FOI 3798 - Document 1

From: Bec Turner
To: Robertson, Belinda
Subject: Global Signals Exchange Announcement
Date: Friday, 11 October 2024 4:03:58 PM

You don't often get email from s 47F @google.com. Learn why this is important

Hi Belinda,

Thanks for your time on the phone earlier this week!

We are pleased to share Google's recent announcement in relation to scams and intel sharing.

We announced a partnership with the Global Anti-Scam Alliance (GASA) and the DNS Research Federation (DNSRF) to launch the Global Signal Exchange (GSE). The GSE is a first-of-its-kind platform that serves as a global clearinghouse to exchange scams and fraud bad actor signals.

Here is a blog post should you be interested in learning more we would be more than happy to brief you and/or the Minister.

Cheers,

Bec

Bec Turner
Government Affairs and Public Policy
Google Australia
s 22 @google.com
s 22

Read the latest Google and YouTube reports
See what's trending in Australia today

FOI 3798 - Document 2

From: Lucinda Longcroft
To: Stephen Jones MP (DPS - Unclassified DLM); Robertson, Belinda
Cc: Stef Lovett
Subject: Google Australia update
Date: Friday, 1 November 2024 11:19:02 AM

You don't often get email from s 47F @google.com. Learn why this is important

Dear Stephen and Belinda,

I wanted to thank you for open and collaborative engagement over the past five years, as I step away from my role at Google Australia. I've loved working with you to share understanding of Google's role in tech and innovation and the needs of the wider tech ecosystem, to listen and respond to your questions and concerns, and to work together to realise the positive benefits of technology for Australians.

I'm so proud of what our team has achieved, most particularly the Digital Future Initiative for Australia which brings $1b and Google's skills and unique technologies to help build a stronger digital future and partner to solve the challenges we face as Australians. I look forward to seeing Australia's innovation and information ecosystem thrive.

My colleague, Stef Lovett, will take the interim lead role from Monday, and brings her long and respected experience of government affairs and public policy to the position and to our engagements.

It's been a privilege to have served in this role and I've loved our work together. I will continue to support and champion the role of technology for our society going forward.

If you would like to stay in touch, my email is s 47F @gmail.com and my phone number is s 47F .

Thanks again! Wishing you the best of success.

warm regards,

Lucinda

Lucinda Longcroft
Director, Government Affairs & Public Policy, Australia and New Zealand
s 47F @google.com
s 47F

Me!

Tue, 24 Sep at 12:23 pm

You missed a call, but the caller didn't leave a message.

Hi Belinda, I wonder if you might have a couple of minutes at some point for me to share a heads up on a new AI product we're introducing in Australia? Best regards, Lucinda

Tue, 24 Sep at 3:41 pm

Hi Lucinda .. I'm free until 4pm and then at 5pm. Cheers Bel

Mon, 28 Oct at 5:17 pm

You missed a call, but the caller didn't leave a message.

Mon, 28 Oct at 6:34 pm

Hi Belinda, thanks for calling back - I can speak now, though as it's not time sensitive I could call tomorrow if that's easier? Best wishes, Lucinda

FOI 3798 - Document 4

FOI 3798 - Document 5

From: Assistant Treasurer
To: s 47F @google.com
Subject: Invitation - The Scams Prevention Framework: keeping Australian's money safe [SEC=OFFICIAL]
Date: Thursday, 3 October 2024 2:49:01 PM

OFFICIAL

Dear Lucinda,

I hope you and your colleagues can join me next week as I provide an address – hosted by Australia's leading class action law firm Maurice Blackburn and independent public policy think tank Per Capita – on the Albanese Labor Government's landmark legislation to establish the Scams Prevention Framework.

Time: 10:00am-11:00am
Date: Friday 11 October
Location: Maurice Blackburn Offices, Level 21, 380 La Trobe St, Melbourne
RSVP: Online

Scammers are a scourge on a modern, digitally enabled society. Under the previous government, scam losses doubled and doubled again in their final 2 years of government to exceed $3 billion. Scams cause not only economic loss, but emotional damage and mental strain for victims, their families, and friends. They also undermine trust in modern e-commerce and how we use technology.

Since being elected in 2022, the Albanese Labor Government has undertaken a series of measures aimed at making Australia the toughest target in the world for scammers. Labor's approach has led to 2024 being the first year since 2016 where losses to scams reduced.

The latest phase of this work is the introduction of world-leading legislation – the Scams Prevention Framework – to place clear obligations on businesses to stop scammers, and strong penalties of up to $50 million for failure to meet their responsibilities to protect consumers. The Framework establishes scam prevention principles in legislation that will guide industry-specific, mandatory obligations on designated sectors. The principles create obligations to Prevent; Detect; Report; Disrupt; and Respond to scams, and to establish governance systems accordingly.

Taking an ecosystem approach, the Framework will require sectors where scams originate – such as digital platforms or telecommunications – and where money is lost – such as the banking sector – to take action to protect Australians from scam activity.

The address will be followed by a Q&A session and morning tea.

I hope that you can join me on this occasion.

Sincerely,

Stephen Jones MP

Assistant Treasurer and Minister for Financial Services

s 22

From: Robertson, Belinda
Sent: Wednesday, 6 November 2024 2:52 PM
To: s 22 Bec Turner
Cc: s 22
Subject: UNDER EMBARGO: Final Scams Prevention Framework Bill 2024 [SEC=OFFICIAL]
Attachments: EM_Scams Prevention Framework.pdf; Bill_Scams Prevention Framework.PDF

Hi s 22 Bec

Please find attached the *Scams Prevention Framework Bill 2024* and associated EM that will be introduced into the House of Representatives tomorrow morning (time TBC).

These documents are provided **UNDER EMBARGO** until they are tabled in the House tomorrow.

Please don't hesitate to reach out if you have any questions.

Kind regards
Belinda

Belinda Robertson — **Chief of Staff**
Office of the Hon Stephen Jones MP | Assistant Treasurer & Minister for Financial Services
Mobile: s 22
Email: s 22 @treasury.gov.au
Address: M1.27 Parliament House Canberra ACT 2600

2022–2023–2024

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

SCAMS PREVENTION FRAMEWORK BILL 2024

EXPLANATORY MEMORANDUM

(Circulated by authority of the Assistant Treasurer and Minister for Financial Services, the Hon Stephen Jones MP and Minister for Communications the Hon Michelle Rowland MP)

Table of Contents

Glossary

This Explanatory Memorandum uses the following abbreviations and acronyms.

Abbreviation	***Definition***
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ACMA Act	*Australian Communications and Media Authority Act 2005*
AFCA	Australian Financial Complaints Authority
ASIC	Australian Securities and Investments Commission
ASIC Act	*Australian Securities and Investments Commission Act 2001*
Bill	Scams Prevention Framework Bill 2024
CCA	*Competition and Consumer Act 2010*
Corporations Act	*Corporations Act 2001*
EDR	External dispute resolution
IDR	Internal dispute resolution
ITAA 1936	*Income Tax Assessment Act 1936*
ITAA 1997	*Income Tax Assessment Act 1997*
NASC	National Anti-Scam Centre
PGPA Act	*Public Governance, Performance and Accountability Act 2013*
Privacy Act	*Privacy Act 1988*

Regulatory Powers Act	*Regulatory Powers (Standard Provisions) Act 2014*
SPF	Scams Prevention Framework
Telecommunications Act	*Telecommunications Act 1997*

General outline and financial impact

Scams Prevention Framework

Outline

The Bill implements a legislative framework to prevent and respond to scams. The amendments introduce a framework with overarching principles and a multi-regulator framework, and enables sector codes to be made and an EDR scheme to be authorised.

Date of effect

The Bill commences the day after Royal Assent.

Proposal announced

The Bill implements the Government's election commitment to require social media companies, banks and telecommunications providers to take robust steps to prevent and respond to scams impacting consumers, announced on 29 November 2021.

It also partially implements the 2024-25 Budget Measure titled 'Fighting Scams', by facilitating the introduction of mandatory industry codes to be established under a whole-of-economy legislative framework.

Financial impact

The Bill is estimated to have a negative impact of $51.9 million in underlying cash balance over the four years to enable regulators to administer and enforce the SPF and provide seed funding for AFCA to establish EDR rules and processes for the SPF. ASIC and ACMA functions will be subject to cost recovery arrangements.

All figures in this table represent amounts in $million, rounded to the nearest $0.1 million each year.

	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

Impact Analysis

The Impact Analysis relating to this Bill has been included at Attachment 1.

Human rights implications

The Bill raises human rights issues. See Statement of Compatibility with Human Rights — Chapter 2.

Compliance cost impact

It is estimated that this reform would result in an overall increase in regulatory compliance costs of around $228.8 million in the initial year of operation and $88 million for each year ongoing across entities in industry sectors that the Government has indicated will be designated.

Chapter 1: Scams Prevention Framework

Table of Contents:

Outline of chapter

1.1 The Bill implements a legislative framework to prevent and respond to scams impacting the Australian community, called the SPF. The amendments introduce a framework for regulated entities to implement measures to prevent, combat and respond to scams. The SPF includes the following features:

- overarching principles (SPF principles) that apply to regulated entities;
- sector-specific codes (SPF codes) that apply to regulated entities in certain regulated sectors;
- rules (SPF rules) to support the effective operation of the framework;

- a multi-regulator framework;
- regulatory and enforcement mechanisms, including a two-tier civil penalty framework; and
- dispute resolution mechanisms.

1.2 The legislative framework allows a Treasury Minister to designate sectors of the economy to be subject to the SPF principles, make an SPF code for that sector, and designate a regulator to enforce that code.

1.3 Legislative references in this Chapter are to the CCA unless otherwise specified.

Context of amendments

1.4 The digital economy has revolutionised the way Australians communicate, conduct business, access services and make payments, bringing significant efficiencies to individuals and businesses. These gains in speed and convenience have been accompanied by an evolution of the risks when conducting business, communicating and making payments. This includes a rise in sophisticated scams over recent years, which manipulate consumers and undermine trust in digital services.

1.5 Scammers stole $2.7 billion from Australian consumers in 2023. Scams not only have a financial toll on victims but can also cause psychological and emotional harm. Regardless of the value stolen, the impact on victims can be irreversible.

1.6 The SPF is an economy-wide reform to prevent and respond to scams impacting the Australian community by requiring the private sector to adhere to consistent principles-based obligations and enforceable mandatory codes. The consistent and enforceable approach of the SPF will ensure that incentives and obligations are in place across key sectors where scammers act to cause harm in the community.

1.7 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. As it is common for scammers to use multiple platforms and services to steal from consumers, the SPF will ensure that all participants in the ecosystem are held accountable.

- The telecommunications sector has taken action to combat scams by implementing the Reducing Scam Calls and Scam SMs Code in 2022. It requires telecommunication providers to take steps to identify, trace and block scam calls and messages. The Government also passed

legislation in August 2024 for the SMS Sender ID Register, which will require the telecommunications sector to check whether messages being sent under a brand name match the legitimate registered sender.

- The banking sector plays a pivotal role in the scams ecosystem, with banks usually being the terminating point of a scam when a consumer transfers money to the scammer. In 2023, ASIC found the overall approach to scams strategies and governance in Australia's major banks was variable and less mature than expected, with gaps in scam detection, response and victim support.
- In late 2023, members of the Australian Banking Association and Customer Owned Banking Association committed to implement a range of measures to improve scam protections and consumer outcomes through the industry-led Scam Safe Accord. Since its introduction, banks have reported a disruption of scams through a range of approaches. As part of the Scam Safe Accord, banks, credit unions and building societies are deploying confirmation of payee technology in 2024 or 2025.
- Digital platforms remain a point of vulnerability in the scams ecosystem and have taken limited action to protect Australian consumers from scams. While economy-wide scam losses decreased in 2023, scam losses originating from social media were up by 17 per cent and scam reports were up by 31 per cent. As part of the 5th Interim Report of the Digital Platform Services Inquiry, the ACCC recommended that digital platforms should be required to implement processes to prevent and remove scams, including a notice and action mechanism and verification of certain business users, including advertisers of financial services and products.
- Some digital platforms have begun moving towards improving scam protections, as outlined in the voluntary Australian Online Scams Code, published by the Digital Industry Group Inc. in July 2024. An uplift in protections is welcome, however there needs to be consistency and a common standard adopted by all with binding obligations.

1.8 The Government has committed to initially designating telecommunications services, banking services and digital platform services relating to social media, paid search engine advertising and direct messaging, as each of these sectors represent a significant vector of scam activity. The SPF is responsive and adaptable, and enables other sectors to be brought under the framework where scam harms arise.

1.9 The dispute resolution obligations imposed on regulated sectors will be critical for the effectiveness of the SPF. The SPF will require regulated entities to have an IDR process in place and to become a member of a designated EDR scheme. In September 2024, the Government announced it will authorise the

AFCA as the designated EDR scheme for the three initial sectors designated under the SPF.

1.10 It is intended that there will be a 'no wrong door' approach for IDR and a 'single door' approach for the EDR scheme for the three initial sectors to be designated under the SPF. This means consumers will have access to fair and transparent dispute resolution processes if they are the victim of a scam where a regulated entity has not met its obligations.

1.11 The consumer protections introduced through the SPF will help safeguard the benefits of the digital economy and provide the community with confidence to embrace the efficiency and convenience of the digital economy without fear of exploitation.

1.12 The SPF is being introduced as part of a broader effort to modernise Australia's laws for the digital age and consumer protection agenda. This includes reforms to Australia's privacy laws, payment systems, and money laundering and cyber settings, as well as the introduction of online safety measures, safe and responsible use of artificial intelligence measures, product safety standards, unfair trading practices and Digital ID.

1.13 The transnational nature of scam activity reiterates the importance for global collaboration. The SPF will facilitate further engagement on how economies can disrupt and share intelligence to increase the effectiveness of the fight against scammers.

1.14 The SPF is a robust whole-of-ecosystem approach that will make Australia the toughest target for scammers.

Summary of new law

1.15 The amendments introduce a framework for preventing and responding to scams impacting the Australian community with the following features:

- overarching principles (SPF principles) that apply to regulated entities;
- sector-specific codes (SPF codes) that apply to regulated entities in certain regulated sectors;
- rules (SPF rules) to support the effective operation of the framework;
- a multi-regulator framework;
- regulatory and enforcement mechanisms, including a two-tier civil penalty framework; and
- dispute resolution mechanisms.

1.16 The SPF principles apply to all regulated entities. These principles are enforced by the ACCC as the SPF general regulator (or an appropriately delegated

person or authority) under the CCA. The SPF principles are about governance arrangements relating to anti-scam actions, and preventing, detecting, reporting, disrupting and responding to scams.

1.17 SPF codes will provide sector-specific, prescriptive obligations for each regulated sector that are consistent with the SPF principles. In assessing whether a regulated entity has complied with the SPF principles, a relevant consideration is the extent to which the entity has complied with any relevant SPF code obligations. However, SPF codes will not set out an exhaustive list of obligations to satisfy compliance with SPF principles. Rather, the SPF codes will provide a set of minimum standards that may be directed at addressing sector-specific harms related to scams.

1.18 This means that in some cases, taking reasonable steps to meet one or more of the SPF principles may require a regulated entity to take steps beyond the sector-specific obligations set out in an SPF code.

1.19 An SPF code applies in relation to a regulated sector. An SPF code will be enforced by a designated regulator, known as the SPF sector regulator for the sector.

1.20 The tiered regulatory design of the SPF will be administered and enforced via a multi-regulator model. This will deliver a whole-of-ecosystem approach to enforcement, and leverage existing regulatory relationships, supervision and surveillance frameworks already established by regulators.

1.21 This approach is supported by the ability of the SPF general regulator to delegate its functions and powers to an SPF sector regulator to ensure the effective regulation of regulated sectors.

1.22 Regulated entities that provide a service that is regulated by the SPF must have an accessible and transparent IDR mechanism and become a member of the EDR scheme that is authorised by a Treasury Minister for the regulated sector.

1.23 The Minister's intention is to authorise the AFCA scheme as the single SPF EDR scheme for the initially designated sectors. This will offer SPF consumers a holistic experience where multiple regulated entities are involved in a complaint. It will also bring consistency in consideration of complaints and be less burdensome for SPF consumers and regulated entities when compared with multi-scheme alternatives.

1.24 The SPF enables arrangements for the sharing of information about scams by regulated entities to SPF regulators (including through authorised third-party data gateways, portals or websites), by the SPF general regulator to regulated entities, between SPF regulators in the multi-regulator model, and between SPF regulators and the operator of the SPF EDR scheme. The SPF also enables arrangements for the sharing of information about scams by the SPF general regulator with foreign agencies responsible for scam prevention, provided the SPF regulator is satisfied the foreign agency has given an undertaking to control the storage, handling and use of any information received and that it will be used only for the purpose for which was disclosed to the agency.

1.25 The commencement of the SPF does not in itself impose any obligations on entities until a designation is made with respect to a regulated sector, and that designation instrument is in force (and any transitional arrangements in the instrument are taken into account). Upon designation of a regulated sector:

- regulated entities operating in the sector are then subject to the obligations in the SPF principles, enforced by the ACCC as the SPF general regulator; and
- if an SPF code is made for the sector, regulated entities operating in that sector are then also subject to the obligations in the SPF code, enforced by the relevant SPF sector regulator.

Detailed explanation of new law

Division 1 – Preliminary

1.26 The amendments introduce Part IVF to the CCA, which establishes an overarching SPF. The object of the SPF is to prevent and respond to scams that impact the Australian community that relate to, are connected with, or use certain services.
[Schedule 1, item 1, section 58AA]

1.27 Simplified outlines throughout Part IVF provide a succinct overview of the relevant provisions to assist readers. However, readers should rely on substantive provisions as the outlines are not intended to be comprehensive. The simplified outline in Division 1 provides that:

- The SPF is a multifaceted approach for preventing and responding to scams impacting the Australian community by requiring regulated entities in selected sectors of the economy to take a variety of steps to combat scams relating to, connected with, or using their services.
- Regulated entities must comply with the overarching principles of SPF, which are about governance arrangements relating to scams, and preventing, detecting, reporting, disrupting and responding to scams.
- Under the SPF, a Treasury Minister (or an appropriately delegated authority) may make an SPF code for a regulated sector. An SPF code will generally contain detailed (but not exhaustive) sector-specific obligations for regulated entities to comply with the SPF principles.
- The SPF also provides that a Treasury Minister may authorise an SPF EDR scheme for a regulated sector. An SPF EDR scheme will provide pathways for redress (including compensation) where regulated entities have not met their SPF obligations.

- The ACCC is the SPF general regulator that regulates and enforces compliance with the SPF principles. A Treasury Minister may also select other Commonwealth entities to be SPF sector regulators to regulate and enforce compliance with SPF codes.

[Schedule 1, item 1, section 58AB]

Regulated sectors, entities and services

1.28 The SPF applies to regulated entities in regulated sectors with respect to the regulated services of those entities. A Treasury Minister may designate a sector of the economy to be a regulated sector. A regulated sector covers the businesses or services referred to in the designation instrument. The persons that carry on or provide these businesses or services are the regulated entities subject to the SPF.
[Schedule 1, item 1, sections 58AC and 58AD]

Regulated sectors

1.29 A Treasury Minister may, by legislative instrument, designate one or more businesses or services to be a regulated sector for the purposes of the SPF.
[Schedule 1, item 1, subsection 58AC(1)]

1.30 This designation instrument is subject to Parliamentary scrutiny through the disallowance process and sunsetting.

1.31 The Treasury Minister may designate an individual business or service, or designate businesses or services by class (see subsection 13(3) of the *Legislation Act 2003*). This means that the Minister may in effect designate specific entities to be a 'regulated sector' within a designation instrument.
[Schedule 1, item 1, note 1 to subsection 58AC(1)]

1.32 This legislation-making power is appropriate as the designation instrument may contain complex and specific details to ensure the relevant businesses and services are appropriately described for the purposes of sector designation. This may involve designating an individual person, business or service and is therefore more suited to being set out in delegated legislation.

1.33 The legislation-making power also ensures there is sufficient flexibility for the Government to respond quickly to changing scam methods and trends which may target particular sectors of the economy. A legislative instrument can be made quickly to bring additional sectors into the SPF to require regulated entities in those sectors to uplift their anti-scam practices.

1.34 Alongside the power to designate a sector, a Treasury Minister may also designate a Commonwealth entity to be an SPF sector regulator for a regulated sector (see Division 5 – Regulating the SPF). For example, if the banking sector is a regulated sector, the Minister may designate ASIC to be the SPF sector regulator for that sector in the same or separate instruments.

1.35 The Treasury Minister may vary or repeal the designation instrument once made (see subsection 33(3) of the *Acts Interpretation Act 1901*).
[Schedule 1, item 1, note 2 to subsection 58AC(1)]

1.36 Without limiting the businesses or services that may be designated, a Treasury Minister may designate the following classes of businesses or services to be a regulated sector (or a subset of those business or services):

- banking businesses, other than State banking (within the meaning of paragraph 51(xiii) of the Constitution) not extending beyond the limits of the State concerned;
- insurance businesses, other than State insurance (within the meaning of paragraph 51(xiv) of the Constitution) not extending beyond the limits of the State concerned;
- postal, telegraphic, telephonic or other similar services (within the meaning of paragraph 51(v) of the Constitution), which can include, but is not limited to:
  - carriage services within the meaning of the Telecommunications Act*;*
  - electronic services within the meaning of the *Online Safety Act 2021*, such as social media services within the meaning of that Act;
  - broadcasting services within the meaning of the *Broadcasting Services Act 1992*.

