, an inspector of the SPF regulator must reasonably believe that a person has contravened a relevant civil penalty provision: **proposed section 58FO**. An infringement notice must be issued within 12 months of the alleged contravention having occurred: **proposed paragraph 58FO(4)(a)**. The infringement notice penalty for a body corporate is 60 penalty units ($19,800), or 12 penalty units ($3,960) for an individual: **proposed section 58FQ**.

Can victims of scams seek damages?

The Bill offers avenues of redress for victims of scams. However, it **does not require** that victims of scams will be mandatorily reimbursed for all, or any, of the monies they have lost to scammers.

It appears that sectors, including the banking sector, will **not** be automatically liable for compensating victims. This differs from the UK reimbursement scheme (discussed in Table 1 below), which will 'require UK payment service providers to reimburse all in-scope customers who fall victim to APP [authorised push payment] fraud, save for limited exceptions'. However, in Senate Estimates on 6 November 2024, a Treasury official stated that 'there are multiple channels that you can go through if you want to pursue redress.' The official listed the IDR and EDR mechanisms, and the ability for victims to seek redress through the court (Proof Committee Hansard, p. 111). Consumers may seek redress (including compensation) through these avenues if a regulated entity has not met their SPF obligations.

IDR and EDR mechanisms to recover loss

As outlined in the EM (p. 55, emphasis added), the IDR mechanism is 'intended to encourage the early resolution of complaints, **including for compensation** or other remedies to be provided to SPF consumers where there has been a breach of an SPF provision.' The SPF EDR scheme is also 'intended to provide a pathway for redress, **including compensation**', for those consumers who fail to resolve their complaints at the IDR stage or if the outcome is unsatisfactory (EM, p. 58, emphasis added).

Scam-victim can take action to recover loss

A person who suffers loss or damage by conduct of another, done in contravention of a civil penalty provision of an SPF principle or SPF code, may recover the amount of loss or damage by taking action against that other person: **proposed subsection 58FZC(1)** (see also EM, p. 98). If the victim provides written consent to the SPF regulator, then the SPF regulator may make a claim for damages on behalf of the victim: **proposed subsection 58FZC(2)**. A claim for damages may be made any time within 6 years of the conduct causing loss: **proposed subsection 58FZC(3)**.

If a court considers it appropriate that a person (the defendant) is liable to pay a penalty for contravening a civil penalty provision as well as pay compensation to a scam victim, but the defendant does not have sufficient resources to pay both, the court must give preference to making an order for compensation: **proposed section 58FD**.

Stakeholder comments regarding consumer redress

Some stakeholders, by way of submissions to the Senate Economics Committee, raised concerns about the redress mechanisms and process. For instance, several stakeholders referred to the complexity in relation to the IDR and EDR processes. Google (pp. 2–3; 7–9) stated that the proposed processes 'are extremely complex and could lead to perverse outcomes'. Google (p. 7) raised the example of proving that an entity's actions were reasonable, which would require an entity to 'adduce in evidence extremely sensitive information about how they combat bad actors', the disclosure of which 'risks the information falling into the wrong hands, thereby facilitating bad actors to circumvent detection and protections.'

Other stakeholders were concerned about uncertainty in relation to how a regulated entity should bear losses, and how liability for losses should be apportioned for consumers. As the Telecommunications Industry Ombudsman (p. 6) highlights, this is particularly pertinent given that 'provisions of the SPF Bill do not address the question of multi-party liability for

scam losses … [which] does not answer the key questions consumers who experience losses will have – how do I get my money back? How do I recover my losses?' Google (pp. 7–8) noted that where multiple regulated entities are responsible for a scam, consumers will bear the burden of pursuing claims through multiple forums, which will likely frustrate consumer claims and delay recovery of losses.