[Schedule 1, item 1, subsection 58AC(2)]

1.37 The description of the businesses and services in the preceding paragraph are based on the relevant constitutional heads of power and provide flexibility for the SPF to be expanded to a wide range of sectors over time. It is not intended to provide a roadmap of the exact sectors the Government is proposing to designate. The Government's intention is to initially designate telecommunications services, banking services and certain digital platform services.

Designation of a regulated sector

1.38 Before designating a sector to be subject to the SPF, the Treasury Minister must consider all the following matters:

- Scam activity in the sector. For example, the Minister may identify that certain businesses or services experience high levels of scam activity.
[Schedule 1, item 1, subparagraph 58AE(1)(a)(i)]
- The effectiveness of existing industry initiatives to address scams in the sector. For example, there may be existing initiatives in a sector seeking to protect against scams but do not appropriately address scam

activity in that sector.
[Schedule 1, item 1, subparagraph 58AE(1)(a)(ii)]

- The interests of persons who would be SPF consumers of regulated services for the sector if the Minister were to make the designation. For example, designation may be appropriate if the Minister considers that consumers would be better protected against scams arising out of activity in a sector if it is subject to the SPF, rather than relying on existing frameworks.
[Schedule 1, item 1, subparagraph 58AE(1)(a)(iii)]

- The likely consequences (including benefits and risks) to the public and to the businesses or services making up the sector if the Minister were to make the designation.
[Schedule 1, item 1, subparagraphs 58AE(1)(a)(iv) and (v)]

- Any other matters the Minister considers relevant to the decision to designate a sector to be subject to the SPF. For example, this could include the compliance and regulatory costs of designating sectors, the privacy or confidentiality of consumers' information, the regulatory impact of designation, the outcomes of consultation with impacted entities and consumers, and scam activity in the relevant sector in another jurisdiction.
[Schedule 1, item 1, subparagraph 58AE(1)(a)(vi)]

1.39 Before designating a sector, the Treasury Minister must also consult relevant consumer groups and the businesses or services making up the sector, or such associations or other bodies representing them as the Minister thinks appropriate. Given the nature and scope of the requirements under the SPF, this is appropriate to ensure consumers and affected entities are given notice of the Government's intention to designate the relevant sector. It will also provide these stakeholders with an opportunity to give feedback on the details of the designation instrument, including on any application provisions or transition period before the SPF comes into effect for the sector.
[Schedule 1, item 1, paragraphs 58AE(1)(b) and (c)]

1.40 This consultation requirement is intended to operate alongside the general consultation requirement in section 17 of the *Legislation Act 2003*. This means the Treasury Minister may undertake additional consultation, including public consultation, on the designation instrument as appropriate.

1.41 Failure by the Treasury Minister to consult consumer groups or the relevant businesses or services, or to consider the above matters in making a designation, does not invalidate the designation instrument. This provides certainty on the regulated sectors within the scope of the SPF. The provision reflects the general position in section 19 of the *Legislation Act 2003* that the validity or enforceability of a legislative instrument is not affected by a failure to consult. This approach also ensures certainty for regulated entities who may

have undertaken investment and preparatory work to comply with the SPF.
[Schedule 1, item 1, subsection 58AE(2)]

Delegation of Treasury Minister's designation power

1.42 A Treasury Minister may, in writing, delegate the power to make an instrument designating businesses or services to be a regulated sector to another Minister. This may be appropriate when the sector sits outside of the Treasury Minister's portfolio and another Minister is responsible for policy matters in that sector.
[Schedule 1, item 1, section 58AF]

1.43 The provisions relating to delegation in sections 34AA to 34A of the *Acts Interpretation Act 1901* apply to a delegation of the Treasury Minister's power to make a designation instrument. For example, under section 34A of that Act, if the Treasury Minister delegates this power to the Communications Minister, then the matters the Treasury Minister must consider before designating a sector and relevant consultation requirements must be satisfied by the Communications Minister before the Communications Minister makes a designation instrument as a delegate.
[Schedule 1, item 1, note to section 58AF]

Regulated entities and their regulated services

1.44 The amendments set out which entities are regulated entities, and the regulated services for those entities, for a regulated sector. A regulated entity for a regulated sector must comply with the obligations of the SPF and any SPF code for the sector, subject to any carve outs. Generally, the obligations are framed by reference to the regulated services of the regulated entity for that sector.

Entities with businesses or services within the banking, insurance or communications constitutional powers

1.45 To the extent that a regulated sector includes a business or service covering banking businesses, insurance businesses, or communication services (within the meaning of paragraph 51(xiii), (xiv) or (v) of the Constitution respectively – see above), or a subset of such a business or service:

- the person who carries on or provides that business or service is a regulated entity for the sector; and
- that business or service if a regulated service of the regulated entity for the sector.

[Schedule 1, item 1, subsection 58AD(1)]

1.46 For example, if banking services were to be designated as a regulated sector, a banking entity that offers both insurance and banking services would only be regulated as part of the banking sector under the SPF for the purposes of its banking services, not its insurance services.

1.47 The designation instrument and explanatory materials will also confirm these matters to ensure affected entities and consumers have a clear understanding of who is a regulated entity and what the regulated services are.

1.48 References to 'person' in the SPF have the same meaning as in section 2C of the *Acts Interpretation Act 1901*, which defines 'person' as encompassing individuals, bodies politic and bodies corporate. Division 7 of the SPF (see below) extends this definition to also cover partnerships, unincorporated associations and trusts.
[Schedule 1, item 1, note 2 to subsections 58AD(1) and (2)]

Other regulated entities and regulated services

1.49 Beyond those entities already discussed, the following entities and services will be regulated entities and regulated services for a regulated sector:

- A corporation (as defined in section 4 of the CCA) that carries on or provides a business or service that is part of the regulated sector. That business or service is a regulated service of the regulated entity for the sector.
- A person to the extent that the person is carrying on or providing a business or service that is part of the regulated sector, and is either:
  - acting using a postal, telegraphic, telephonic or other like service (within the meaning of paragraph 51(v) of the Constitution); or
  - acting in the course of, or in relation to, trade or commerce between Australia and places outside Australia, trade or commerce between the States, or trade or commerce within a Territory, between a State or Territory, or between two Territories (noting this reflects various heads of power under the Constitution).
- The business or service that is part of the regulated sector, to the extent that it relates to the person acting in that way, is a regulated service of the regulated entity for the sector.

[Schedule 1, item 1, subsections 58AD(2) and (3)]

1.50 These provisions are mainly relevant for future sectors that may be designated under the SPF, beyond the Government's intention to initially designate telecommunications services, banking services, and certain digital platform services.

Exceptions

1.51 The SPF rules may specify that a person is not a regulated entity to the extent the specified exception applies to the person.
[Schedule 1, item 1, paragraph 58AD(4)(a)]

1.52 The SPF rules will set out additional detail in relation to information sharing obligations (see SPF Principle 4: Report). It may be appropriate to exclude certain regulated entities or classes of entities in a regulated sector from these obligations, for example, due to their size or role in the scams ecosystem. The SPF rules may exclude certain entities from these obligations where appropriate, to avoid undue regulatory burden. It is appropriate for this exclusion to sit in the SPF rules, so that the scope of information sharing obligations and their application is specified in the same instrument.

1.53 Similarly, the SPF rules may specify that a business or service is not a regulated service of a person for a regulated sector, to the extent that the specified exception applies to the business or service.
[Schedule 1, item 1, paragraph 58AD(4)(b)]

1.54 This may occur, for example, where an entity within a regulated sector is unlikely to be susceptible to a risk of scam harm due to the limited number of SPF consumers that interact with its services.

1.55 In addition, a Treasury Minister may designate a regulated sector, but exclude the application of specified SPF provisions for particular regulated entities or regulated services within the sector. This is appropriate given the SPF is an economy-wide reform and there may be instances where some of the obligations under the SPF are unsuitable for a particular sector or entity. Without this mechanism, these entities and services could not be designated or would be subjected to undue and disproportionate requirements if they were designated, which would limit the effectiveness and benefits of the SPF.
[Schedule 1, item 1, subsection 58AD(5)]

1.56 For example, the Treasury Minister may designate a particular sector or entity only for the purposes of the information sharing provisions under the SPF. This would allow entities within that sector to report information about suspected scams to the SPF general regulator and obtain information from the SPF general regulator (which could enable the entity to disrupt the scam), without contravening the privacy law.

1.57 The SPF rules or designation instrument may specify or declare an individual person, business or service, or do so by class (see subsection 13(3) of the *Legislation Act 2003*).
[Schedule 1, item 1, notes to subsections 58AD(4) and (5)]

Meaning of key terms

1.58 The amendments introduce the following key terms to support the operation of the SPF:

- ‘scam’;
- ‘SPF consumer’; and
- ‘actionable scam intelligence’.

Meaning of scam

1.59 'Scam' is defined to provide certainty on the scope of harms intended to be captured by the SPF.

1.60 A scam is a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:

- involves deception; and
- would, if successful, cause loss or harm including the obtaining of SPF personal information of, or a benefit (such as a financial benefit) from, the SPF consumer or the SPF consumer's associates.

[Schedule 1, item 1, subsection 58AG(1)]

1.61 The elements of the definition of 'scam' are objective in nature and do not require the scammer's state of mind to be established. This definition 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. The SPF rules can also provide an appropriate safeguard to exclude conduct that is not intended to be captured under the SPF.

1.62 The definition of scam captures both successful scams which have caused loss or harm to an SPF consumer, and scam attempts which have not yet resulted in loss or harm to an SPF consumer. This reflects the obligations in the SPF principles (see Division 2), which require regulated entities to take action against scams, regardless of whether the scam has resulted in loss or harm to an SPF consumer or an associate of the SPF consumer.

1.63 The use of 'attempt' in the definition of scam has its ordinary meaning, which is intended to cover efforts made to engage an SPF consumer. There may be an attempt to engage an SPF consumer even if the attempt is indirect, such as where it is directed at a cohort which includes the SPF consumer or is directed at the public more generally.

1.64 The attempt to engage an SPF consumer may be a single act or a course of conduct.
[Schedule 1, item 1, subsection 58AG(3)]

1.65 Where the attempt to engage an SPF consumer involves ongoing engagement with that consumer, the regulated entity may be required to take several and ongoing steps to, for example, detect and disrupt the scam activity to satisfy its obligations under the SPF principles (see Division 2). For example, if a scam involves a series of phone calls or text messages between the scammer and the SPF consumer over a protracted period of time, the obligation to take reasonable steps to disrupt a scam is intended to apply to the series of conduct, rather than an individual phone call or text message.

1.66 'SPF personal information' means personal information as defined in the Privacy Act and information relating to a person that may be used to access a

service or an account, or funds, credit or other financial benefits. This definition therefore includes one-time passwords and verification codes that may be used to access a bank account or social media account.
[Schedule 1, item 5, subsection 4(1)]

1.67 The concept of 'benefit' is broad and includes non-monetary benefits and assets, such as cryptocurrency or loyalty and rewards points.
[Schedule 1, item 1, subparagraph 58AG(1)(b)]

1.68 An 'associate' of an SPF consumer is an associate (within the meaning of section 318 of the ITAA 1936) of the SPF consumer who is a natural person who is in Australia or is ordinarily resident in Australia. This generally includes the entity's relative, spouse, child, a partner of a partnership or a trustee of a trust.
[Schedule 1, item 5, subsection 4(1)]

1.69 The conduct covered within the meaning of scam may interact with other regulatory frameworks, such as the ePayments Code. This is to ensure that key scam typologies including remote access scams and phishing scams are covered by the SPF. The intention is that where there are interactions with other regulatory frameworks, a regulated entity should not be required to compensate for the same loss or damage twice, under two different regimes.

1.70 An attempt will involve deception if the attempt:

- deceptively represents something to be, or to be related to, the regulated service;
- impersonates a regulated entity in connection with the regulated service;
- is an attempt to deceive the SPF consumer into either performing an action using the regulated service or facilitating another person to perform such an action; or
- is an attempt to deceive the SPF consumer that is made using the regulated service.

[Schedule 1, item 1, subsection 58AG(2)]

1.71 In practice, these types of conduct may not be mutually exclusive, and often end-to-end scam activity involves a number of these types of conduct. If the attempt in question is consistent with one or more of the four types of conduct, and would, if successful, cause loss or harm to an SPF consumer or their associates, the conduct is a scam. Each of these types of conduct is explained in further detail in the following sections.

Deceptively representing something to be, or to be related to, a regulated service

1.72 The reference to deceptively representing something to be, or to be related to, the regulated service, refers to conduct where a scammer deceives (or attempts

to deceive) an SPF consumer by making a representation in relation to a regulated service.

1.73 For example, where the banking sector is a regulated sector, this may include an imposter bond scam, where a scammer impersonates a financial advisor and makes a false representation in relation to an investment product or bond offered by a banking entity that does not exist to obtain a benefit from the consumer. The scammer may demonstrate specialised financial knowledge and provide convincing documents, fake websites and fake information. This type of scam involves deceptively representing something to be related to a regulated service (banking services) by making false representations about the product offered. This is distinct from poor financial advice (which is not considered to be a scam), as in this case the scammer is making false representations about a product offered by a regulated service that does not exist. Conversely, poor financial advice may be where a financial advisor recommends a risky or inappropriate strategy by failing to appropriately assess a consumer's circumstances.
[Schedule 1, item 1, paragraph 58AG(2)(a)]

Impersonating a regulated entity in connection with its regulated service

1.74 The reference to impersonating a regulated entity in connection with its regulated service refers to, for example, impersonation scams where a scammer mirrors the brand of the regulated entity to mislead an SPF consumer into providing personal information, transferring money or otherwise providing a benefit to the scammer.

1.75 For example, where the banking sector is a regulated sector, this may include an impersonation scam where a consumer receives a text message that uses the alphanumeric tag from a well-known banking entity. The text message appears in the existing chain of text messages from that entity and notifies the consumer that an irregular payment had been detected. It also provides a phone number to contact. The consumer was told their account had been compromised and their funds needed to be transferred to a specific new safe account that had been opened. The consumer then transfers their funds to the scammer. This type of scam involves deceiving a consumer by impersonating a brand of a banking entity related to its regulated service (a banking service).
[Schedule 1, item 1, paragraph 58AG(2)(b)]

Deceiving an SPF consumer into performing an action using a regulated service, or facilitating another person to perform such an action

1.76 The reference to deceiving an SPF consumer into performing an action using a regulated service, or facilitating another person to perform such an action includes circumstances where the SPF consumer is deceived into undertaking an action using the regulated service under false pretences.

1.77 This limb includes circumstances where, if the banking sector is a regulated sector, an SPF consumer is deceived into performing an action themselves, for

example where an SPF consumer sends money from their bank account to the scammer. It also includes circumstances where an SPF consumer facilitates an action performed by the scammer, for example where an SPF consumer provides a scammer with access to their personal device, or provides personal information or a one-time passcode over the phone that is then used by the scammer to make a transfer of money. As the SPF consumer has facilitated the action performed by the scammer, this comes within the meaning of involving deception and is therefore a scam.
[Schedule 1, item 1, paragraph 58AG(2)(c)]

Deceiving an SPF consumer using a regulated service

1.78 An attempt will involve deception where a scammer uses a regulated service to make a false representation or to otherwise deceive an SPF consumer.

1.79 For example, where paid search advertising services are a regulated sector, this would include false advertisements that trick consumers into providing their personal information or transferring money. Where telecommunications services are a regulated service, this would include circumstances where text messages or phone calls are used to initiate contact between a scammer and an SPF consumer to deceive the consumer.
[Schedule 1, item 1, paragraph 58AG(2)(d)]

SPF rules may prescribe attempts that are not scams

1.80 The SPF rules may prescribe specific kinds of attempts to engage an SPF consumer of a regulated sector that are not scams for the purposes of the SPF. This empowers a Treasury Minister, by legislative instrument, to exclude specific activities or conduct that are not intended to fall within the broad scope of the definition of a 'scam'. This power is not able to expand on what a scam is for the purpose of the SPF – it may only limit the definition.
[Schedule 1, item 1, subsections 58AG(4) and 58GE(1)]

1.81 Examples of exclusions from the meaning of scam may include:

- certain subsets of fraud that involve dishonestly obtaining a benefit without any action from the consumer (such as credit card fraud);
- cybercrime (including information obtained as part of a data breach or hack);
- certain conduct regulated under anti-money laundering and counter-terrorism financing legislation;
- misleading and deceptive conduct in trade or commerce, as defined in Schedule 2 to the CCA; or
- performing a transaction under the threat of imminent violence (such as burglary or mugging).

Examples of attempts that may be considered a scam

1.82 Without limiting what may be considered a scam for the purposes of the SPF, some examples of attempts that may be considered a scam and an example that may not be considered a scam for the purposes of the SPF are outlined below. It is assumed that the businesses and services being described in the examples are regulated by the SPF.

Example 1.1 Scam attempt that is not successful

An SPF consumer is exposed to an online advertisement prompting them to invest in financial products, with the promise of high returns. The advertised product does not exist and is an attempt to deceive potential consumers into transferring funds to the advertiser's account. The SPF consumer considers this to be 'too good to be true' so they do not transfer money from their bank account for the product.

- *Scam:* This is a scam because it is an attempt to deceive the SPF consumer using a regulated service (display advertising). This is because a scammer uses a fake advertisement to attempt to engage an SPF consumer into believing that they are obtaining investment products that do not exist. This is also an attempt to deceive the SPF consumer into performing an action using a regulated service (by transferring money from their bank account to the scammer). While the attempt in the example was not successful, it still meets the definition of a scam because it would cause loss or harm if successful, in the form of financial loss in seeking to obtain non-existent investment products.
- In this example, SPF obligations are triggered in relation to the display advertising service used to attempt to deceive the consumer. SPF obligations may also be triggered in relation to the banking entity to take preventative steps, if it is reasonable to do so in the circumstances.

Example 1.2 Successful scam that involves ongoing conduct across multiple sectors

An SPF consumer gets contacted on a social media platform seeking a relationship. The profile, operated by a scammer, fosters a fake relationship with the consumer and takes the communication 'offline' to SMS.

Over weeks or months, the SPF consumer is deceived into believing they have built a relationship and trust with the scammer. The scammer then discloses that they have been in an accident and urgently need money, which is paid by the SPF consumer to the

scammer via bank transfer. The SPF consumer begins expressing suspicion about the money, after which they never hear from the scammer again.

- *Scam:* This is a scam because it is an attempt to deceive the SPF consumer using a regulated service, including both the social media service as the original communication channel and subsequently via SMS. The scammer creates a fake profile posing as a fictitious person to convince a consumer to send money through a financial transaction. This creates several touchpoints to regulated entities across the life of the scam. These are attempts to deceive the SPF consumer using a regulated service (initially social media messaging and then shifting to a telecommunications service), with the consumer also deceived into performing an action using a regulated service by transferring money via their bank account to the scammer.
- This ongoing engagement in its entirety is a scam, which triggers the relevant obligations under the SPF for each regulated entity involved (social media messaging, telecommunications, and banking).

Example 1.3 Conduct that involves consumer-facilitated action

An SPF consumer is contacted by a third party using a telecommunications service offering to check their broadband. The consumer downloads a remote access tool and then makes a small payment from their banking app on the same device to pay for the 'service'. The scammer then uses the remote access tool to make further large transactions using the banking service through the consumer's device.

- *Scam:* This course of conduct is a scam because an SPF consumer has been deceived into facilitating an action performed by the scammer, by downloading a remote access tool which is then used by the scammer to make transactions through the consumer's device. There is also an attempt to deceive the SPF consumer using the regulated service (telecommunications) and an attempt to deceive the SPF consumer into facilitating an action performed by the scammer using a regulated service (banking service).
- In this example, SPF obligations are triggered in relation to the telecommunications service provider because the telecommunications service was used to deceive the consumer into facilitating an action (downloading the remote access tool). SPF obligations are also triggered in relation to the banking entity as its banking service was used by the scammer to perform the action of making large

transactions out of the SPF consumer's account. Although the consumer's action of downloading the remote access tool was not made using a regulated service, the action subsequently performed by the scammer is using a regulated service (banking) and therefore the SPF obligations apply in relation to that activity.

Example 1.4 Conduct that involves consumer-facilitated action

An SPF consumer receives a text message using a telecommunications service purporting to be from a trusted postal service, asking them to confirm their credit card details. The consumer clicks a link and provides their credit card details. The scammer then uses the credit card details to make online purchases.

- *Scam:* This course of conduct is a scam because there is an attempt to deceive the consumer that is made using a regulated service (telecommunications service) and an attempt to deceive the consumer into facilitating an action performed by the scammer using a regulated service (banking service). The SPF consumer has facilitated online purchases made by the scammer using a banking service, by providing their credit card credentials.
- In this example, SPF obligations are triggered in relation to the activity on the telecommunications service used to deceive the consumer. SPF obligations are also triggered in relation to the banking service as this was the service used by the scammer, as facilitated by the consumer, to perform the action of making online purchases.

Example 1.5 Not a scam for the purposes of the SPF – Conduct already regulated by consumer law

An SPF consumer is looking to buy a trailer and comes across an advertisement on the internet for a trailer. The advertisement is from a legitimate business. The SPF consumer visits the legitimate business website and calls the dealer to place a deposit and settle the details of the payment. They agree that the SPF consumer will pay using a direct transfer. The SPF consumer makes the payment but does not receive the trailer within the agreed time.

- *Scam:* This does not fall within the definition of a scam as there was no deceptive impersonation of a regulated entity or attempt to deceive the consumer into facilitating an action using the regulated service. The consumer made a payment via bank transfer for the intended purpose and did not engage in the payment on false pretences. The issues in relation to the delay in receiving the trailer may be dealt with in other consumer law provisions.

Meaning of SPF consumer

1.83 The amendments introduce the concept of an 'SPF consumer'. The obligations imposed on regulated entities are often in relation to an SPF consumer. This is intended to clearly set out the scope of obligations under the SPF and who they are designed to protect.

1.84 An SPF consumer of a regulated service is:

- a natural person, or a small business operator, who is or may be provided or purportedly provided the service in Australia; or
- a natural person who is ordinarily resident in Australia and is or may be provided or purportedly provided the service outside of Australia by a regulated entity that is either an Australian resident or is providing or purportedly providing the service through a permanent establishment in Australia.

[Schedule 1, item 1, subsections 58AH(1) and (2)]

1.85 The meaning of 'Australian resident' and 'permanent establishment' with respect to the regulated entity in this context leverages the existing established definitions in the ITAA 1997.

1.86 An SPF consumer is intended to cover any natural person or small business operator who is in Australia when they are provided the regulated service, regardless of where that service is based (for example, the regulated service may be based overseas). This includes natural persons who are only temporarily in Australia. The definition also intends to cover any natural person who is ordinarily resident in Australia but is overseas when they are provided a regulated service that is based in Australia.

1.87 For example, an SPF consumer could be (assuming the following services are regulated services):

- an Australian resident in Australia using either an Australian-based or overseas-based messaging service that is offered in Australia;
- a person ordinarily resident in Australia who is overseas but using an Australian-based banking service; or
- a tourist visiting Australia using an Australian-based or overseas-based telecommunication service that is offered in Australia.

1.88 It is not intended that a foreign entity will be regulated with respect to consumers in foreign markets. For example, where an Australian consumer is overseas and is impacted by a scam on a social media service offered by an entity based overseas, this is not intended to be within the scope of the SPF.

1.89 Small businesses are not excluded from being SPF consumers based on their corporate structure. The small business may be in the form of a sole trader,

company, unincorporated association, partnership or trust.
[Schedule 1, item 1, note 2 to subsection 58AH(2)]

1.90 However, whether a small business is a small business operator for the purposes of the SPF will differ slightly depending on whether the small business is a body corporate or not.

1.91 If a small business is a body corporate, it is a small business operator if it meets all of the following conditions:

- the sum of the business' employees and the employees of any body corporate related to the business, is less than 100 employees;
- the annual turnover of the business during the last financial year is less than $10 million; and
- the business has a principal place of business in Australia.

[Schedule 1, item 1, subsection 58AH(5)]

1.92 If a small business is not a body corporate, it is a small business operator if it meets all of the following conditions:

- the business has less than 100 employees;
- the annual turnover of the business, worked out as if the person were a body corporate, during the last financial year is less than $10 million; and
- the business has a principal place of business in Australia.

[Schedule 1, item 1, subsection 58AH(5)]

1.93 The meaning of annual turnover and related body corporate in this context leverages the existing and established definitions in the Corporations Act.
[Schedule 1, item 1, subsection 58AH(5)]

1.94 A small business operator that is an SPF consumer at the time it is impacted by a scam continues to be an SPF consumer for that time, even if, for example, that business later has 100 or more employees.
[Schedule 1, item 1, note 1 to subsection 58AH(2)]

1.95 As stated above, an SPF consumer of a regulated service is a particular kind of person to whom the regulated service is or may be provided or purportedly provided. This includes, but is not limited to, the provision or purported provision of a regulated service:

- directly or indirectly to the SPF consumer;
- whether or not under a contract, arrangement or understanding with the SPF consumer;
- whether or not the provider of the service knows that the person is an SPF consumer; or

- that involves the supply of goods.

[Schedule 1, item 1, subsection 58AH(3)]

1.96 A person can be an SPF consumer of a regulated service even if they do not have a direct customer relationship with the regulated entity providing or carrying on that regulated service for the regulated sector. This reflects that an individual's experience with a scam is often not limited to entities the individual has a direct customer relationship with. For example:

- where an individual makes a payment to the scammer which is received by a banking service that the individual does not have a direct customer relationship with; or
- where an individual is deceived through an impersonation scam involving an entity that the individual does not have a direct customer relationship with; or
- where an individual receives a phone call or text message from a scammer, from a carriage service provider or intermediary that the individual does not have a direct customer relationship with.

1.97 SPF codes may set out more specific obligations on regulated entities, which could include obligations that relate to certain classes of SPF consumers. An example of such a class is SPF consumers that have a direct customer relationship with the regulated entity. This reflects that it may not be appropriate or practical to extend certain obligations beyond SPF consumers with a direct customer relationship with the regulated entity.

1.98 Without limiting who may be considered an SPF consumer of a regulated service, some examples are outlined below. It is assumed that the businesses and services being described in the examples are regulated under the SPF.

Example 1.6 SPF consumer – No direct relationship or contract

An individual observes a fraudulent advertisement impersonating a known banking entity selling a banking service on a social media service. The individual is not a direct customer of the banking entity and does not hold an account to use the banking service. The individual holds an account with the social media service provider.

- *SPF consumer*: The individual is an SPF consumer of the banking service being impersonated by the fraudulent advertisement, and the social media service. This is because while the individual does not have a direct contract with the banking service, its banking service may be provided to the individual. The individual is also an SPF consumer of the social media service, as they directly hold an account and receive the service from the provider.

- In this example, SPF obligations are triggered in relation to the banking entity and the social media service provider. However, as the banking entity does not have a direct relationship with the SPF consumer, it is likely that the reasonable steps it may take in relation to preventing, detecting, disrupting and responding to the scam may be more limited than the social media service provider who has a direct relationship with the SPF consumer. For example, if the banking entity has actionable scam intelligence regarding the impersonation scam, it may be expected to engage with the social media service provider to request the content be removed, and issue public warnings to notify the community that there is a scam advertisement impersonating its brand. In contrast, the social media service provider may be expected to take more direct steps to identify impacted SPF consumers and remove the advertisement.

Example 1.7 Indirect relationship involving the supply of goods and services

An individual receives a scam text message impersonating the Australian Taxation Office in relation to outstanding taxes.

- *SPF consumer:* A text message from a scammer to an individual involves one or more carriage services, as it may need to be carried by one or more transit (or intermediary) carriage services. A transit carrier or carriage service providers may or may not know whether the services it provides are to an SPF consumer through another entity. However, it is assumed that the transit carrier service is being provided indirectly to an SPF consumer (unless otherwise known) and therefore the individual is an SPF consumer of the sending carriage service provider (used by the scammer to send the text message), the receiving carriage service provider (the SPF consumer's telecommunications service provider) and any intermediaries (used to facilitate the message being received by the SPF consumer).
- As a result, transit carriers or carriage service providers that connect other transit carriers or carriage service providers and International Operators to pass call traffic or SMS traffic between them will need to treat the service they are providing as having one or more SPF consumers. This is unless the transit carrier or carriage service provider knows the transited call or SMS is not being directly provided to or for an SPF consumer.
- In this example, SPF obligations are triggered in relation to the transit carrier and carriage service provider. However, as

the transit carrier does not have any direct engagement with the SPF consumer, it may have more limited means to detect or validate the legitimacy of the traffic, meanwhile it may be more equipped to take preventative action. This will be a relevant consideration in determining reasonable steps in the context of satisfying the SPF principles.

Example 1.8 Australian resident accessing a service overseas

A person ordinarily resident in Australian who is overseas is using a social media service to check for updates. The individual comes across a scam advertisement impersonating a well-known figure, clicks on the link and makes a payment through their Australian banking service.

- *SPF consumer:* The individual is an SPF consumer for the purposes of the banking service. This is because although they are accessing the service overseas, the banking entity is an Australian resident and providing the service through a permanent establishment in Australia. The individual is not an SPF consumer for the purposes of the social media service, as the social media service provider does not meet Australian residency requirements and the content is being accessed overseas.
- In this example, SPF obligations are triggered in relation to the banking service only, and protection to the SPF consumer under the SPF will only apply in relation to the course of conduct involving the Australian banking service.

1.99 A person is a not an SPF consumer of the regulated service if a condition prescribed by the SPF rules applies to the person in relation to regulated services of that kind.
[Schedule 1, item 1, subsection 58AH(4)]

1.100 To avoid doubt, an 'SPF consumer' under the SPF is distinct from a 'consumer' as defined in section 4B of the CCA.
[Schedule 1, item 1, subsection 58AH(6)]

Meaning of actionable scam intelligence

1.101 Several obligations in the SPF relate to a regulated entity having actionable scam intelligence.

1.102 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 relating to, connected with, or using a regulated service of the entity is a scam.
[Schedule 1, item 1, section 58AI]

1.103 As this definition relies on the meaning of scam, it is inherently tied to information about an SPF consumer.

1.104 A regulated entity may receive or identify actionable scam intelligence from a range of sources, including (but not limited to):

- a report about a scam made to a regulated entity;
- information provided by SPF regulators; or
- a regulated entity's own investigation into suspected scam activity.

1.105 Whether there are reasonable grounds for an entity to suspect that an activity is a scam is an objective test. Rather than a requirement to have formed a suspicion, the test is whether it is reasonable in the circumstances for the regulated entity to form a suspicion.
[Schedule 1, item 1, note 1 to section 58AI]

1.106 Relevant information that may lead a regulated entity to have reasonable grounds to suspect that an activity is a scam includes:

- information about the mechanism or identifier being used to scam SPF consumers, such as URLs, email addresses, phone numbers, social media profiles, digital wallets and bank account information of the scam promotors;
- information about the suspected scammer; and
- information (including complaints) provided by SPF consumers.

[Schedule 1, item 1, note 1 to section 58AI]

1.107 For example, a regulated entity (such as a banking entity offering a banking service) receives several consumer reports about a phishing scam tricking consumers into making a payment that is not owed. The consumer reports indicate that the phishing scam originates via text message, with a link that sends consumers to a fraudulent website impersonating the brand of the regulated entity. The regulated entity does not communicate with consumers via text message and observes that the website link is fraudulent. In this case, the regulated entity has actionable scam intelligence because there are reasonable grounds to suspect that an activity related to its regulated service is a scam. The actionable scam intelligence may include the phone numbers used to send messages to the SPF consumers, the website where payments were facilitated and the bank account the SPF consumers were asked to make payments to.

1.108 Actionable scam intelligence may include information about how other entities and services are being used to facilitate scam activity, as long as there is a connection between the scam and the regulated service of the regulated entity holding the information. This includes information about sectors that are not regulated under the SPF. In the example above, the regulated entity holds information about the digital platform hosting the website, telecommunications

providers and other banking services. This information all forms part of the actionable scam intelligence that the regulated entity has, because the information relates to a scam that uses a regulated service of the regulated entity.

1.109 A regulated entity has several obligations under the SPF in relation to actionable scam intelligence. For example, SPF Principle 4: Report includes requirements for regulated entities to provide the SPF general regulator with reports of and about actionable scam intelligence if required by the SPF rules. SPF Principle 5: Disrupt includes requirements for regulated entities to take reasonable steps to disrupt scams on receipt of actionable scam intelligence. Gathering and reporting this information is intended to minimise the harm to SPF consumers from scams.
[Schedule 1, item 1, note 2 to section 58AI]

Extension to external territories

1.110 Each SPF provision extends to every external Territory. SPF provisions are:

- provisions of Part IVF (about the SPF);
- provisions of legislative instruments made under Part IVF (including the SPF rules and SPF codes);
- provisions of the CCA to the extent that they relate to a provision of Part IVF or a provision of a legislative instrument made under Part IVF; and
- provisions of the Regulatory Powers Act to the extent they apply in relation to a provision of Part IVF or a provision of legislative instrument made under Part IVF.

[Schedule 1, item 1, subsection 58AJ(1)]

1.111 The SPF provisions also extend to acts, omissions, matters and things outside of Australia.
[Schedule 1, item 1, subsection 58AJ(2)]

Application to acts done by agents of regulated entities

1.112 If an element of the SPF provisions is done by or in relation to agents of regulated entities and section 97 of the Regulatory Powers Act is applicable, the conduct is also attributed to the regulated entities.
[Schedule 1, item 1, subsection 58AK(1)]

1.113 If an element of the SPF provisions is done by a person in relation to an agent who is acting on behalf of a regulated entity, and the agent is acting within the scope of their actual or apparent authority, the conduct is also taken as having

been done in relation to the regulated entity.
[Schedule 1, item 1, subsection 58AK(2)]

Division 2 – Overarching principles of the SPF

1.114 The simplified outline in Division 2 provides that:

- All regulated entities must comply with the overarching principles of the SPF.
- These principles require each regulated entity to document and implement governance arrangements to combat scams and take reasonable steps to prevent, detect, report, disrupt and respond to scams relating to, connected with, or using the entity's regulated service.
- Obligations contained in the SPF principles are civil penalty provisions. Compliance with the SPF principles will be monitored, investigated and enforced by the ACCC as the SPF general regulator. Division 6 of the SPF sets out further remedies for non-compliance with these provisions.

[Schedule 1, item 1, section 58BA]

1.115 The SPF principles will generally be supported by an SPF code for each regulated sector. An SPF code is a legislative instrument which will set out detailed and sector-specific obligations relating to the SPF principles (excluding SPF Principle 4: Report).

1.116 SPF codes are intended to ensure that there are robust and targeted obligations for each regulated sector, recognising their different roles in the scams ecosystem and the differing action that is needed by each sector to combat scams. The SPF codes are expected to include more tailored obligations that a regulated entity must comply with to support their compliance with the SPF principles.

Meaning of reasonable steps

1.117 The SPF principles are principle-based obligations that require a regulated entity to take a comprehensive approach to compliance. Accordingly, a number of the provisions in the SPF principles require a regulated entity to take 'reasonable steps'. This includes the requirement to take reasonable steps to prevent scams from being committed in section 58BJ and the requirement to take reasonable steps to detect a scam relating to, connected with, or using a regulated service of the entity in section 58BM.

1.118 Whether a regulated entity has taken reasonable steps is an objective assessment that depends on the particular facts and circumstances. Relevant

matters to be considered in determining whether a regulated entity has taken reasonable steps include:

- the size of the entity;
- the regulated services of the entity;
- the consumer base of those services;
- the kinds of scam risks those services face; and
- whether the entity has complied with any relevant SPF code obligations relating to the provision concerned.

[Schedule 1, item 1, section 58BB]

1.119 The factors in determining reasonable steps are to be considered collectively, rather than in isolation.

1.120 All regulated entities must comply with the 'reasonable steps' obligations under the SPF, subject to any applicable exceptions or carve outs in the SPF rules or designation instrument. However, how they give effect to the obligations may differ depending on the matters set out above.

1.121 For example, the size of the entity may reflect its capability to implement measures to address scams. While some larger entities may be able to make direct changes to systems and processes to fulfill their obligations under the SPF, other entities may have to manage arrangements with third party service providers that manage processes and systems. The reasonable steps test recognises that different sized entities may appropriately meet their obligations in different ways.

1.122 An assessment of reasonable steps also involves consideration of what is practical in the circumstances based on, for example, the regulated service provided by the entity. For example, if a transit carrier or a regulated entity without any direct engagement with an SPF consumer has limited or no means to detect or validate the legitimacy of an interaction, and could not take steps to do so, this would be a relevant factor in determining what the reasonable steps are in the circumstances, for the purposes of relevant SPF principles.

1.123 The principles-based nature of these obligations goes beyond requiring only strict administrative steps, which may not otherwise be effective to prevent and respond to scams impacting SPF consumers. By requiring a regulated entity to take reasonable steps (which depend on the particular facts and circumstances), the SPF principles ensure the integrity of a regulated entity's response to scams, regardless of the kind of entity it is or the nature of the scams impacting that entity. This also reflects that the SPF is designed to be an economy-wide framework that is flexible enough to apply across entities in differing sectors that face unique scams-related challenges.

1.124 The meaning of reasonable steps makes clear that compliance with any relevant SPF code obligations is a relevant factor in determining whether a

regulated entity has taken reasonable steps for the purposes of meeting a relevant SPF principle. This reflects that a regulated entity is required to comply with the SPF code for its sector and the matters that an SPF code can deal with must be consistent with the SPF principles.

1.125 However, given the SPF will apply to a diverse range of entities, both across and within regulated sectors, it is not intended that the SPF codes will set out an exhaustive list of requirements that would be reasonable for every entity in every set of circumstances. Consequently, compliance with SPF code obligations will not automatically equate to compliance with the corresponding SPF principles.

1.126 While compliance with the SPF code provisions may be sufficient to satisfy compliance with the SPF principles in certain circumstances, there may cases where it is reasonable for a regulated entity to take additional steps beyond SPF code obligations. This may occur, for example, where an entity is facing a specific, targeted and heightened risk that requires action above and beyond the sector-wide measures set out in the SPF code.

SPF Principle 1: Governance

1.127 The simplified outline in Subdivision B of Division 2 provides that:

- Regulated entities must document and implement governance policies, procedures, metrics and targets for combatting scams relating to, connected with, or using a regulated service of the entity.
- These policies, procedures, metrics and targets must be certified annually by a senior officer of the entity.
- The regulated entities must keep records in relation to its SPF governance policies and procedures and share these with the SPF general regulator or applicable SPF sector regulator upon request.
- An SPF code for a regulated sector may include sector-specific obligations for this SPF principle, which a regulated entity in that sector must also comply with.

[Schedule 1, item 1, section 58BC]

Developing and implementing policies, procedures, metrics and targets

1.128 A regulated entity must:

- document and implement governance policies and procedures that set out the entity's approach to scam prevention, detection, disruption, response and reporting, in relation to scams relating to, connected with, or using the entity's regulated services for the sector; and

- develop and implement performance metrics and targets to measure the effectiveness of its governance policies and procedures, and comply with any requirements prescribed by the SPF rules.

[Schedule 1, item 1, subsection 58BD(1)]

1.129 Policies and procedures may include the steps an entity is taking to:

- comply with SPF provisions;
- identify actionable scam intelligence;
- assess and address the risk of scams relating to, connected with, or using the entity's regulated services for the sector; and
- meet performance metrics and targets developed for those policies and procedures.

1.130 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BD(2)]

Annual certification requirements

1.131 A regulated entity's SPF governance policies, procedures, metrics and targets must be approved by a senior officer of the entity in writing on an annual basis. This approval must state whether those governance policies, procedures, metrics and targets comply with this SPF principle for the regulated sector.
[Schedule 1, item 1, subsection 58BE(1)]

1.132 This requirement ensures that regulated entities consider and approve their governance arrangements at least on a yearly basis, so they remain fit for purpose over time.

1.133 The approval by the senior officer must occur within 12 months of the day the entity becomes a regulated entity for the sector and within seven days after each 12-month anniversary of that day.
[Schedule 1, item 1, paragraphs 58BE(1)(a) and (b)]

1.134 As the SPF could apply to a range of businesses with varying structures, 'senior officer' is intended to apply broadly and is defined as an 'officer' or 'senior manager' within the meaning of the Corporations Act. For example, this includes a director or secretary of a company, a partner in a partnership or an office holder of an unincorporated association.
[Schedule 1, item 5, subsection 4(1)]

1.135 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BE(2)]

Record-keeping requirements

1.136 A regulated entity must keep records of information of a material nature relating to activities taken to comply with certain obligations under the SPF for at least six years. These records include information on:

- the initial documenting, and each revision of the documenting, of the entity's SPF governance policies, procedures, metrics and targets;
- the initial implementation, and each reimplementation, of those SPF governance policies, procedures, metrics and targets by the entity;
- each consideration (including certification) by the entity's senior officer of those SPF governance policies, procedures, metrics and targets, including in relation to their documenting, implementation and review; and
- any other activities that are prescribed by the SPF rules.

[Schedule 1, item 1, subsection 58BF(1)]

1.137 The requirement to keep records of information of a 'material nature' ensures entities are not required to keep records of documents that are inconsequential to these activities. For example, an entity may not be required to retain every meeting invitation, email, or text message relating to the above matters. Rather, it is intended to ensure that only relevant and meaningful information about those matters is kept.