Some stakeholders have referred to the potential for including a 'waterfall approach' regarding consumer redress, like Singapore's Scams Framework (discussed in Table 1 below). For instance, Communications Alliance (p. 3) suggested that

> … banks, as custodians of consumers' monies, pay full compensation if found in breach of their sector-specific obligations. If banks are in compliance with their respective obligations but other sector(s) are not, those other sector(s) pay compensation, through a scheme of apportioning compensation …

International comparative scams frameworks

Table 1 UK and Singapore Scams Framework models

	United Kingdom *'Authorised Push Payment Fraud Reimbursement'*	Singapore *'Shared Responsibility Framework'*
When did the policy commence?	Commenced 7 October 2024.	Commenced 16 December 2024.
Which agencies oversee the policy?	UK Payment Systems Regulator.	The Monetary Authority of Singapore and the Infocomm Media Development Authority.
Who is covered by the scams policy?	As stated in the Reimbursement Rules (Rules 3.1, 10.4) victims of scams that are eligible to be reimbursed are: • **individuals** • **microenterprises** (employing fewer than 10 persons and not exceeding a certain annual turnover) and • **charities** (with income less than £1 million per year).	Account holders (meaning any person in whose name a payment account has been opened, or to whom a payment account has been issued, including joint account holders): see paragraph 2.1 of the Guidelines on Shared Responsibility Framework (SRF Guidelines).
What type of scams are covered?	Authorised Push Payment (APP) scams. The UK Payment Systems Regulator (PSR)[2] has stated that 'APP fraud happens when someone is tricked into sending money to a fraudster via bank transfer'.	Phishing scams (paragraph 3.1), which are scams where consumers are deceived into clicking on a phishing link and entering their credentials on a fake digital platform, which is often impersonating a legitimate business or government entity.

2 The PSR is the independent regulatory body in the UK that oversees and regulates payment systems. As outlined on the PSR website, in 2023 PSR oversaw a total value of £102 trillion worth of payments.

	United Kingdom *'Authorised Push Payment Fraud Reimbursement'*	Singapore *'Shared Responsibility Framework'*
What entities are captured?	Sending Payment Service Providers (PSP) (that is, financial institutions which the consumer payment was made from) (Reimbursement Rules, Rules 3.1–3.5) and receiving PSPs (that is, the financial institutions receiving the scam payments) (Reimbursement Rules, Rules 5.1–5.4).	As stated in paragraph 1.1 of the SRF Guidelines, entities regulated include: • Banks and relevant payment service providers and • Mobile network operators.
What is the required connection to the country?	Payments are covered if they are made within the UK – consumers are not covered for payments sent overseas (UK Finance).	A 'clear' Singapore nexus, meaning that the scammer is either Singapore-based, or based overseas but offering services to Singapore residents (p. 6, para 3.1).
Who pays the reimbursement, and how does it work?	Payment service providers (PSPs) who provides services to persons for the purposes of enabling the transfer of funds are liable for reimbursement (Reimbursement Rules, Rule 4.14). Both the sending and receiving firms are to split the reimbursement cost 50:50. However, in practice decisions on reimbursement are made exclusively by the *sending* PSP, which could later recover certain amounts from the *receiving* PSP (Reimbursement Rules, Rule 5.7).	Losses from scams are to be shared across scam victims, financial institutions, and mobile network operators (see paragraphs 6.1–6.9 of the SRF Guidelines). The operational workflow is undertaken in four stages: claim stage, investigation stage, outcome stage, and recourse stage (see paragraphs 7.1–7.14 of the SRF Guidelines for further details, including which person has responsibilities at each stage). The Monetary Authority of Singapore has provided an infographic workflow of the stages.