1.138 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BF(2)]

Providing information about governance arrangements to an SPF regulator

1.139 Copies of a regulated entity's SPF governance policies, procedures, metrics and targets, and any other records the entity is required to keep under this SPF principle, must be given to the SPF general regulator and the relevant SPF sector regulator upon written request. The regulated entity must comply with the request within 10 business days after receiving the request, or a longer period as allowed by the SPF regulator.
[Schedule 1, item 1, subsection 58BG(1)]

1.140 This requirement allows for effective regulation and enforcement of this SPF principle and any SPF code relating to this principle for the regulated sector.

1.141 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BG(2)]

Sector-specific obligations relating to SPF Principle 1: Governance

1.142 An SPF code may be made for a regulated sector setting out detailed, sector-specific obligations consistent with this SPF principle.
[Schedule 1, item 1, section 58BH]

1.143 An SPF code may include, for example, sector-specific provisions about governance arrangements, including:

- the policies and procedures to be documented;
- the implementation of policies and procedures;
- the development of performance metrics and targets;
- the certification of these policies, procedures, metrics and targets;
- the publication of information about these policies, procedures, metrics and targets;
- record keeping of compliance with the SPF provisions; and
- reporting about compliance with this SPF principle.

SPF Principle 2: Prevent

1.144 The simplified outline in Subdivision C of Division 2 provides that:

- Regulated entities must take reasonable steps to prevent scams relating to, connected with, or using a regulated service of the entity.
- An SPF code for the sector may include sector-specific provisions in relation to this SPF principle.

[Schedule 1, item 1, section 58BI]

1.145 This SPF principle is aimed at stopping scams from reaching or impacting SPF consumers, rather than stopping or identifying scams that are already underway (covered in SPF Principle 3: Detect and SPF Principle 5: Disrupt).

1.146 This means that the reasonable steps a regulated entity may take to meet its obligations under this SPF principle may include steps to educate its consumers, educate its staff, and implement robust measures or processes to prevent scammers from accessing or using its regulated service in any way to perpetuate scams.

Overarching obligation to take reasonable steps to prevent scams

1.147 Under this SPF principle, a regulated entity must take reasonable steps to prevent another person from committing a scam relating to, connected with, or using a regulated service of the entity.
[Schedule 1, item 1, subsection 58BJ(1)]

1.148 The provisions in Division 7 of the amendments extend the meaning of 'person' for partnerships, unincorporated associations and trusts.
[Schedule 1, item 1, note to subsection 58BJ(1)]

1.149 A contravention of this obligation does not occur merely because an individual scam has not been prevented. Whether a regulated entity meets the obligation in taking reasonable steps to prevent scams is an objective test which will depend on the circumstances, including the relevant matters set out in section 58BB (about the meaning of reasonable steps). The SPF code for a regulated sector may also include sector-specific provisions describing what are reasonable steps for the purposes of this obligation.

1.150 In addition to those matters, taking reasonable steps in this context requires more than merely acting on actionable scam intelligence that is provided to the regulated entity. This makes clear that in complying with this obligation, a regulated entity must be proactive and take a comprehensive approach to prevent scams as they relate to, connect with, or use the entity's regulated service or services.
[Schedule 1, item 1, subsection 58BK(1)]

1.151 Reasonable steps in this context may include (but are not limited to):

- introducing additional identity verification requirements for new accounts to use the regulated service;
- providing warnings to SPF consumers about scams related to, connected with or using the regulated service and steps that SPF consumers can take to minimise the risk of harm;
- proactively seeking out information and data from other sources on emerging scams, to understand scam trends and identify whether there are any particular vulnerabilities associated with the regulated service; and
- training staff on emerging scams to assist them in identifying and responding to scams.

1.152 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BJ(2)]

Sector-specific obligations relating to SPF Principle 2: Prevent

1.153 An SPF code may be made for a regulated sector setting out detailed, sector-specific obligations consistent with this SPF principle.
[Schedule 1, item 1, section 58BK(2)]

1.154 An SPF code may, for example, include sector-specific provisions:

- describing what reasonable steps are to prevent scams;

- requiring each regulated entity for that sector to identify its SPF consumers that are at risk, or who have a higher risk, of being targeted by a scam; or
- requiring each regulated entity for the sector to provide information about such scams to an SPF consumer at risk, or who have a higher risk, of being targeted.

[Schedule 1, item 1, subsection 58BK(2)]

1.155 An SPF code may therefore require an entity to identify classes of its SPF consumers that are at a heightened risk of scams, so that additional preventative steps can be taken with respect to these consumers where appropriate. This may include consideration of how an SPF consumer is using the regulated service or specific vulnerabilities the consumer may have that could be targeted by a scammer.

1.156 The obligations included in any SPF code made for a regulated sector are not intended to be exhaustive in relation to the reasonable steps the regulated entity for the sector must take. A regulated entity may still be in breach of their obligations under the SPF principles even if they comply with the obligations in an SPF code, although compliance with the SPF code obligations is a relevant factor in considering whether a regulated entity has taken reasonable steps.

SPF Principle 3: Detect

1.157 The simplified outline in Subdivision C of Division 2 provides that:

- Regulated entities must take reasonable steps to detect scams, which includes timely investigations of activities that are the subject of its actionable scam intelligence and identifying SPF consumers that are or may have been impacted by such activities in a timely way.
- An SPF code for the sector may include sector-specific obligations in relation to this SPF principle.

[Schedule 1, item 1, section 58BL]

1.158 A regulated entity's obligations under this SPF principle are linked to and flow through other obligations in the SPF principles. For example, identifying suspected scams through detection activities triggers the:

- obligation to report actionable scam intelligence to the SPF general regulator under SPF Principle 4: Report; and
- obligation to take reasonable steps to disrupt scam activity under SPF Principle 5: Disrupt.

Overarching obligation to take reasonable steps to detect scams

1.159 A regulated entity must take reasonable steps to detect a scam related to, connected with, or using an entity's regulated service. This includes (but is not limited to) taking reasonable steps to detect such scams as they are happening or after they have happened, regardless of whether an SPF consumer or their associate has already incurred a loss or before a loss has occurred. ***[Schedule 1, item 1, subsections 58BM(1) and (3)]***

1.160 The obligation to take reasonable steps to detect a scam as it is happening reflects that a scam may extend over a long period of time. For example, a scam advertisement may be available on a digital platform service for an extended period of time, so the obligation to take reasonable steps to detect scams as they are happening will apply in this context over the period of time that the advertisement is available.

1.161 The obligation to take reasonable steps to detect a scam after it has happened supports broader disruptive and preventative activity. For example, where an SPF consumer has made a payment to a scammer using a regulated service, it is important that the regulated entity takes reasonable steps to detect that activity to ensure that steps can be taken to protect that consumer from further harm, and to protect other consumers.

1.162 Some regulated entities may have more limited means to detect scams than others, particularly those without direct relationships with SPF consumers. For example, in the telecommunications sector where there are multiple parties involved in the delivery of a telecommunications call or SMS, typically, only the originating carriage service provider will have visibility over a customer's rights to use a number, and therefore will have the greatest ability to detect scams.

1.163 A contravention of this obligation does not occur merely because an entity fails to detect a single scam. Whether an entity has taken reasonable steps is an objective test that will depend on the particular circumstances, including the relevant matters in section 58BB (about the meaning of reasonable steps). The SPF code for a regulated sector may also include sector-specific provisions describing what are reasonable steps for the purposes of this obligation.

1.164 Depending on the circumstances, taking reasonable steps to detect scams may involve (but is not limited to) detecting scams using:

- information received in consumer reports;
- actionable scam intelligence received from the SPF general regulator;
- the entity's internal systems which flag higher risk transactions or suspicious activity.

1.165 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set

out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BM(2)]

Investigating actionable scam intelligence

1.166 Where a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using the entity's regulated service, the entity must take reasonable steps to investigate whether the activity is a scam within 28 days. This 28-day period starts on day the intelligence became actionable scam intelligence for the entity, which is the day the entity has reasonable grounds to suspect the activity to be a scam.
[Schedule 1, item 1, subsection 58BN(1)]

1.167 This 28-day period is consistent with the safe harbour in section 58BZA for actions taken to disrupt an activity while investigating whether the activity is a scam (see SPF Principle 5: Disrupt). This ensures that a regulated entity is required to take reasonable steps to investigate actionable scam intelligence during the same period in which the safe harbour protection applies.

1.168 This obligation is designed to ensure regulated entities act on actionable scam intelligence within a reasonable period.

1.169 A contravention of this obligation does not occur merely because the regulated entity fails to conclude whether or not the actionable scam intelligence is associated with scam activity in 28 days. Whether a regulated entity meets this obligation is an objective test that will depend on the circumstances, including consideration of the matters set out in section 58BB (about the meaning of reasonable steps). The SPF code for a regulated sector may also include sector-specific provisions describing what reasonable steps are for the purposes of this obligation.

1.170 If, after taking reasonable steps to investigate whether actionable scam intelligence about an activity is a scam, the regulated entity has not been able to come to a conclusion within 28 days, the safe harbour protection for disruptive action in 58BZA will no longer apply. However, the regulated entity will still be required to comply with the overarching obligation to take reasonable steps to detect scam activity and is therefore expected to continue to take steps to act on the actionable scam intelligence.

1.171 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BN(2)]

Identifying impacted SPF consumers

1.172 If a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity, the entity must take reasonable steps in a reasonable time to identify the persons who were

SPF consumers of that service at the time when the persons were or may have been impacted by the activity.
[Schedule 1, item 1, subsection 58BO(1)]

1.173 It will generally be reasonable for a regulated entity to identify SPF consumers with whom they have a direct customer relationship under this obligation. However, given the broad definition of SPF consumers and depending on the circumstances, it may not be reasonable for a regulated entity to identify every impacted SPF consumer, particularly those that do not have a direct customer relationship with the regulated entity.

1.174 A contravention of this obligation does not occur merely because the regulated entity has failed to identify each SPF consumer who was or may have been impacted. Whether a regulated entity meets this obligation is an objective test which will depend on the circumstances, including the relevant matters set out in section 58BB (about the meaning of reasonable steps). The SPF code for a regulated sector may also include sector-specific provisions describing what are reasonable steps and what is a reasonable time for the purposes of this obligation.

1.175 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BO(2)]

Sector-specific obligations relating to SPF Principle 3: Detect

1.176 An SPF code may be made for a regulated sector setting out detailed, sector-specific obligations consistent with this SPF principle. An SPF code may include, for example, sector-specific provisions describing:

- what reasonable steps are to detect scams, investigate actionable scam intelligence and identify impacted SPF consumers; or
- what a reasonable time is for the purpose of identifying impacted SPF consumers.

1.177 [Schedule 1, item 1, section 58BP]

1.178 An SPF code may also include obligations requiring regulated entities to identify the nature of the impact of that activity on SPF consumers. This may include both financial and non-financial harm, including the loss of any SPF personal information. This is important in informing the proportionate disruptive action that is then taken by the regulated entity.

SPF Principle 4: Report

1.179 The simplified outline in Subdivision E of Division 2 provides that:

- Regulated entities must give the SPF general regulator reports of any actionable scam intelligence the entity has about activities relating to, connected with, or using the entity's regulated services.
- Regulated entities must give an SPF regulator (either the SPF general regulator or relevant SPF sector regulator) a report about a scam on request.
- The SPF general regulator may disclose information about scams to specified entities.

[Schedule 1, item 1, section 58BQ]

1.180 Efficient and timely sharing of scam-related information by regulated entities and the SPF general regulator is critical to meet the object of the SPF, as it will ensure SPF regulators, law enforcement agencies and other regulated entities are equipped to take action to prevent and respond to scams that impact the Australian community.

1.181 The reporting obligations in the SPF, including in SPF Principle 5: Disrupt, are designed to operate alongside other Commonwealth frameworks. Accordingly, where a regulated entity provides information required under the SPF, this is not intended to result in a breach of any requirements under other Commonwealth legislation. This includes under the privacy law, relevant secrecy provisions, and the anti-money laundering and counter terrorism financing legislation.

Actionable scam intelligence reports

1.182 Where a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity, the entity must give the ACCC, as the SPF general regulator, a report about the actionable scam intelligence within the period prescribed by the SPF rules. The report must contain the kinds of information, and be in the manner and form, prescribed by the SPF rules. This requirement only applies to a regulated entity when the SPF rules prescribe these matters.
[Schedule 1, item 1, subsections 58BR(1) and (2)]

1.183 The SPF rules may, for example, prescribe that the report is to include the sources or evidence that the entity has for that intelligence, or provide that the report may be given via access to a specified data gateway, portal or website. Different matters may be prescribed for different kinds of regulated entities. Further information about how a report may be given via access to a specified data gateway, portal or website is set out under the heading 'Authorised third party schemes for giving reports'.
[Schedule 1, item 1, subsection 58BR(5)]

1.184 This approach to using the SPF rules is appropriate and necessary to ensure the reporting requirements can be quickly adapted as new scam trends emerge. It

will also provide flexibility to adjust reporting requirements as data sharing capabilities mature across different sectors.

1.185 The actionable scam intelligence that must be reported under the SPF rules is expected to be information that is necessary to disrupt scam activity. As a result, this will likely focus on information about the mechanism or identifier used to perpetuate the scam. This means the regulated entity may need to include SPF personal information in the report, such as:

- the bank account an SPF consumer has transferred a payment to (as instructed by the scammer);
- a phone number used by the scammer to contact SPF consumers, or a phone number advertised on a scam advertisement; or
- details in relation to a scam advertisement or social media account used to perpetuate a scam.

[Schedule 1, item 1, subsection 58BR(6)]

1.186 An entity is not required to report actionable scam intelligence in certain circumstances prescribed by the SPF rules. For example, the SPF rules may specify that entities are not required to report actionable scam intelligence it received from the SPF general regulator to avoid duplication. The SPF rules may also specify an entity is not required to share information where doing so would be inconsistent with an overseas privacy law that also applies to the actionable scam intelligence. The defendant bears an evidential burden in relation to establishing that the circumstance in the SPF rules applies to the entity (see section 96 of the Regulatory Powers Act) because this operates as an exception to a general obligation of the SPF.
[Schedule 1, item 1, subsection 58BR(4)]

1.187 This refers to the burden of adducing or pointing to evidence that suggests a reasonable possibility that the exception in the SPF rules apply. This is appropriate as the relevant matters are peculiarly within the knowledge of the regulated entity, and would avoid costly and difficult investigations by the regulator to enforce the reporting requirement.

1.188 Failure to comply with this reporting requirement may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BR(3)]

1.189 For the avoidance of doubt, regulated entities and other entities may voluntarily share actionable scam intelligence that is not required under the SPF rules with the SPF general regulator, provided they comply with any relevant laws (such as the privacy law and any applicable secrecy provisions).

Reporting scams to SPF regulators on request

1.190 A regulated entity must give an SPF regulator (whether the SPF general regulator or SPF sector regulator) a report about a scam relating to, connected with, or using the entity's regulated service on written request from that regulator, within the period set out in the request. The report must be in the manner and form, and contain the kinds of information, set out in the request.
[Schedule 1, item 1, subsections 58BS(1) and (2)]

1.191 Examples of the kinds of information the SPF regulator may request in the report relate to the:

- loss or harm that may have resulted from the scam;
- disruptive actions the entity has taken in relation to the scam and whether any of those actions have been reversed;
- steps the entity is taking to disrupt similar scams; and
- steps the entity is taking to prevent loss or harm resulting from similar scams.

[Schedule 1, item 1, paragraph 58BS(4)(b)]

1.192 For example, the ACCC, as the SPF general regulator, may request scam reports, to obtain qualitative information about a widespread scam that may not be available through the actionable scam intelligence routinely shared with the ACCC, or for individual instances where there are significant losses to better understand those circumstances. It is expected that the ACCC will provide more detailed guidance on reporting requirements for regulated entities once the legislation has passed and subordinate instruments are further developed.

1.193 The request may also ask for the report to include SPF personal information. Where this occurs, the request must require the entity to de-identify the information unless the SPF regulator reasonably believes that doing so would not achieve the object of the SPF. Information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.
[Schedule 1, items 1 and 5, subsections 4(1) and 58BS(5)]

1.194 The SPF regulator's request may also provide the report be given via access to a specified data gateway, portal or website. Further information about this process is set out in the next section.
[Schedule 1, item 1, paragraph 58BS(4)(a)]

1.195 If a regulated entity has already provided a scam report to an SPF regulator, and another SPF regulator later requests a scam report about the same matter, then the entity only needs to provide to the second SPF regulator a report setting out that an earlier scam report about these matters was given to the first SPF regulator on a specified date and time. This avoids duplication of

reporting requirements for regulated entities.
[Schedule 1, item 1, subsection 58BS(6)]

1.196 Failure to comply with this reporting requirement may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BS(3)]

1.197 If the SPF regulator makes a request to a regulated entity for specific information and the entity cannot reasonably locate that information (for example, because they do not have access to the information and cannot otherwise obtain the information), it is not intended that they would be in breach of this obligation.

1.198 SPF regulators may share scam reports with another SPF regulator upon request or on their own initiative under Subdivision C of Division 5. Further information about this is set out under the heading 'Division 5 – Regulating the SPF'.
[Schedule 1, item 1, note to subsection 58BS(6)]

Authorised third party schemes for giving reports

1.199 A regulated entity is required to give the following reports:

- reports of actionable scam intelligence to the SPF general regulator under SPF Principle 4: Report;
- reports about scams to an SPF regulator under SPF Principle 4: Report; and
- reports on the outcomes of investigations of activities relating to actionable scam intelligence to the SPF general regulator under SPF Principle 5: Disrupt.

1.200 These reports may be given via a data gateway, portal or website prescribed by the SPF rules.
[Schedule 1, item 1, paragraphs 58BR(5)(a), 58BS(4)(a) and 58BY(4)(a)]

1.201 The SPF rules may prescribe a scheme for authorising third parties to operate data gateways, portals or websites that give access to reports under the SPF principles, including reports given by regulated entities and the SPF regulators.
[Schedule 1, item 1, subsection 58BT(1)]

1.202 The use of a third-party scheme is intended to streamline and standardise the process of giving reports by regulated entities, and reports by SPF regulators to regulated entities, including by leveraging existing schemes that may already receive scam-related information.

1.203 As part of prescribing the scheme, the SPF rules may include (but are not limited to):

- provisions conferring functions or powers on the SPF general regulator under the scheme;
- the criteria for a person to be authorised under the scheme;
- provisions providing that authorisations may be granted subject to conditions, and that conditions may be imposed on an authorisation after it has been granted;
- provisions providing that authorisations may be granted at different levels corresponding to different risks;
- provisions specifying what a person authorised at a particular level is authorised to do (or not authorised to do);
- provisions dealing with the period, renewal, transfer, variation, suspension, revocation or surrender of authorisations;
- notification requirements on persons whose authorisations have been varied, suspended, revoked or surrendered;
- transitional rules for when an authorisation is varied, is suspended or ends, including in relation to SPF personal information; and
- provisions for the making of applications for internal review, or of applications to the Administrative Review Tribunal for review, of decisions of a person under the scheme.

[Schedule 1, item 1, subsection 58BT(2)]

1.204 These rules are intended to provide clarity on the role and scope of any authorised third-party scheme, to ensure regulated entities understand their reporting obligations. The ability for the SPF rules to confer functions or powers on the SPF general regulator under the scheme is intended to ensure any new third-party scheme which might be made for the purpose of the SPF, is governed and administered by an appropriate body.

1.205 A person authorised under the scheme may use or disclose SPF personal information to the extent that is reasonably necessary to achieve the object of the SPF.
[Schedule 1, item 1, subsection 58BT(3)]

Duty of confidence and authorised disclosures

1.206 A duty of confidence, which is a legally enforceable obligation to maintain confidence, owed under an agreement or arrangement has no effect to the extent that it would otherwise prevent information from being reported as required under this SPF principle.
[Schedule 1, item 1, section 58BU]

1.207 Duties of confidence are overridden to ensure all required and relevant information is reported to the relevant SPF regulator. The significant financial

and emotional harm caused by scams warrants prioritising information sharing to combat scams over a duty of confidence. It is expected that in most cases the party owed the duty of confidence will directly benefit from the sharing of information to disrupt scams.

1.208 The requirements for a regulated entity to give reports of actionable scam intelligence and scam reports are also a requirement by law to disclose the information that is required to be contained in those reports. Therefore, a regulated entity's compliance can be a defence to a secrecy provision, such as section 276 of the Telecommunications Act (see paragraph 280(1)(b) of that Act) and is authorised under Australian Privacy Principle 6 in the Privacy Act (see paragraph 6.2(b) of that Principle).
[Schedule 1, item 1, note to section 58BU]

SPF general regulator may share information with specified persons

1.209 The ACCC, as the SPF general regulator, may disclose information relating to an action which is a 'scam' (as defined in the Bill or within the ordinary meaning of that expression) to a specified entity. In this context, actions which constitute a scam are referred to as a 'scamming action'.
[Schedule 1, item 1, subsection 58BV(1)]

1.210 The intention for including both scams as defined in the Bill and within the ordinary meaning of the expression is to ensure the ACCC is not unnecessarily restricted by the definition of scam in the SPF in its ability to share information, when doing so would support a coordinated response to scams and support the objectives of the SPF. For example, this will allow the ACCC to share information to a specified person about a scam within the ordinary meaning of scam, but which is not a scam associated with a regulated entity in the SPF and therefore not a scam within the definition of scam in the Bill.

1.211 Under this provision, the ACCC may disclose information relating to scamming action to the following entities:

- a regulated entity;
- a Commonwealth agency or authority involved in developing Government policy relating to the SPF;
- a law enforcement agency of the Commonwealth, or of a State or Territory;
- an agency of a foreign country, or of part of a foreign country, that is a law enforcement agency, or is a regulatory agency responsible for scam prevention, if the ACCC is satisfied that:
  - the agency has given an undertaking for controlling the storage, handling and use that will be made of the information and ensuring that the information will be used only for the purpose for which it is disclosed to the agency; and

– it is appropriate, in all the circumstances, to disclose the information to the agency.

[Schedule 1, item 1, subsections 58BV(2) and (3)]

1.212 SPF regulators may also disclose information and documents to each other under Division 5. Further information about this is set out under the heading 'Division 5 – Regulating the SPF'.

1.213 The information that may be disclosed includes SPF personal information, which may include information about:

- a person reasonably suspected of committing a scam, or being involved in the commission of a scam;
- an SPF consumer who was engaged (or was attempted to be engaged) as part of a scam;
- a person who reports a scam on behalf of an SPF consumer; or
- a person who is impersonated in connection with a scam.

[Schedule 1, item 1, subsection 58BV(4)]

1.214 The sharing of SPF personal information to the specified entities is necessary to support the SPF's object to prevent and respond to scams impacting SPF consumers as it will ensure these entities have the intelligence necessary to take appropriate action to prevent, detect, disrupt and respond to scams as quickly as possible and reduce the possibility of harm to consumers. In particular, the sharing of this information will ensure:

- regulated entities across the scams ecosystem have the information they need to take preventative and disruptive action in relation to scams;
- a Commonwealth agency or authority involved in developing Government policy relating to the scams can provide up-to-date policy advice to the Government on the regulatory environment to combat scams, noting the fast-evolving nature of scams;
- SPF sector regulators have relevant information about scams occurring in their regulated sectors so inadequate action taken by regulated entities or potential breaches can be quickly identified and enforcement action taken, where appropriate;
- law enforcement agencies have information to support criminal proceedings and action being taken in response to scams, against scammers; and
- international law enforcement and regulatory agencies responsible for scams prevention have relevant scams information, recognising that the transnational nature of scams requires a coordinated international approach to minimise scam harms.

1.215 For example, if a banking entity provides a report to the SPF general regulator about a scam that originated through a fraudulent advertisement on a social media platform, this will allow the SPF general regulator to share this information with the social media service provider. The social media service provider can then quickly remove an advertisement or suspend an account suspected to be associated with scam activity and prevent further consumers from being impacted.

1.216 However, if the disclosure is to another Commonwealth agency or authority involved in developing the Government policy relating to the SPF, then any SPF personal information must first be de-identified. This reflects that de-identified information will be sufficient in any policy development or consideration regarding the SPF.
[Schedule 1, item 1, subsection 58BV(4)]

1.217 Enabling the SPF general regulator to share scam information with international law enforcement and regulatory agencies responsible for scam prevention is consistent with Australia's commitment made as a signatory of the Global Fraud Summit Communiqué on 11 March 2024 to 'share learning, information, and resources across government, law enforcement, industry and regulators'. The Communiqué was agreed between the Assistant Treasurer on behalf of the Australian Government and ministers and representatives of Canada, France, Germany, Italy, Japan, New Zealand, the Republic of Korea, Singapore, the United Kingdom and the United States of America.

1.218 This will enable the SPF general regulator to enter into agreements with partner jurisdictions to share valuable scam information, and therefore better support domestic efforts to curb the harms caused by scams.

1.219 For example, if the SPF general regulator has information that an overseas bank account has been used by suspected scammers, the SPF general regulator could share that information with the relevant regulator or law enforcement agency to enable it to take prompt action, helping to prevent and respond to scams impacting SPF consumers.

1.220 This would also support the SPF general regulator to enter into bilateral information sharing arrangements with partner jurisdictions. For example, if the SPF general regulator has an information sharing arrangement with an overseas regulator, the overseas regulator may share information relating to a suspected scam account in its jurisdiction that is being used to facilitate scams in Australia. The SPF general regulator would be able to share this information with banking entities once they are designated, who could take reasonable steps to disrupt the scam domestically by blocking payments to the international account that is suspected of being part of a scam, in order to prevent and respond to scams impacting SPF consumers.

1.221 The SPF general regulator can only share scam information with an international agency under the SPF if the agency has given an undertaking for controlling the storage, handling and use of the information and ensuring that the information will be used only for the purpose for which it is disclosed to

the agency. For the avoidance of doubt, this does not require an undertaking to be provided for every isolated instance of data sharing, rather a general undertaken can be provided up front to enable ongoing data sharing, provided it is consistent with the general undertaking.

Example 1.9 The SPF general regulator disclosing a scam in the banking, telecommunications and digital platforms sectors

In this example, the banking sector, telecommunications sector and digital platforms sector (including social media services) are regulated sectors. The ACCC, as the SPF general regulator, receives actionable scam intelligence from a banking entity about an investment scam. The report included the suspected scammer's bank account and an advertisement on social media that included the suspected scammer's phone number.

- Disclosure: The SPF general regulator may disclose the suspected scam advertisement to the social media company that is hosting the advertisement. The disclosure would enable the social media company to take reasonable steps to disrupt the scam, for example, by taking down the advertisement or social media account and blocking the relevant users.
- Disclosure: The SPF general regulator may disclose the suspected scammer's banking details to banking entities. This would enable banking entities to take reasonable steps to disrupt the scam, for example, by adding friction or blocking payments made to the suspect account.
- Disclosure: The SPF general regulator may disclose the suspected scammer's phone number to telecommunications providers. This would enable telecommunications providers to take reasonable steps to disrupt the scam, for example, by screening calls to and from the suspect number.

SPF Principle 5: Disrupt

1.222 The simplified outline in Subdivision F of Division 2 provides that:

- Regulated entities must take reasonable steps to disrupt an activity suspected of being a scam and prevent losses arising from such an activity.
- Regulated entities must give a report to the SPF general regulator about whether the entity reasonably believes that an activity is a scam following their investigation.

- The entity will not be liable for damages when taking certain actions to disrupt such an activity during the investigation period.
- An SPF code for the sector may include sector-specific obligations in relation this SPF principle.

[Schedule 1, item 1, section 58BW]

Overarching obligation to take reasonable steps to disrupt scams

1.223 Where a regulated entity has actionable scam intelligence about an activity relating to, connected with or using a regulated service of the entity, the entity must take reasonable steps within a reasonable time to disrupt the activity and prevent loss or harm (including further loss or harm) arising from the activity.
[Schedule 1, item 1, subsection 58BX(1)]

1.224 To avoid doubt, this includes taking reasonable steps to disrupt activity that is already underway from continuing or further impacting SPF consumers.

1.225 A contravention of this obligation does not occur merely because an entity fails to disrupt a scam. Whether an entity has taken reasonable steps is an objective test that will depend on the particular circumstances, including the relevant matters in section 58BB (about the meaning of reasonable steps). The SPF code for a regulated sector may also include sector-specific provisions describing what are reasonable steps and what is a reasonable time for the purposes of this obligation.

1.226 The steps taken by a regulated entity to disrupt the activity should also be proportionate to the actionable scam intelligence that the entity has.
[Schedule 1, item 1, subsection 58BX(3)]

1.227 Depending on the regulated service of a regulated entity, reasonable steps may include:

- removing content associated with scam activity (including scam advertisements or fraudulent accounts);
- blocking phone numbers, accounts, or content associated with scam activity;
- rejecting payments to enable the regulated entity to contact the consumer and provide them with information that the account they are making a payment to has been identified as associated with scam activity; or
- confirming payee details.

1.228 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BX(2)]

Safe harbour for proportionate disruptive action

1.229 A safe harbour applies for any proportionate disruptive action taken by a business while it is investigating actionable scam intelligence it has about an activity relating to, connected with, or using a regulated service of the entity.

1.230 Where a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity, the entity will not be liable in relation to a civil action or proceeding for taking action to disrupt that activity.
[Schedule 1, item 1, subsections 58BZA(1) and (2)]

1.231 However, this protection will only apply if:

- the regulated entity is acting in good faith and in compliance with the SPF provisions;
- the disruptive action is reasonably proportionate to the activity that is the subject of the actionable scam intelligence, and to the information that would be reasonably expected to be available to the entity about the activity;
- the action is taken during the period starting on the day that the information becomes actionable scam intelligence for the entity, and ending when the entity reasonably believes that the activity is or is not a scam, or after 28 days (whichever is the earlier); and
- the action is promptly reversed if the entity identifies the activity is not a scam and it is reasonably practicable to reverse the action.

[Schedule 1, item 1, subsections 58BZA(1) and (2)]

1.232 To determine whether the action is reasonably proportionate, the relevant matters include the potential loss or damage to SPF consumers or to persons carrying on the activity if the action is not taken, and such loss or damage if the action *is* taken and the activity is *not* a scam.
[Schedule 1, item 1, subsection 58BZA(3)]

1.233 In assessing the likely loss or damage to SPF consumers if no action is taken and the activity is a scam, a regulated entity may consider the number of consumers that have interacted with the suspected scam conduct, the information available providing the reasonable suspicion about the conduct, and the suspected losses associated with the activity (if known). This information provides the regulated entity with an understanding of the potential risk to SPF consumers if no action is taken.

1.234 In assessing the likely loss or damage if the action is taken and the activity is not a scam, the regulated entity may consider the potential economic, commercial, and social impacts of the disruption based on the nature of the activity. The safe harbour does not provide a protection for blunt and disproportionate action, such as stopping all real-time payments, blocking calls

and text messages at mass based on a word or phrase (for example, blocking all texts that say 'mum' following the 'hi mum' scam), or taking down a small business's social media page after receiving a single report that suggests it may be associated with scam without any other corroborating evidence. Action taken that constitutes a proportionate step will depend on the level of certainty the regulated entity has that the identified activity is a scam.

1.235 Whether an action is reasonably proportionate should also involve some consideration of competitive interests. Anti-competitive action is not proportionate action, and it is expected that regulated entities will have regard to the circumstances and information available in determining what action is appropriate. The safe harbour protection will not apply where the action taken is not considered to be proportionate and in good faith.

1.236 For example, a regulated entity has received a number of reports in relation to an advertisement on its regulated service. However, some of these complaints appear to use the term 'scam' in an incorrect context and raise issues with other areas of consumer law, such as poor product quality. It is unclear whether the advertisement is associated with scam activity based on the information available to the entity. In determining proportionate action in this case, the regulated entity must assess the potential loss or damage to SPF consumers if action is not taken. This may involve assessing the information available about the activity, the level of consumer interaction with this account, and the losses reported to date. The regulated entity must also consider the loss or damage if the action is taken, and the activity is not a scam. This may include consideration of the potential commercial interests of the advertiser if the content is legitimate and taken down. On balance, given the information available and the risks to commercial interests, it may be appropriate for the entity to determine that no action is proportionate in the circumstances.

1.237 The intention of the safe harbour provision is to enable timely and responsive disruptive action where a regulated entity reasonably suspects scam activity, while also setting clear guardrails and parameters to ensure third parties are protected from ongoing disruptive action where they are not involved in scam activity. For example, a regulated entity may take down a legitimate business's website based on actionable scam intelligence while the regulated entity investigated whether the conduct or activity was associated with a scam. Once the regulated entity concludes that the website has not been used for scam activities, the regulated entity must reverse its actions promptly to minimise disruption to the business.

1.238 The safe harbour protection applies to allow proportionate action for a maximum of 28 days. After the conclusion of an investigation, or after 28 days, whichever is sooner, the regulated entity must:

- if the activity is a scam, implement ongoing disruptive steps, such as permanently removing a scam advertisement or social media account associated with scam activity; or

- if the activity is not a scam, promptly reverse the proportionate action taken during the safe harbour period where practicable; or
- if the entity has not concluded its investigation, continue to take reasonable steps to investigate the activity under the overarching obligation to detect. The safe harbour protection will no longer apply to any proportionate disruptive action taken after the 28-day period.

1.239 In some cases, it will not be possible to reverse specific disruptive action that has been taken during the safe harbour period. For example, it will not be possible for a telecommunications provider to restore a blocked text message or for a banking entity to restore a blocked payment. The intent in these instances is to require the regulated entity to cease the action that is leading to the disruption and enable the use of that service to resume. For example, where text messages from a certain phone number were blocked during the 28-day safe harbour period and it is later identified that the number is not associated with scam activity, the reversal of this action refers to the regulated entity allowing the use of that phone number to resume.

1.240 A regulated entity who wishes to rely on this protection from liability bears an evidential burden in relation to all elements of the safe harbour protection. This refers to the burden of adducing or pointing to evidence that suggests a reasonable possibility that the elements of the safe harbour protection apply. This is appropriate as the relevant matters are peculiarly within the knowledge of the regulated entity, and are not readily available to other parties in a civil action or civil proceeding.

Reporting outcomes of investigations

1.241 Where a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using the entity's regulated service, the entity must give a report about that intelligence to the ACCC as the SPF general regulator before the end of the period prescribed by the SPF rules. The report must contain the kinds of information and be in the manner and form prescribed by the SPF rules.
[Schedule 1, item 1, subsections 58BY(1) and (2)]

1.242 This reporting requirement only applies to a regulated entity when the SPF rules prescribe these matters.
[Schedule 1, item 1, note to subsection 58BY(2)]

1.243 The intention of this requirement is to ensure the ACCC as the SPF general regulator has oversight of the investigations undertaken by regulated entities and the outcomes of those investigations. This is critical for monitoring and enforcement of the requirement to investigate actionable scam intelligence and will ensure the ACCC can then share any relevant information with other entities to support the SPF's object to prevent and respond to scams impacting SPF consumers.

1.244 Failure to comply with this obligation may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BY(3)]

1.245 The SPF rules may prescribe:

- that the report may be given via access to a specified data gateway, portal or website (discussed above under the heading 'Authorised third party schemes for giving reports');
- that the report sets out whether the entity reasonably believes that the activity that is the subject of the intelligence is a scam; and
- different matters for different kinds of activities.

[Schedule 1, item 1, subsection 58BY(4)]

1.246 Consistent with the obligation to report actionable scam intelligence, the report may be required to include SPF personal information, and a duty of confidence owed under any agreement or arrangement is of no effect to the extent that it is contrary to the entity's obligation to report.
[Schedule 1, item 1, subsections 58BY(5) and (6)]

Sector-specific obligations relating to SPF Principle 5: Disrupt

1.247 An SPF code may be made for a regulated sector setting out detailed, sector-specific obligations consistent with this SPF principle. An SPF code may include, for example, sector-specific provisions that:

- describe what are reasonable steps or what is a reasonable time for the purposes of the overarching obligation to disrupt scam activity; and
- require each regulated entity for the sector to provide its SPF consumers with information about activities that are the subject of the entity's actionable scam intelligence.

[Schedule 1, item 1, section 58BZ]

1.248 For example, SPF codes may include provisions requiring a regulated entity to:

- quickly respond to information that identifies scams, such as through requirements to block or suspend an account or a transaction;
- disclose information to impacted SPF consumers in a specified timeframe which may include steps for those consumers about how to prevent further harm or losses; and
- introduce new systems or functionality to enable SPF consumers to take action to stop scams (for example, technology that allows an SPF consumer to stop a transaction or freeze their own accounts).

SPF Principle 6: Respond

1.249 The simplified outline in Subdivision G of Division 2 provides that:

- Regulated entities must have an accessible mechanism for its SPF consumers to report activities that are or may be scams.
- Regulated entities must also have an accessible and transparent IDR mechanism for SPF consumers to make complaints about scam activities and the entity's conduct relating to such activities.
- When undertaking internal dispute resolution, the regulated entity must have regard to any processes prescribed by the SPF rules and any guidelines prescribed by the SPF rules for apportioning liability.
- A regulated entity must be a member of an authorised EDR scheme for dealing with complaints about scams if it provides a regulated service.
- Regulated entities must publish information about these reporting and dispute resolution mechanisms.
- An SPF code for a regulated sector may set out additional conditions relating to consumer reporting, IDR and EDR requirements.

[Schedule 1, item 1, section 58BZB]

Reporting mechanism

1.250 Regulated entities must have an accessible mechanism for a person to report to the entity a scam or possible scam that relates to, is connected with, or uses a regulated service of the entity. This mechanism needs to allow a person who was an SPF consumer of the service at the time they were impacted by the scam or possible scam to make such a report, even if they are no longer an SPF consumer of the service at the time they are making the report.
[Schedule 1, item 1, subsection 58BZC(1)]

1.251 Given the broad definition of SPF consumer, this reporting mechanism will also need to extend to scams and possible scams impacting a person at a time when the regulated service is only purportedly being provided to the person.
[Schedule 1, item 1, note to subsection 58BZC(1)]

1.252 For a reporting mechanism to be accessible to SPF consumers, all classes of SPF consumers must be able to easily locate, access and use the mechanism to make a scam report. This will require a regulated entity to consider the classes of consumers using its service and how they use those services. For example, if a regulated entity has a diverse consumer base, it may be appropriate to go beyond a purely digital mechanism for reporting scams and offer a telephone line.

1.253 Therefore, the relevant form of the reporting mechanism may be different for each regulated entity, depending on its regulated services and SPF customer

base. This may involve an entity allowing SPF consumers to report scams in-person, via phone, or online on a website or a digital application. A combination of methods may be available.

1.254 A regulated entity may also enable an authorised person or organisation to assist with or make a report on behalf of an SPF consumer.

1.255 The reporting mechanism is a critical element of the SPF. It will provide regulated entities with necessary information to fulfil their other obligations under the SPF regarding the prevention, detection, disruption and reporting of scams.

1.256 Failure to comply with the obligation to have an accessible reporting mechanism may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BZC(2)]

Internal dispute resolution

1.257 Regulated entities must have an accessible and transparent IDR mechanism to deal with an SPF consumer's complaint. Under the IDR mechanism, a person can bring a complaint about:

- an activity that is or may be a scam and that relates to, is connected with, or uses a regulated service of the entity, provided the activity impacted the person at the time when they were an SPF consumer of the service; or
- the entity's conduct relating to such an activity.

[Schedule 1, item 1, subsection 58BZD(1)]

1.258 An effective IDR mechanism will benefit both SPF consumers and regulated entities. IDR will provide regulated entities with an opportunity to assess their conduct and resolve the SPF consumer's complaints in a timely and efficient manner. The IDR obligation 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.

1.259 The relevant IDR mechanism must be accessible to SPF consumers and should provide flexibility in how complaints can be lodged. For example, a complaint may be made in-person, via phone, letter, online or a combination of these methods. The regulated entity may enable an authorised person or organisation to assist or progress a complaint on behalf of an SPF consumer.

1.260 To ensure the IDR mechanism is accessible for SPF consumers, the regulated entity should set out its complaints handling process in writing and make it available on the entity's website. This would also support the obligation on regulated entities to publish information about the rights of SPF consumers, discussed in further detail below.

1.261 Failure to comply with these obligations may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'. ***[Schedule 1, item 1, subsection 58BZD(2)]***

Processes and guidelines for undertaking IDR

1.262 When undertaking IDR in dealing with a person's complaint, regulated entities must have regard to any processes prescribed by the SPF rules and any guidelines prescribed by the SPF rules for apportioning any liability arising from the complaint.
[Schedule 1, item 1, subsection 58BZE(1)]

1.263 Prior to making the SPF rules, the Treasury Minister must be satisfied that appropriate and reasonably practicable consultation is undertaken. This is required under section 17 of the *Legislation Act 2003*.

1.264 Processes or guidelines may set out the information that regulated entities should provide to SPF consumers in responding to a complaint at the IDR stage. For example, in providing a written IDR response, regulated entities may be required to provide information to the consumer addressing and setting out the entity's position on the issues raised and providing enough documentation for the consumer to understand the entity's compliance with its obligations. This is intended to address the information asymmetry between regulated entities and consumers, where the consumer is unlikely to have all the information about the actions taken by a regulated entity to comply with the requirements under the SPF. It is also intended to help inform the consumer when deciding whether to escalate their complaint to an EDR scheme.

1.265 However, it is not intended that regulated entities will be expected to provide information in an IDR process that would reveal the specific steps the entity is taking to comply with SPF provisions, if that were to risk providing scammers with a pathway to avoid detection.

1.266 Any processes or guidelines prescribed by the SPF rules are intended to assist regulated entities to effectively deal with complaints, including those involving multiple regulated entities that have not met their SPF obligations. For example, a complaint might involve a regulated entity in the telecommunications sector and a regulated entity in the banking sector where a scammer engages an SPF consumer via a text message, which results in the consumer making an electronic bank payment to the scammer.

1.267 In these instances, without guidance, consumers may undergo IDR with multiple entities and be unsuccessful due to each regulated entity shifting responsibility to another entity or entities. This may prevent quick and fair resolutions at the IDR stage and result in a higher number of complaints escalating to EDR.