	United Kingdom *'Authorised Push Payment Fraud Reimbursement'*	Singapore *'Shared Responsibility Framework'*
What is the maximum reimbursement amount?	£85,000 (approximately $168,000 AUD). While £85,000 is the standard, 'banks and payment firms can still reimburse above that amount'. Any amount a Sending PSP reimburses beyond the maximum amount is considered 'a Voluntary reimbursement'. A Sending PSP cannot request reimbursement from the Receiving PSP for a Voluntary reimbursement (Reimbursement Rules, Rule 3.7).	In relation to a scam, a financial institution will first assess whether it breached its SRF duties. If it breached its duties, it will be expected to pay the consumer.[3] A telecommunication company will then assess whether it has breached its duties, and if so, will also be expected to pay the consumer. A telecommunication company will only bear losses when a responsible financial institution complies with all of its duties, and the loss arises because of the telecommunication company's non-compliance (paragraph 6.4 of the SRF Guidelines). If relevant financial institutions and telecommunication companies have *not* breached their duties, there will be no payout required to the consumer.

3 As stated in paragraph 6.2 of the SRF Guidelines, the responsible financial institution 'is expected to bear *any* loss' if such loss arises from non-compliance by the institution (emphasis added).

	United Kingdom *'Authorised Push Payment Fraud Reimbursement'*	Singapore *'Shared Responsibility Framework'*
What are entities required to do to prevent scams?	There appears to be somewhat limited guidance on what relevant entities are required to do to prevent APP Fraud. However, the Financial Conduct Authority, the conduct regulator for approximately 50,000 financial service firms and markets in the UK, published on 7 October 2024 its expectation for PSPs regarding their role in preventing fraud. This includes that: > PSPs should be working to reduce APP fraud by improving their anti-fraud systems and controls. This is also the best way for PSPs to limit their potential liability. These systems and controls, including at onboarding and through ongoing transaction monitoring, firstly help to prevent customers from falling victim to APP fraud, and secondly help to identify fraudsters and prevent them from receiving payments. Ongoing monitoring will help to improve PSP involvement in any available data sharing initiatives (p. 3).	Financial institutions are required to adhere to five duties (see paragraph 4.2 of the SRF Guidelines): 1. a 12-hour cooling-off period upon activation of digital security tokens 2. real-time notification alerts for the activation of digital tokens 3. real-time outgoing transaction notifications 4. a 24/7 reporting channel and self-service feature ('kill switch'), allowing users to report and block unauthorised access to their accounts and 5. real-time fraud surveillance systems to detect unauthorised transactions. Telecommunication companies are required to adhere to three duties (see paragraph 5.2 of the SRF Guidelines): 1. deliver Sender ID SMS to subscribers only if it is received from authorised aggregators 2. block Sender ID SMS which are received from sources other than authorised aggregators and 3. implement an anti-scam filter for all SMS to determine if any contain malicious URLs.
Are there circumstances where PSPs are not required to reimburse persons?	In some circumstances, PSPs may not be required to reimburse consumers including where the consumer has been complicit in the fraud or grossly negligent. Additionally, consumers may not be eligible for reimbursement if they did not comply with prescribed standards (Reimbursement Rules, Rule 3.6).	Excluded from the framework (pp. 8–9, para 4.4) are: • Scams where the victims authorise payments to the scammer which victims intended to be performed at the point of the transaction • Scams where a person provided credentials via text messages, and through non digital means including phone calls or face-to-face and • Unauthorised transaction scams not involving phishing (including hacking, identity theft, and malware-enabled variants)

Source: as compiled by the Parliamentary Library, from hyperlinked sources in Table 1.

Acknowledgement of Country

We acknowledge the traditional owners and custodians of country throughout Australia and acknowledge their continuing connection to land, waters and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

The Parliamentary Library of Australia was established in 1901 and serves as a trusted source of information, analysis and advice for the Australian Parliament. The Library is part of the Department of Parliamentary Services.

Our services are confidential, impartial, and offered on an equal basis to all parliamentarians, parliamentary committees, and to staff acting on their behalf.

Our published material is available to everyone at:

aph.gov.au/library

Australian Parliamentary Library

@ParlLibrary

Confidential, Impartial, Timely

ISSN 1328-8091