1.268 The processes and guidelines prescribed by the SPF rules will assist in streamlining IDR for complaints involving multiple regulated entities. For

example, the Minister may prescribe a process outlining how regulated entities should interact with each other at the IDR stage to allow for early resolution of disputes where more than one entity may not have met its obligations under the SPF. The Minister may also prescribe guidance on how to apportion liability between multiple regulated entities that have breached their SPF obligations in a particular type of scam.

1.269 Using the SPF rules to prescribe processes and guidelines is appropriate as it provides the flexibility to include details about specific types of scams. This would not be appropriate for inclusion in the primary law given the evolving and often complex nature of scams. It is also appropriate for these processes be prescribed in the SPF rules rather than SPF codes that only apply to a particular regulated sector because scams are likely involve multiple regulated entities.

1.270 Failure to comply with the obligation to have regard to the processes and guidelines prescribed by the SPF rules may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BZE(2)]

Publishing information about the rights of SPF consumers

1.271 A regulated entity must make information about the rights of its SPF consumers publicly available. Specifically, the entity must publish information about SPF consumers' rights with respect to the entity's reporting mechanism, IDR mechanism and SPF EDR scheme for which the entity is a member.
[Schedule 1, item 1, subsection 58BZF(1)]

1.272 This will ensure SPF consumers can easily access relevant information to understand their options for dealing with an activity that is or may be a scam and how to make a complaint about the regulated entity's conduct with respect to the SPF.

1.273 Failure to comply with obligation may attract civil penalties. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsection 58BZF(2)]

External dispute resolution

1.274 A Treasury Minister may authorise an SPF EDR scheme for the purposes of the SPF and one or more regulated sectors. This may include an existing scheme (such as the AFCA scheme that is authorised under Part 7.10A of the Corporations Act) or a new scheme. More than one SPF EDR scheme may be authorised for the purposes of the SPF – for example, a different SPF EDR scheme for each regulated sector.
[Schedule 1, item 1, section 58DB]

1.275 A regulated entity must not provide a regulated service if they are not a member of an SPF EDR scheme.
[Schedule 1, item 1, subsection 58BZG(1)]

1.276 An EDR mechanism is intended to provide a pathway for redress, including compensation, for an SPF consumer of a regulated service where a regulated entity has not complied with its obligations under the SPF.

1.277 The authorised SPF EDR scheme is intended to offer an independent, impartial and fair mechanism for SPF consumers to escalate their complaints where they are not resolved at the IDR stage or if the IDR outcome is unsatisfactory. It is not intended for SPF consumers to be charged any fee for escalating their complaints to an SPF EDR scheme.

1.278 Although more than one SPF EDR scheme may be authorised, the intention is that a single authorised SPF EDR scheme will cover multiple regulated sectors. In particular, the Minister has announced his intention to authorise AFCA as the single EDR scheme for the initially designated sectors.

1.279 This will provide SPF consumers with a straightforward path to EDR where multiple regulated entities are involved in a single complaint, and therefore lower the administrative burden for both SPF consumers and regulated entities compared to if multiple SPF EDR schemes were available for a particular complaint. This is also intended to ensure consistency in the experience of SPF consumers and in the consideration of complaints.

1.280 A regulated entity that is a member of an SPF EDR scheme must give reasonable assistance to, and cooperate with, the operator of the scheme. The entity must do so regardless of whether the entity is subject to a complaint under the scheme.
[Schedule 1, item 1, subsection 58BZG(2)]

1.281 This requirement to cooperate with the operator of the SPF EDR scheme includes:

- giving effect to any determination made by the operator in relation to the complaint; and
- identifying, locating and providing to the operator any documents and information that it reasonably requires for the purposes of resolving the complaint within a reasonable time.

1.282 Failure to comply with the EDR obligations, including any relevant obligations in the SPF code for the regulated sector, may attract a civil penalty. Subdivision C of Division 6 deals with civil penalty provisions. Further information is set out under the heading 'Division 6 – Enforcing the SPF'.
[Schedule 1, item 1, subsections 58BZG(3) and (4)]

Sector-specific obligations relating to SPF Principle 6: Respond

1.283 An SPF code may be made for a regulated sector setting out detailed, sector-specific obligations consistent with this SPF principle. An SPF code may include, for example, sector-specific provisions setting out:

- conditions that must be met for the reporting mechanism;
- conditions (such as standards and requirements) that must be met for the IDR mechanism;
- obligations that must be met in relation to an SPF EDR scheme.

[Schedule 1, item 1, section 58BZH]

1.284 For example, the SPF codes may contain requirements about the type of information that the regulated entity must include in its reporting form, such as contact details used by the scammer, the type of scam or outcome of the scam.

1.285 These requirements are more suitable to be included in SPF codes as they may vary depending on the regulated sector and to allow for flexibility to quickly update requirements in response to changes in scam trends in certain sectors.

1.286 In relation to the conditions that must be met for the IDR mechanism, the SPF code may set out the timeframes for responding to a complaint, requirements for regulated entities to engage and cooperate with other relevant parties (including other regulated entities) during the IDR process, record-keeping obligations and obligations relating to the process to escalate a complaint beyond IDR.

1.287 For example, the SPF codes may set out mandatory maximum periods for regulated entities to provide an IDR response to complaints. This could include different timeframes depending on the complexity of a complaint or the particular sector.

1.288 SPF codes may also set out guidelines about the information that regulated entities should provide to SPF consumers in responding to a complaint at the IDR stage, with reference to the complexity of the complaint or the particular complaint made by the consumer.

1.289 However, it is not intended that regulated entities will be required to disclose specific information that would breach some other legislative obligation, including under the privacy law and anti-money laundering and counter terrorism legislation.

1.290 As the Treasury Minister may authorise more than one EDR scheme for the purposes of the SPF, it is necessary that the SPF codes are able to set out requirements on regulated entities relating to the relevant EDR scheme.

Application of the SPF principles

Example 1.10 A scam in the banking sector

ABC Bank is a regulated entity in the banking sector. It has been targeted by a large-scale spoofing scam where scammers' messages are appearing on the same SMS message chain as the legitimate SMS message chain from the bank. The scammer impersonates the banking entity to deceive the consumer to authorise a transfer of money from the consumer's account to another account by asking the consumer to provide their one-time passcode to authorise that transfer. For the purposes of the example, there is not yet an SPF code made for the sector.

While obligations will also apply to the telecommunications provider in relation to this activity, this example focuses on how ABC Bank may meet its obligations under the SPF. ABC Bank will not have contravened its obligations merely because the scam activity is occurring using its service, rather it will be found to have breached its obligations if it failed to take reasonable steps in the circumstances. Without setting out an exhaustive list of reasonable steps under each obligation, examples of steps the entity may be expected to take are set out below:

- Prevent: ABC Bank publishes a warning on its website in relation to this scam and the steps it is taking to protect consumers. This warning clearly communicates that ABC Bank will never ask a consumer for their one-time passcode so consumers can easily identify scam activity. ABC Bank works with its telecommunications provider to better protect its SMS Alphanumeric Tag so that scammers are unable to impersonate it.
- Detect: ABC Bank takes steps to investigate consumer reports and trace actionable scam intelligence received within 28 days.
- Report: ABC Bank shares actionable scam intelligence as prescribed by the SPF rules in relation to the SMS and bank accounts used by the scammer, identified through reports by consumers, with the SPF general regulator.
- Disrupt: ABC Bank rejects high value transfers and contacts consumers to understand the nature of the transaction before authorising the payment. It also displays a visible warning in apps and online banking

services to consumers before they finalise payment to disrupt the scam attempt.

Example 1.11 A scam in the telecommunications sector

XYZ Mobile is a regulated entity in the telecommunications sector providing services as a carriage service provider. It receives information from the SPF general regulator that consumer reports indicate that a significant number of impersonation scams are being received by its customers.

XYZ Mobile will not have contravened its obligations merely because the scam activity is occurring and affecting its customers, rather it will be found to have breached its obligations if it failed to take reasonable steps in the circumstances. Without setting out an exhaustive list of reasonable steps under each obligation, examples of steps the entity may be expected to take are set out below:

- Prevent: XYZ Mobile makes information available on its website about an increase in scam activity observed and provides updated information on what steps it is taking to manage scam activity.
- Detect: XYZ Mobile strengthens mechanisms to detect recent abnormally high volumes of traffic from a service provider and traces the originating point of spoofed phone calls.
- Report: XYZ Mobile shares information about any consumer reports received in relation to scam activity to the SPF general regulator.
- Disrupt: Where XYZ Mobile has formed a reasonable view that it has detected a number being used for scam calls, it blocks those numbers.

Example 1.12 A scam in the digital platforms sector

FriendZone is a regulated social media service provided by FriendZone Ltd as the regulated entity under the SPF. FriendZone receives an increase in consumer reports relating to fraudulent advertisements on its service for cryptocurrency investment schemes. Upon examination, the cryptocurrency is non-existent, and the advertisement involves deceiving victims to enter their personal details on a fake exchange platform.

FriendZone will not have contravened its obligations merely because the scam activity is occurring using its service, rather it

will be found to have breached its obligations if it failed to take reasonable steps in the circumstances. Without setting out an exhaustive list of reasonable steps under each obligation, examples of steps the entity may be expected to take are set out below:

- Prevent: FriendZone has additional identity verification for accounts looking to post advertisements on its service. FriendZone makes information available to consumers about an increase in fraudulent investment advertisements in their feed and steps they can take to stay vigilant.
- Detect: FriendZone scans its systems using algorithms to identify suspicious businesses and account holders involved in cryptocurrency advertisements. It takes steps to investigate the actionable scam intelligence received through consumer reports within 28 days.
- Report: FriendZone shares actionable scam intelligence about the fraudulent accounts reported by consumers with provides the SPF general regulator.
- Disrupt: FriendZone suspends reported fraudulent advertisements and associated accounts for a period of 28 days while undertaking investigative action to verify the nature of those advertisements. Any verified scam advertisements are removed, and disruptive action is unwound for any legitimate advertisements and accounts identified within the 28 day period.

Division 3 – Sector-specific SPF codes

1.291 The simplified outline in Division 3 provides that:

- A Treasury Minister may make an SPF code for each regulated sector.
- Each SPF code is to include sector-specific provisions relating to the SPF principles, other than SPF Principle 4: Report.
- Requirements in a code can be civil penalty provisions. The relevant SPF sector regulator will monitor, investigate and enforce compliance with these provisions. Division 6 sets out remedies for non-compliance.

[Schedule 1, item 1, section 58CA]

1.292 A Treasury Minister may by legislative instrument make an SPF code for a regulated sector.
[Schedule 1, item 1, section 58CB]

1.293 These SPF codes are intended to support the SPF principles that underpin the framework to prevent and respond to scams impacting SPF consumers. However, the SPF is designed to operate even if an SPF code is not made for a regulated sector, as the overarching SPF principles will generally apply when an entity becomes a regulated entity.

1.294 SPF codes will be subject to sunsetting and Parliamentary scrutiny through the disallowance process.

1.295 An SPF code must:

- be consistent with the SPF principles;
- only deal with the themes or matters covered by the following SPF principles: governance, prevent, detect, disrupt, and respond, and
- if applicable, include provisions about matters prescribed by the SPF rules.

[Schedule 1, item 1, subsection 58CC(1)]

1.296 An SPF code is expected to set out detailed obligations that are specific to a regulated sector. This recognises the differing roles each regulated sector has in the broader scams ecosystem and the unique scams-related challenges faced by regulated entities in different sectors.

1.297 There may also be circumstances where the provisions of an SPF code only apply to certain regulated entities within the sector. For example, different obligations may apply to regulated entities in the sector that are at different stages of the supply chain. For example, an SPF code for the telecommunications sector may set out different obligations for carriage service providers and transit carriers, given their different role in the supply chain.

1.298 The SPF code obligations will generally only create minimum standards for that sector, which an entity may be required to go beyond to comply with the SPF principles. Accordingly, compliance with relevant provisions of an SPF code is relevant to, but not determinative of, whether a regulated entity has taken reasonable steps for the purposes of an SPF principle (see section 58BB for the meaning of reasonable steps).

1.299 Under the Attorney-General's Department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, serious pecuniary penalties are most appropriately placed in primary Acts of Parliament rather than subordinate legislation. While there the SPF codes may include obligations that are civil penalty provisions, the maximum penalty that can be ordered for a contravention of such a provision has been placed in primary law. As such, the amendments broadly meet the principles set out in the Guide.

1.300 An SPF code may also deal with related or incidental matters, including (but not limited to):

- provisions relating to only certain types of regulated services for the sector;
- provisions relating to only certain kinds of SPF consumers of regulated services for the sector;
- circumstances where persons are relieved from compliance with SPF requirements that would otherwise apply to them;
- provisions that confer powers on the SPF sector regulator or on another person (subject to the constraint that SPF code provisions must be consistent with the SPF principles);
- provisions that depend on the SPF sector regulator being satisfied of one or more specified matters;
- the internal review processes that persons acting under the SPF code must establish and have in place or for making applications to the Administrative Review Tribunal;
- the manner in which persons or bodies may exercise powers or must meet the requirements under the SPF code. For example, requiring the use of a form approved by the SPF sector regulator or SPF general regulator;
- whether a regulated entity for the sector may charge a fee, the manner in which the fee may be charged, the time in which a fee can be paid and how the fee needs to be communicated (including how notice may be given to the person that is required to pay the fee);
- provisions that require an agent of a regulated entity to do or not do specific things when acting on behalf of the regulated entity and within the scope of the agent's actual or apparent authority;
- provisions that authorise a regulated entity for the sector to use or disclose SPF personal information to the extent necessary to comply with the entity's obligations under the code; and
- any other matters that the provisions in Part IVF provide may be included or dealt with in the SPF code.

[Schedule 1, item 1, subparagraph 58CC(1)(b)(ii) and subsection 58CC(2)]

1.301 Provisions of the SPF code may be civil penalty provisions (within the meaning of the Regulatory Powers Act).
[Schedule 1, item 1, subsection 58CC(3)]

1.302 An SPF code may make provisions that apply, adopt, or incorporate other instruments or writing in force at a particular time or from time to time. This is necessary to ensure that where there are existing scam prevention frameworks already in place for a particular sector, they can be brought into the SPF to ensure that the new obligations under the SPF apply alongside and in respect of

those existing frameworks. This ability to incorporate other documents in writing is explicitly provided for in the primary law, to ensure subsection 14(2) of the *Legislation Act 2003* does not prevent this effect.
[Schedule 1, item 1, subsections 58CC(4) and (5)]

1.303 The Treasury Minister's power to make an SPF code may be delegated in writing to another Minister, the ACCC, or the entity that is, or will be, the SPF sector regulator.
[Schedule 1, item 1, section 58CD]

1.304 This delegation may be exercised where the Treasury Minister considers that another Minister or another regulator has the necessary industry knowledge, understanding and information to best address scams in that sector and to make an appropriate SPF code. Some sectors will have regulators that have experience monitoring and enforcing comparable regulatory regimes to the SPF who will also have the capability to develop an SPF code for that sector. They may also have strong stakeholder relationships and industry expertise that could be leveraged during the instrument development process. For example, the telecommunications industry is already regulated by ACMA, and it may be appropriate for the delegation to be made to ACMA with respect to the telecommunications sector.

Division 4 – External dispute resolution

1.305 The simplified outline in Division 4 provides that:

- One or more EDR schemes may be authorised for dealing with complaints about scams in designated sectors.
- An existing EDR scheme such as AFCA could be authorised, or new schemes could be developed and authorised.

[Schedule 1, item 1, section 58DA]

1.306 A key component of the SPF is the availability of EDR to resolve disputes relating to scams that could not be satisfactorily resolved through IDR, and to provide pathways for redress where regulated entities have not met their SPF obligations.

1.307 The amendments provide that a Treasury Minister may, by legislative instrument, authorise an EDR scheme, called an SPF EDR scheme, for the purposes of the SPF and for one or more regulated sectors. This may include an existing scheme or a new scheme.
[Schedule 1, item 1, section 58DB]

1.308 A regulated entity must not provide a regulated service if they are not a member of an SPF EDR scheme authorised by the Treasury Minister for their regulated sector.
[Schedule 1, item 1, subsection 58BZG(1)]

1.309 More than one EDR scheme may be authorised under the SPF. However, the intention is that the AFCA scheme (within the meaning of the Corporations Act) will be authorised as the single SPF EDR scheme for the three initially designated sectors.

1.310 Having the AFCA scheme as the single SPF EDR scheme ensures SPF consumers in these sectors have access to straightforward, 'single door', free and fair complaints resolution mechanism for their scams-related complaints. This will lower the administrative burden for consumers and regulated entities as multiple SPF EDR schemes will not need to be involved in a single complaint involving multiple regulated entities across different sectors. A single scheme is also intended to ensure consistency in consumers' experiences accessing EDR under the SPF and in the consideration of complaints.

Authorisation of an EDR scheme

1.311 A Treasury Minister may, by legislative instrument, authorise an SPF EDR scheme for the purposes of the SPF and one or more regulated sectors if:

- the scheme is already authorised under a Commonwealth law for another purpose; or
- the Minister is satisfied that the requirements prescribed by the SPF rules are met by the scheme.

[Schedule 1, item 1, subsection 58DB(1)]

1.312 This instrument will be subject to sunsetting and Parliamentary scrutiny through the disallowance process.

1.313 Before authorising a scheme, the Minister must consider the accessibility, independence, fairness, accountability, efficiency and effectiveness of the scheme, and any other matters the Minister considers relevant. However, failure to consider these matters does not invalidate the instrument authorising the scheme.
[Schedule 1, item 1, subsection 58DB(2)]

1.314 In accordance with subsection 33(3) of the *Acts Interpretation Act 1901*, the Minister may also vary and repeal the authorising instrument.
[Schedule 1, item 1, note 2 to subsection 58DB(1)]

1.315 The Minister may specify conditions on the SPF EDR scheme in the instrument authorising the scheme.
[Schedule 1, item 1, subsection 58DB(3)]

1.316 If the Minister chooses to authorise a new SPF EDR scheme, the Minister must set out the details of the scheme in the legislative instrument which authorises that scheme.
[Schedule 1, item 1, subsection 58DB(4)]

1.317 More than one SPF EDR scheme may be authorised under the SPF. The Minister may also authorise an SPF EDR scheme that applies to one or more regulated sectors.
[Schedule 1, item 1, subsection 58DB(5)]

1.318 However, the Minister is expected to authorise the AFCA scheme (within the meaning of the Corporations Act) as the single SPF EDR scheme for the three initial sectors that will be designated to be regulated sectors under the SPF. The AFCA scheme is authorised under Part 7.10A of the Corporations Act and is overseen by ASIC. If the Minister chooses to authorise the AFCA scheme as the SPF EDR scheme for one or more regulated sectors, all of ASIC's existing functions and powers to oversee the AFCA scheme under Part 7.10A of Corporations Act (for example, section 1052A of that Act) will apply to regulate the scheme for the purposes of the SPF and those sectors.
[Schedule 1, item 1, note 1 to subsection 58DB(1)]

1.319 The Minister may authorise a new SPF EDR scheme for the purposes of the SPF and one or more regulated sectors if the Minister is satisfied that the requirements prescribed by the SPF rules are met by the scheme.
[Schedule 1, item 1, paragraph 58DB(1)(b)]

1.320 The SPF rules may prescribe the following requirements for a new SPF EDR scheme:

- organisational requirements for membership of the scheme;
- requirements for the operator of the scheme;
- requirements for how the scheme is to operate;
- requirements to be complied with by members of the scheme; and
- requirements for making changes to the scheme.

[Schedule 1, item 1, subsection 58DC(1)]

1.321 For example, the SPF rules may require that the complaints mechanism under the scheme is appropriately accessible, that appropriate expertise is available to deal with complaints, or that determinations made by the operator of the new SPF EDR scheme be binding on members of the scheme but not binding on complainants under the scheme.

1.322 The instrument authorising a new SPF EDR scheme may provide for the following:

- powers of one or more of the Minister, an SPF regulator, or a Commonwealth entity within the meaning of the PGPA Act under the scheme;
- powers of the scheme's operator under the scheme, including powers to seek information, make determinations of complaints and make determinations imposing financial and non-financial remedies;

- appeals to the Federal Court of Australia from determination by the scheme's operator;
- information sharing and reporting;
- a provision that depends on the scheme's operator or another person being satisfied of one or more specified matters; and
- provisions about any other matters that provisions of the SPF provide may be specified, or otherwise dealt with, in the scheme.

[Schedule 1, item 1, paragraphs 58DC(2)(a) to (e) and (g)]

1.323 Such a scheme may also include provisions about the manner in which the scheme's operator may charge a fee under the scheme, the time for paying a fee and giving notice of, or publicising, a fee or matters about a fee. For example, the scheme may require that operations of an SPF EDR scheme be financed through fees charged to members of the scheme. It is not intended that such a scheme would ever require SPF consumers to be charged a fee to submit a complaint to the scheme.
[Schedule 1, item 1, paragraph 58DC(2)(f)]

1.324 Prescribing certain kinds of provisions in the SPF rules does not automatically include those provisions in any new SPF EDR scheme. The SPF rules can only prescribe provisions that can be validly included in the instrument authorising a new SPF EDR scheme. Allowing the SPF rules to prescribe matters that a new SPF EDR scheme may deal with is necessary as the relevant SPF EDR scheme may vary depending on the regulated sector.

Reporting obligations

1.325 Under the SPF, the operator of an SPF EDR scheme has certain obligations to report to SPF regulators.

1.326 The operator of an SPF EDR scheme must give particulars of a matter to the SPF general regulator and the SPF sector regulator for the sector, if the operator becomes aware that:

- a serious contravention of any law may have occurred in connection with a complaint under the scheme; or
- a party to a complaint under the scheme may have failed to give effect to a determination by the operator relating to the complaint (including a refusal to give effect to that determination); or
- there is a systemic issue arising from the consideration of complaints under the scheme.

[Schedule 1, item 1, subsection 58DD(1)]

1.327 If the matter relates to multiple entities in different sectors, the operator of an SPF EDR scheme must provide particulars of the matter to each of the relevant SPF sector regulators, as well as the SPF general regulator.

1.328 In relation to serious contraventions of law, this reporting requirement is intended to relate to laws that are relevant to the complaint made to the SPF EDR scheme, rather than necessarily a contravention of any law. At a minimum, the operator of the SPF EDR scheme must report serious contraventions of SPF provisions. However, other laws, such as the privacy law or corporations law, may also be relevant to the subject matter and circumstances of the complaint. The operator of the SPF EDR scheme should consult with the SPF general regulator and the SPF sector regulator for the sector (as appropriate) if it is unsure about whether or not to refer a particular matter.

1.329 If the parties to a complaint made to an SPF EDR scheme for a regulated sector agree to settle a complaint, and the operator of the scheme thinks the settlement may require investigation, the operator may give particulars of the settlement to the SPF general regulator and to the SPF sector regulator for the sector. This may include providing particulars to multiple SPF sector regulators if the settlement relates to multiple entities in more than one sector.
[Schedule 1, item 1, subsection 58DD(2)]

1.330 The matters that may be relevant for the operator of the SPF EDR scheme to consider in deciding whether a settlement requires regulatory investigation includes where:

- the settlement precludes an SPF consumer from referring a complaint to an SPF regulator, lodging further action or taking other action in relation to matters that are not subject to the complaint; or
- the settlement was offered on onerous or unjust terms, or entered into as a result of duress or misrepresentation.

1.331 If these reporting obligations require the operator of the SPF EDR scheme to give any SPF personal information, the operator must de-identify that information unless the operator reasonably believes that doing so would not achieve the object of the SPF.
[Schedule 1, item 1, subsection 58DD(3)]

Information sharing

1.332 The amendments also provide for information sharing from SPF regulators to the operator of an SPF EDR scheme, to ensure the scheme can operate efficiently and effectively.

1.333 An SPF regulator may disclose information to the operator of an SPF EDR scheme for the purposes of enabling or assisting the operator to perform any of the operator's functions or powers. Any SPF personal information disclosed must be de-identified unless the SPF regulator reasonably believes that doing

so would not achieve the object of the to prevent and respond to scams impacting SPF consumers.
[Schedule 1, item 1, subsections 58DE(1) and (3)]

1.334 An SPF regulator may impose conditions to be complied with by the operator in relation to the information. For example, the SPF regulator may require the operator to observe any confidentiality requirements that apply to the information or require the operator to disclose information to an SPF consumer and regulated entity who are participating in EDR.
[Schedule 1, item 1, subsection 58DE(2)]

Division 5 – Regulating the SPF

1.335 The simplified outline in Division 5 provides that:

- The ACCC, as the SPF general regulator, is the regulator of most aspects of the SPF, including the overarching principles.
- Commonwealth entities may be selected to be regulators of each of the SPF codes (SPF sector regulators).
- The SPF general regulator must enter into arrangements with the SPF sector regulators about the regulation and enforcement of the SPF.
- The regulators may share information and documents about the regulation and enforcement of the SPF.

[Schedule 1, item 1, section 58EA]

1.336 The SPF will be administered and enforced through a multi-regulator framework comprising of an SPF general regulator and SPF sector regulators.

1.337 The multi-regulator model is intended to deliver a whole-of-ecosystem approach to the administration and enforcement of the SPF. This approach will support and harness each regulator's mandate and leverage existing supervision, surveillance and enforcement frameworks already established by regulators.

1.338 The multi-regulator model also recognises existing regulatory relationships and the existing roles and expertise various regulators have across the scams ecosystem.

1.339 The ACCC is the SPF general regulator, responsible for monitoring compliance and administering the SPF, in particular, the SPF principles.

1.340 Commonwealth entities with regulatory functions may be selected to be an SPF sector regulator for an SPF code. The ACCC may also be selected to be the SPF sector regulator. If no other entity is selected, the ACCC will be the SPF sector regulator for an SPF code. SPF sector regulators are responsible for administering and taking enforcement action for breaches of an SPF code.

1.341 To support the multi-regulator framework, the amendments provide for:

- delegation of the SPF general regulator's functions and powers to SPF sector regulators;
- arrangements between SPF regulators concerning the regulation and enforcement of the SPF;
- information sharing between SPF regulators, where relevant to the operation (including enforcement) of the SPF;
- a suite of investigation, monitoring and enforcement powers available to SPF regulators; and
- the power for a Treasury Minister to declare alternative powers (monitoring and investigation powers) apply for an SPF sector regulator.

Regulators of the SPF

SPF general regulator

1.342 The ACCC is the SPF general regulator.
[Schedule 1, item 1, subsection 58EB(1)]

1.343 The SPF general regulator's role in overseeing the SPF provisions across all regulated sectors will support an ecosystem wide approach to the administration and enforcement of the SPF. This is particularly important given the cross-sectoral nature of scam activity. This approach also enables a sector to be brought within the SPF before there is an SPF code or SPF sector regulator designated for the sector.

1.344 The ACCC, in its capacity as the SPF general regulator, has the following functions and powers:

- reviewing and advising the Treasury Minister about the operation of the SPF provisions;
- the ACCC's functions and powers under section 155 of the CCA (which concerns the power to obtain information, documents and evidence) to the extent that section 155 relates to:
  - SPF provisions (other than provisions of SPF codes); or
  - a 'designated scams prevention framework matter' (within the meaning of that section), other than the performance or exercise of a function or power conferred by or under an SPF code;
- developing and publishing non-binding guidance and material relating to the SPF provisions (other than provisions of SPF codes); and

- the functions and powers of the SPF general regulator conferred by any other SPF provisions (for example, powers under the Regulatory Powers Act conferred by an SPF provision).

[Schedule 1, item 1, subsection 58EB(2)]

1.345 The SPF general regulator may also monitor and supervise compliance with the SPF provisions through undertaking activities such as thematic reviews, and undertaking investigation and enforcement of breaches of the SPF in the following circumstances:

- where there has not been a breach of an SPF code, but a regulated entity has breached an obligation in the overarching SPF provisions (such as the SPF principles);
- where an SPF sector regulator refers a matter to the SPF general regulator to take action;
- where the SPF general regulator considers enforcement action under the CCA is appropriate (such as in cases of suspected systemic or cross-sectoral breaches).

1.346 A 'designated scams prevention framework matter' in section 155 of the CCA is a reference to the performance of a function, or the exercise of power, conferred on the ACCC as the SPF general regulator by or under Part IVF of the CCA (introduced by the Bill), legislative instruments (such as an SPF code) made under the CCA for the purposes of Part IVF, or the Regulatory Powers Act to the extent that it applies in relation to provisions of Part IVF.
[Schedule 1, item 11, subsection 155(9AC)]

Delegation by the ACCC (the SPF general regulator)

1.347 To ensure the effective regulation of regulated sectors, the amendments permit the ACCC, or a member of the ACCC, to delegate their respective functions and powers to certain persons.

1.348 Specifically, the ACCC may, by resolution, delegate its functions and powers (as the SPF general regulator) under SPF provisions and under section 155 of the CCA (as described in paragraph 58EB(2)(b)). A member of the ACCC may also delegate, by writing, any of the member's functions and powers under section 155 to the extent that section relates to SPF provisions (other than provisions of SPF codes) or a 'designated scams prevention framework matter' (within the meaning of section 155), other than the performance or exercise of a function or power conferred by or under an SPF code.
[Schedule 1, item 1, subsections 58EC(1) and (2)]

1.349 However, the delegation may only be to any of the following persons:

- a person who is an employee of the ACCC who is an SES employee (or acting SES employee), or holds or performs the duties of an

Executive Level 1 or 2 position, if the ACCC is satisfied that person has the appropriate qualifications, training, skills or experience;

- an SPF sector regulator;
- a member of an SPF sector regulator;
- an employee of an SPF sector regulator who holds or performs the duties of a position that is equivalent to an SES employee (or acting SES employee) or Executive Level 1 or 2 position.

[Schedule 1, item 1, paragraphs 58EC(3)(b) to (e)]

1.350 The ACCC may also delegate the above mentioned powers and functions to a member of the ACCC.
[Schedule 1, item 1, paragraph 58EC(3)(a)]

1.351 The ability to delegate the SPF general regulator's powers and functions to an SPF sector regulator supports an efficient and comprehensive approach to the operation of the multi-regulator model. It also recognises that in certain circumstances, it may be more appropriate for an SPF sector regulator to take forward enforcement action for a breach of the overarching SPF principles. This may occur, for example, where an SPF sector regulator is taking forward enforcement action for related misconduct and breaches across other areas of law, and it is more efficient to pursue all breaches for related misconduct collectively. It may also occur where it is determined that there are separate breaches of both the SPF principles and SPF code provisions. This will enable one regulator to take forward enforcement action against a regulated entity, where appropriate, rather than multiple regulators.

1.352 However, a delegation by the ACCC or a member of the ACCC must not be made to an SPF sector regulator or a member or employee of an SPF sector regulator unless the relevant SPF sector regulator has agreed to the delegation in writing.
[Schedule 1, item 1, paragraph 58EC(4)(a)]

1.353 If the delegation is to an employee of an SPF sector regulator, that SPF sector regulator must also be satisfied that the person has appropriate qualifications, training, skills or experience to perform or exercise the functions or powers.
[Schedule 1, item 1, paragraph 58EC(4)(b)]

1.354 In performing or exercising any functions or powers under a delegation, the delegate must comply with any directions of the delegator (being either the ACCC or a member of the ACCC).
[Schedule 1, item 1, subsection 58EC(5)]

SPF sector regulators

1.355 The amendments provide for the designation of a Commonwealth entity with existing regulatory functions to be an SPF sector regulator for an SPF code for

a regulated sector. This recognises existing regulatory relationships, and the roles and expertise regulators have across the ecosystem.

1.356 SPF sector regulators will be responsible for monitoring compliance with SPF codes and pursuing enforcement actions for suspected breaches. SPF regulators may share information on their regulatory activities in relation to the administration of SPF codes with the SPF general regulator, and in some cases, other SPF sector regulators.

1.357 A Treasury Minister may, by legislative instrument, designate a Commonwealth entity (within the meaning of the PGPA Act) that is already conferred functions by or under a law, to be the SPF sector regulator for a regulated sector. Designation of an SPF sector regulator for a regulated sector may be included in the same instrument as the instrument designating the regulated sector, or the SPF code for the regulated sector.
[Schedule 1, item 1, subsection 58ED(1)]

1.358 This instrument will be subject to sunsetting and Parliamentary scrutiny through the disallowance process.

1.359 For example, the Minister may designate telecommunications services to be a regulated sector under the SPF, and designate ACMA to be the SPF sector regulator for that sector, in either the same or separate instruments. Consequently, any SPF code made for the telecommunications sector will be regulated and enforced by ACMA. The ACCC will continue to regulate the telecommunications sector in relation to the SPF principles, and any other SPF provisions not in SPF codes, that apply to the sector. Similarly, the Minister may designate banking services to be a regulated sector under the SPF and designate ASIC to be the sector regulator for that sector.

1.360 The ACCC is the SPF sector regulator for a regulated sector if, and while, there is no Commonwealth entity designated as the SPF sector regulator for the sector. The ACCC may also be designated to be the SPF sector regulator for a regulated sector.
[Schedule 1, item 1, subsection 58ED(2)]

1.361 The functions and powers of the SPF sector regulator for a regulated sector include those conferred by the SPF code for the sector or any other SPF provisions (for example, powers under the Regulatory Powers Act as conferred by an SPF provision).
[Schedule 1, item 1, paragraph 58ED(3)(a) and (b)]

1.362 If the SPF sector regulator is the ACCC, the SPF sector regulator also has the ACCC's functions and powers under section 155 (which concerns the power to obtain information, documents and evidence). However, only to the extent that section relates to the provisions of the SPF code for the sector or a 'designated scams prevention framework matter' (within the meaning of that section) involving the performance or exercise of a function or power conferred by or under the SPF code for the sector.
[Schedule 1, item 1, paragraph 58ED(3)(c)]

1.363 If the SPF sector regulator is not the ACCC, the functions and powers of the SPF sector regulator include the monitoring and investigation functions and powers set out in Division 6.
[Schedule 1, item 1, note to subsection 58ED(3)]

1.364 A Treasury Minister may, in writing, delegate the power to designate a Commonwealth entity to be an SPF sector regulator for a regulated sector to another Minister. Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain relevant provisions relating to delegations.
[Schedule 1, item 1, subsection 58ED(4)]

Delegation by an SPF sector regulator

1.365 An SPF sector regulator may by writing delegate any of the SPF sector regulator's functions and powers under an SPF provision (other than a provision of the Regulatory Powers Act). Where the SPF sector regulator is the ACCC, the ACCC's functions and power under section 155 as described in paragraph 58ED(3)(c) may also be delegated.
[Schedule 1, item 1, subsection 58EE(1)]

1.366 If the ACCC is the SPF sector regulator, a member of the ACCC may also by writing delegate any of the member's functions and powers under section 155 as a described in paragraph 58ED(3)(c).
[Schedule 1, item 1, subsection 58EE(2)]

1.367 The delegation may be to a member of the SPF sector regulator, or to a person who is an employee of the SPF sector regulator who is an SES employee (or acting SES employee) or holds or performs the duties of an Executive Level 1 or 2 position, or otherwise holds or performs the duties of an equivalent position. The SPF sector regulator must be satisfied the person has appropriate, training, skills or experience to perform or exercise the functions or powers to make the delegation.
[Schedule 1, item 1, subsection 58EE(3)]

1.368 However, where the SPF sector regulator is the ACCC, a member of the ACCC cannot delegate to their functions and powers to another member of the ACCC.
[Schedule 1, item 1, subsection 58EE(2)]

1.369 The delegate must comply with any directions of the delegator when performing or exercising any of the functions or powers under a delegation.
[Schedule 1, item 1, subsection 58EE(4)]

1.370 An SPF sector regulators' functions or powers under the Regulatory Powers Act may be delegated in specified circumstances where provided in a provision of Division 6. This includes for example, under subsection 58FF(4) which relates to investigating compliance with an SPF code.
[Schedule 1, item 1, note to subsection 58EE(1)]

Arrangements between SPF regulators

1.371 The ACCC, as the SPF general regulator, and each SPF sector regulator must enter into an arrangement relating to the regulation and enforcement of the SPF provisions.
[Schedule 1, item 1, subsection 58EF(1)]

1.372 Arrangements between the SPF general regulator and SPF sector regulators are intended to support the efficient operation of the multi-regulator model.

1.373 These arrangements are required to manage the risks associated with a multi-regulator model, including unclear roles and responsibilities, an inconsistent regulatory and enforcement approach and duplication in regulatory or enforcement action. These arrangements are intended to establish clear roles and responsibilities and mechanisms to facilitate effective cooperation between regulators. They may also set out agreed priorities for the administration and enforcement of the SPF to support coordinated and targeted action.

1.374 The ACCC may enter into a single arrangement with all, or one or more, SPF sector regulators, or a separate arrangement with each SPF sector regulator. This requirement does not apply to the extent the ACCC is also the SPF sector regulator for a regulated sector.
[Schedule 1, item 1, subsection 58EF(2)]

1.375 The arrangement must include provisions relating to the matters prescribed by the SPF rules, if any. This is intended to ensure that the arrangement deals with all matters relevant to the regulation of the SPF, to ensure effective and efficient regulation by the SPF regulators.
[Schedule 1, item 1, subsection 58EF(3)]

1.376 For example, the SPF rules could require an SPF regulator to notify other SPF regulators of any requests for scam reports made to a regulated entity and require the requesting regulator to share a copy of the scam report to other regulators on request. The details on how the SPF regulators will carry out this requirement may be agreed between the regulators.
[Schedule 1, item 1, note to subsection 58EF(3)]

1.377 To provide flexibility to the SPF regulators as to the specific arrangements that may suit them best, it is not intended that the SPF rules will prescribe how the SPF regulators are to agree on those matters or what kind of arrangement the SPF general regulator must enter into with each SPF sector regulator.

1.378 Each SPF sector regulator that is a party to such an arrangement must publish the arrangement on its website to promote transparency and enable regulated entities to understand the respective SPF regulator's roles and responsibilities.
[Schedule 1, item 1, subsection 58EF(4)]

1.379 These arrangements should be entered into and published as soon as practicable after an SPF sector regulator is designated for a regulated sector.

1.380 A failure to comply with these arrangement requirements does not invalidate the performance of a function or exercise of a power by an SPF regulator. This is to ensure any administrative failings or other instances of non-compliance do not invalidate the general operation and enforcement of the SPF. It also provides certainty to regulated entities regarding the performance of functions or exercise of powers by an SPF regulator, to ensure that enforcement of the SPF is not compromised.
[Schedule 1, item 1, subsection 58EF(5)]

Information sharing between SPF regulators

1.381 The amendments provide for disclosure between the SPF regulators of information or documents relevant to the operation of the SPF. This is intended to support the effective administration and enforcement of the SPF and the practical operation of the multi-regulator model.

1.382 Where information is shared, it is intended to be either for the purpose of notifying another SPF regulator that action is being taken to avoid dual action, or where the information will be acted upon or used in some way to support the relevant SPF regulator's role in administering and enforcing the SPF.

Authorised disclosure

1.383 An SPF regulator may disclose to another SPF regulator particular information or documents, or information or documents of a particular kind, held by the first mentioned SPF regulator that are relevant to the operation (including enforcement) of the SPF provisions. An SPF regulator may make such a disclosure on request or on its own initiative.
[Schedule 1, item 1, subsections 58EG(1) and (2)]

1.384 SPF personal information may be disclosed between SPF regulators. This is appropriate because this information may be necessary for the SPF regulator to carry out its functions and powers under the SPF. Having sufficient information to undertake effective monitoring, investigation and enforcement action with respect to SPF provisions is therefore critical to achieve the object of the SPF, to prevent and respond to scams impacting the Australian community.
[Schedule 1, item 1, subsection 58EG(3)]

1.385 This requirement has the effect of authorising disclosure between the SPF regulators for the purposes of the privacy legislation, as well as secrecy provisions in the CCA or other Commonwealth laws that otherwise restrict information sharing. For example, disclosures made under this provision would be authorised by law for the purposes of:

- paragraph 155AAA(1)(b) of the CCA in relation to protected information;
- section 59DB of the ACMA Act;

- subsection 127(2) of the ASIC Act; and
- Australian Privacy Principle 6 (see the exception in paragraph 6.2(b) of Schedule 1 to the *Privacy Act 1988*).

[Schedule 1, item 1, note to subsection 58EG(2)]

1.386 An SPF regulator must have regard to the object of the SPF when deciding whether to make a disclosure under these powers. Arrangements between SPF regulators may also deal with when disclosures should be made.
[Schedule 1, item 1, section 58EH]

1.387 For completeness, an SPF regulator is not required to disclose information or documents that:

- concern the internal administrative functioning of the regulator;
- disclose a matter in respect of which the regulator or any other person has claimed legal professional privilege; or
- are of a kind prescribed in the SPF rules.

[Schedule 1, item 1, section 58EJ]

Notice of use or disclosure not required

1.388 An SPF regulator does not have to notify any person that the regulator plans to make a disclosure or has made a disclosure of information or documents under the SPF, or plans to use or has used information or documents disclosed under the SPF. Further, the SPF regulator does not need to notify any person that the regulator has collected SPF personal information under the SPF.
[Schedule 1, item 1, section 58EI]

1.389 This has the effect of removing procedural fairness from the use or disclosure of information by SPF regulators. This approach is necessary to enable the quick flow of information between SPF regulators and drive efficient and expedient enforcement action. This ensures that any inadequate action by regulated entities in complying with the SPF is promptly addressed. Given the fast-moving nature of scams, timely enforcement action in response to potential breaches of the SPF is critical to prevent and respond to scams impacting SPF consumers.

1.390 Removing notification requirements will also ensure that a suspected scammer, who may be the subject of the SPF personal information, is not given notice that an SPF regulator has become aware of their suspected activities, which could otherwise reasonably prejudice a law enforcement investigation.

Division 6 – Enforcing the SPF

1.391 The simplified outline in Division 6 provides that:

- The ACCC, in its role as the SPF general regulator or an SPF sector regulator, may use its powers under the CCA (including section 155) to monitor and investigate compliance with the relevant aspects of the SPF.
- If ACMA or ASIC is an SPF sector regulator, it must use powers in its own legislation to monitor and investigate compliance with an SPF code for the sector.
- Other SPF sector regulators may monitor and investigate compliance with an SPF code using the powers set out in this Division, or a Treasury Minister may declare that it can use the powers in its own legislation.
- The amendments set out the maximum penalties for contraventions of the civil penalty provisions of the SPF by a regulated entity. The amendments create two tiers of contraventions, with a tier 1 contravention attracting a higher maximum penalty than a tier 2 contravention.
- The civil penalty regime will be supported by other enforcement tools as an alternative to court proceedings. These include:
  - infringement notices;
  - enforceable undertakings;
  - injunctions;
  - actions for damages;
  - public warning notices;
  - remedial directions;
  - adverse publicity orders; and
  - other punitive and non-punitive orders.
- Some of these remedies may also be available against a person involved in a contravention of the SPF by a regulated entity, such as a senior officer of the regulated entity.

[Schedule 1, item 1, section 58FA]

1.392 The amendments provide SPF regulators with powers to monitor, investigate and enforce compliance with the SPF. Broadly, the powers of the SPF regulators under Division 6 align with existing powers of the SPF regulators or otherwise incorporate by reference Parts of the Regulatory Powers Act.

1.393 Civil penalties are specified within relevant provisions of the new Part. Each penalty reflects the potential seriousness of a contravention of the relevant provision, with the ultimate aim to deter contravention.

1.394 The tiered approach to civil penalties is intended to reflect that higher penalties would be imposed on obligations where breaches would be the most egregious and have the most significant impact on consumers. Higher penalties for those breaches will incentivise compliance and provide a meaningful deterrent to poor behaviour that is not just seen as a cost of doing business. This is particularly important where regulated entities may profit from scammers using their services.

1.395 The enforcement framework of the SPF is consistent with the Attorney-General's Department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*. Consistent with this Guide, the enforcement framework is based on existing powers in law, including in the Regulatory Powers Act, the CCA and the Telecommunications Act. In particular, the standard provisions of the Regulatory Powers Act are an accepted baseline of powers required for an effective monitoring, investigation and enforcement regulatory regime, while providing adequate safeguards and protecting important common law privileges.

1.396 The enforcement framework is also set out in the primary law, rather than being left to subordinate legislation. SPF sector regulators will be designated through subordinate legislation, but their enforcement powers are set out in the primary law. Where the ACCC, ACMA or ASIC is the relevant SPF regulator, their monitoring and investigation powers under the SPF are also contained in the primary law.

Appointing an inspector

1.397 An SPF regulator may appoint a person to be an inspector. An inspector has specified powers with respect to monitoring and investigating compliance with the SPF, as well as the power to issue infringement notices for alleged contraventions of the civil penalty provisions of the SPF.

1.398 The term inspector is included in the definitions section of the CCA. ***[Schedule 1, item 5, subsection 4(1)]***

1.399 An SPF regulator may, in writing, appoint a person who is one of the following to be an inspector of that regulator for the purposes of this Division:

- an employee of the regulator who is an SES employee or acting SES employee (or equivalent), or who holds or performs the duties of an Executive Level 1 or 2 position (or equivalent);
- a member or special member of the Australian Federal Police.

[Schedule 1, item 1, subsection 58FB(1)]

1.400 However, an SPF regulator must not appoint a person as an inspector unless it is satisfied that the person has the appropriate qualifications, training, skills to exercise the powers of an inspector. Given the key role of inspectors in overseeing compliance with the SPF, this requirement is intended to ensure

only suitably experienced and qualified people are appointed as inspectors.
[Schedule 1, item 1, subsection 58FB(2)]

1.401 A person must, in exercising their powers as an inspector, comply with any directions of the SPF regulator that appointed the inspector. These directions must be of an administrative character.
[Schedule 1, item 1, subsection 58FB(3)]

1.402 If an SPF regulator has not appointed an inspector, the SPF regulator itself is the inspector of the SPF regulator for the purposes of Subdivision A of this Division.
[Schedule 1, item 1, subsection 58FB(4)]

Monitoring and investigating compliance with an SPF Code

1.403 The SPF is designed to respond and adapt to evolving areas of scam activity. The legislation therefore allows for the designation of any number of SPF sector regulators, each with differing powers available under their own legislation which have been developed to reflect the various sectors overseen by the regulator.

1.404 The amendments provide a baseline set of powers to any future SPF sector regulator in relation to monitoring, investigating, and enforcing the SPF. This will ensure that any SPF sector regulator has access to adequate investigative and enforcement powers for the purpose of administering the relevant SPF code. This approach supports a flexible and future-proof SPF, and the expansion of the multi-regulator model, if needed, as scam activity shifts.

1.405 The ACCC, ACMA, and ASIC are all expected to be SPF sector regulators. For these regulators, it is intended that they would have access to their existing monitoring and investigation powers under their respective legislation, as those tools are most effective in monitoring and investigating compliance within their respective sectors.

1.406 Where appropriate, a Treasury Minister may declare that alternative monitoring and investigation powers apply to an SPF sector regulator in relation to a specified provision or provisions of the SPF code. The default powers apply unless such a declaration is in force, or the ACCC, ASIC or ACMA is the SPF sector regulator for the sector. The ACCC, ASIC and ACMA will automatically have alternative monitoring and investigation powers under their own respective legislation if they are designated as an SPF sector regulator for a regulated sector.
[Schedule 1, item 1, sections 58FE, 58FF, 58FG and 58FH]

1.407 This type of declaration is expected to be made to enable an SPF sector regulator, where appropriate, to exercise powers under their own legislation for monitoring and investigative purposes. This will allow SPF sector regulators to continue to use established procedures and processes, and will support the efficient monitoring and investigation of compliance of the relevant SPF code.

Similarly, regulated entities would also likely be familiar with the sector regulator's existing powers and have established procedures to respond to those powers. Accordingly, the availability of alternative existing powers will enable regulated entities to respond efficiently to an SPF sector regulator's monitoring and investigation activities.

1.408 It is necessary and appropriate for the Minister to have this power as it is most relevant to the designation of an SPF sector regulator for a particular sector. As the SPF is designed to prevent and respond to scams impacting SPF consumers, it is important that these designations and declarations can be made quickly and effectively to respond to the emergence of scams and shifting of scam activity in different sectors.

1.409 Scam activity is fluid and could become more active in a previously untouched sector of the Australian economy. The Ministerial power is appropriate so that compliance with an SPF code can be effectively monitored and investigated by a regulator who may have sector specific tools available to them that are appropriate to be used in the SPF context. Leveraging existing monitoring and investigation tools by a sector regulator may also reduce compliance costs on industry participants, who will be more familiar with existing regulatory arrangements.

Default monitoring powers

1.410 Default monitoring powers apply for the SPF code for a regulated sector unless the ACCC, ASIC or ACMA is the SPF sector regulator for the sector or a declaration that alternative monitoring powers apply to another SPF sector regulator is in force.
[Schedule 1, item 1, subsection 58FE(1)]

1.411 Each provision of the SPF code is subject to monitoring under Part 2 of the Regulatory Powers Act, including any provision that is not a civil penalty provision. Part 2 of that Act creates a framework for monitoring whether these provisions have been complied with and includes powers of entry and inspection.
[Schedule 1, item 1, subsection 58FE(2)]

1.412 Information given in compliance or purported compliance with the SPF code is subject to monitoring under Part 2 of the Regulatory Powers Act, which creates a framework for monitoring whether the information given is correct. This framework includes powers of entry and inspection.
[Schedule 1 item 1, subsection 58FE(3)]

1.413 The amendments include a range of modifications to the application of Part 2 of the Regulatory Powers Act to ensure they operate effectively in the SPF context. For the purposes of Part 2 of the Regulatory Powers Act, as that Part applies in relation to provisions of an SPF code and the information given in compliance or purported compliance with the SPF code:

- there are no related provisions;
- the inspector of the SPF sector regulator is an authorised applicant and is an authorised person;
- a magistrate is an issuing officer;
- the SPF sector regulator is the relevant chief executive; and
- the Federal Court, the Federal Circuit and Family Court of Australia (Division 2) and a court of a State or Territory that has jurisdiction in relation to the matter are each a relevant court.

[Schedule 1, item 1, subsection 58FE(4)]

1.414 The relevant chief executive (being the SPF sector regulator) may, in writing, delegate the following powers and functions to an SES employee or acting SES employee, of the SPF sector regulator (or to an employee of the SPF sector regulator who holds or performs the duties of an equivalent position):

- powers and functions under Part 2 of the Regulatory Powers Act in relation to provisions in the SPF code for the relevant regulated sector and the information given in compliance or purported compliance with that SPF code; and
- powers and functions under the Regulatory Powers Act that are incidental to those powers or functions.

[Schedule 1, item 1, subsections 58FE(5) and (6)]

1.415 The relevant chief executive may only make the delegation if they are satisfied that the employee has appropriate qualifications, training, skills or experience to perform or exercise the functions or powers.
[Schedule 1, item 1, subsection 58FE(5)]

1.416 A person exercising powers or performing functions under such a delegation must comply with any directions of the relevant chief executive (being the SPF sector regulator).
[Schedule 1, item 1, subsection 58FE(7)]

1.417 An authorised person (being the inspector appointed by the SPF sector regulator) may be assisted by other persons in exercising those powers or performing those functions or duties as set out above.
[Schedule 1, item 1, subsection 58FE(8)]

Default investigation powers

1.418 Default investigation powers apply for the SPF code for a regulated sector unless the ACCC, ASIC or ACMA is the SPF sector regulator for the sector or a declaration that alternative investigation powers apply to another SPF sector regulator is in force.
[Schedule 1, item 1, subsection 58FF(1)]

1.419 Each civil penalty provision of the SPF code is subject to investigation under Part 3 of the Regulatory Powers Act. Part 3 of that Act creates a framework for investigating whether a provision has been contravened, and includes powers of entry, search and seizure.
[Schedule 1, item 1, subsection 58FF(2)]

1.420 The amendments include a range of modifications to the application of Part 3 of the Regulatory Powers Act to ensure they operate effectively in the SPF context. For the purposes of Part 3 of the Regulatory Powers Act, as that Part applies in relation to evidential material that relates to a civil penalty provision of an SPF code:

- there are no related provisions;
- the inspector of the SPF sector regulator is an authorised applicant and is an authorised person;
- a magistrate is an issuing officer;
- the SPF sector regulator is the relevant chief executive; and
- the Federal Court, the Federal Circuit and Family Court of Australia (Division 2) and a court of a State or Territory that has jurisdiction in relation to the matter are each a relevant court.

[Schedule 1, item 1, subsection 58FF(3)]

1.421 The relevant chief executive (being the SPF sector regulator) may, in writing, delegate the following powers and functions to an SES employee, or acting SES employee, of the SPF sector regulator (or to an employee of the SPF sector regulator who holds or performs the duties of an equivalent position):

- powers and functions under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a civil penalty provision of an SPF code; and
- powers and functions under the Regulatory Powers Act that are incidental to those powers or functions.

[Schedule 1, item 1, subsections 58FF(4) and (5)]

1.422 The relevant chief executive may only make the delegation if they are satisfied that the employee has appropriate qualifications, training, skills or experience to perform or exercise the functions or powers.
[Schedule 1, item 1, subsection 58FF(5)]

1.423 A person exercising powers or performing functions under such a delegation must comply with any directions of the relevant chief executive (being the SPF sector regulator).
[Schedule 1, item 1, subsection 58FF(6)]

1.424 An authorised person (being the inspector appointed by the SPF sector regulator) may be assisted by other persons in exercising those powers or

performing those functions or duties as set out above.
[Schedule 1, item 1, subsection 58FF(7)]

Monitoring and investigation powers of the ACCC

1.425 If the ACCC is an SPF sector regulator, the ACCC may use its powers under the CCA, including section 155 to monitor and investigate compliance with an SPF code for the sector. As a consequential amendment to the inclusion of the SPF in the CCA, section 155 is also amended accordingly.
[Schedule 1, items 6 and 7, subparagraph 155(2)(b)(i) and paragraph 155(2)(a)]

1.426 Obtaining complete and accurate information is central to the ACCC's ability to determine whether certain conduct contravenes the CCA or the Australian Consumer Law, and whether enforcement action is required to address any harm to competition and/or consumers.

1.427 For the purposes of the SPF, the ACCC's powers in section 155 would generally be used to investigate matters that constitute or may constitute a contravention of the SPF obligations. This is consistent with its existing robust and considered processes for investigation into the CCA and Australian Consumer Law. In the majority of cases, the ACCC will request that information be provided voluntarily before relying on its section 155 powers.

1.428 Under section 155, the ACCC can require a person to provide information, documents and/or give evidence under oath or affirmation. The ACCC must consider factors including the value of the information to the ACCC's investigation and the burden of the notice on the recipient.

1.429 The ACCC does not use its powers under section 155 to conduct a 'fishing expedition' for information, documents or evidence. It does not, and cannot, issue a section 155 notice unless the ACCC, its Chair or Deputy Chair has a reason to believe that a person is capable of furnishing relevant information, producing relevant documents or giving relevant evidence that relates to the subject matter of the notice. This is distinct from a belief that a person is capable of providing information, documents or evidence that will establish or is likely to establish a contravention.

Monitoring and investigation powers of ACMA

1.430 If ACMA is the SPF sector regulator for a regulated sector, ACMA has access to its existing monitoring and investigating powers for the purposes of the SPF. It is expected that ACMA would be the SPF sector regulator for the telecommunications sector under the SPF.
[Schedule 1, item 1, section 58FG]

1.431 For clarity, ACMA would have access to monitoring and investigation powers in Parts 26 and 27 of the Telecommunications Act.

1.432 Generally, these powers align ACMA's compliance and investigation tools across telecommunications laws.

1.433 The Minister may by legislative instrument, specify modifications to one or more of ACMA's referenced powers to remove doubt as to how those powers would apply in the context of the SPF code. Where there is possible uncertainty, this modification is necessary and appropriate to ensure that ACMA can effectively enforce the SPF code, which is aimed at preventing and responding to scams impacting the Australian community. The intended effect is that the modification is limited only to ensuring that the application of ACMA's existing powers would apply to the SPF effectively, and in a corresponding way. It is not intended to modify the referenced powers as they ordinarily apply.

1.434 This instrument is subject to sunsetting and Parliamentary scrutiny through the disallowance process.

Monitoring and investigation powers of ASIC

1.435 If ASIC is the SPF sector regulator for a regulated sector, ASIC has access to its monitoring and investigating powers for the purposes of the SPF. It is expected that ASIC would be the SPF sector regulator for the banking sector for the purposes of the SPF.
[Schedule 1, item 1, section 58FH]

1.436 The provisions in Divisions 1, 2, 3, 7, 9 and 10 of Part 3 of the ASIC Act (with some exceptions) would be available to ASIC, and apply to the regulated sector for which ASIC is the SPF sector regulator in the corresponding way to how they currently apply to the corporations legislation. These ASIC Act provisions include monitoring and investigation powers.

1.437 These powers include powers to require persons to provide ASIC with documents or information, which ASIC might use when conducting proactive or reactive monitoring and surveillance activities concerning the relevant SPF code, and in formal investigations into suspected contraventions of the relevant SPF code. Additional powers, such as the power to require a person to attend an examination to answer questions, and to provide reasonable assistance to ASIC, would be available for formal investigations only.

1.438 Some examples of how ASIC may use these powers are outlined below. It is assumed that the banking sector is a designated sector and ASIC is the designated SPF regulator for that sector.

Example 1.13 Formal investigation

ASIC has reason to suspect there may have been a contravention by Bank X of an obligation in the SPF banking sector code, regarding Bank X's systems to prevent scams.

ASIC commences a formal investigation in relation to the suspected contravention, under section 13 of the ASIC Act.

In relation to the suspected contravention of the code, ASIC issues Bank X notices to produce certain books relating to the affairs of Bank X, using powers under Division 3 of Part 3 of the ASIC Act such as sections 30 or 33 of the ASIC Act.

ASIC also conducts examinations of key staff of Bank X under section 19 of the ASIC Act, whom ASIC suspects on reasonable grounds can give ASIC information relevant to the matter it is investigating.

Example 1.14 Surveillance

ASIC is conducting a surveillance of Bank Y's compliance with certain obligations in the SPF banking sector code.

For the purposes of ensuring Bank Y's compliance with the relevant Code obligations, ASIC issues Bank Y a notice to produce certain books relating to the affairs of Bank Y, using powers under Division 3 of Part 3 of the ASIC Act such as sections 30 or 33 of the ASIC Act.

1.439 The Minister may by legislative instrument, specify modifications to one or more of ASIC's referenced powers to remove doubt as to how those powers would apply in the context of the SPF code. This modification is necessary and appropriate to ensure that ASIC can effectively enforce the SPF code, which is aimed at preventing and responding to scams impacting the Australian community. The intended effect is that the modification is limited only to ensuring that the application of ASIC's existing powers would apply to the SPF effectively, and in a corresponding way. It not intended to modify the referenced powers as they ordinarily apply.

1.440 This instrument is subject to sunsetting and Parliamentary scrutiny through the disallowance process.

When alternative powers apply

1.441 Alterative power provisions are provisions of another law that:

- provide an entity with powers to monitor compliance or purported compliance with provisions of a law;
- provide an entity with powers to investigate the provisions of a law; or
- enables the effective operation and enforcement of these powers (which covers, for example, a provision making it an offence to fail to appear to answer questions in relation an investigation).

[Schedule 1, item 1, subsection 58FI(1)]

1.442 A Treasury Minister may, by legislative instrument, declare that specified alternative power provisions apply:

- to the entity in the entity's capacity as the SPF sector regulator for a regulated sector; and
- in relation to specified provisions of the SPF code for the sector, in a way that corresponds to the way the alternative power provisions ordinarily apply.

[Schedule 1, item 1, subsections 58FI(2) and (4)]

1.443 The instrument may specify modifications to one or more of the alternative power provisions to remove doubt as to how those powers would apply in the context of the SPF code. Where there is any uncertainty, this modification is necessary and appropriate to ensure that the SPF sector regulator can effectively enforce the SPF code, which is aimed at preventing and responding to scams impacting the Australian community. The intended effect is that the modification is limited only to ensuring that the application of SPF sector regulator's existing powers would apply to the SPF effectively, and in a corresponding way. It is not intended to modify the existing powers as they ordinarily apply.
[Schedule 1, item 1, subsection 58FI(3)]

1.444 This instrument is subject to sunsetting and Parliamentary scrutiny through the disallowance process.

1.445 The ability to specify modifications is necessary to avoid the risk of an SPF sector regulator's monitoring and investigations powers not operating as intended, which would jeopardise fulfilling the object of the SPF to prevent and respond to scams impacting the Australian community.

Civil penalty provisions

1.446 Various provisions of the SPF principles are civil penalty provisions. Where made, SPF codes may also include civil penalty provisions. These penalties are necessary to deter non-compliance with the SPF provisions by regulated entities, to achieve the object of the SPF to prevent and respond to scams impacting the Australian community. Rather than including a general penalty provision for the Part, civil penalty provisions are specified throughout the Bill. This is consistent with the Attorney-General's Department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.

1.447 A civil penalty provision of an SPF principle means:

- a provision of the SPF principles (see Division 2) that is a civil penalty provision (within the meaning of the Regulatory Powers Act); or

- subsection 58FZM(3) in relation to compliance with a remedial direction given by the SPF general regulator.

[Schedule 1, item 5, subsection 4(1)]

1.448 A civil penalty provision of an SPF code means:

- a provision of an SPF code that is a civil penalty provision (within the meaning of the Regulatory Powers Act); or
- subsection 58FZM(3) in relation to compliance with a remedial direction by an SPF sector regulator.

[Schedule 1, item 5, subsection 4(1)]

1.449 A civil penalty provision of an SPF principle or an SPF code is enforceable under Part 4 of the Regulatory Powers Act. Part 4 of that Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for contravention of the provision. This is known as an SPF civil penalty order.
[Schedule 1, items 1 and 5, subsections 4(1) and 58FJ(1)

1.450 For the purposes of Part 4 of the Regulatory Powers Act:

- the SPF general regulator is an authorised applicant in relation to each civil penalty provision of an SPF principle; and
- the SPF sector regulator for a regulated sector is an authorised applicant in relation to each civil penalty provision of the SPF code for the sector.

[Schedule 1, item 1, subsection 58FJ(2)]

1.451 In relation to a civil penalty provision of an SPF principle or SPF code, the Federal Court, the Federal Circuit and Family Court of Australia (Division 2) and a court of a State or Territory that has jurisdiction in relation to the matter are each a relevant court for the purposes of Part 4 of the Regulatory Powers Act.
[Schedule 1, item 1, subsection 58FJ(3)]

1.452 The amendments establish two tiers of contraventions of the SPF civil penalty provisions. A tier 1 contravention attracts a higher maximum penalty than a tier 2 contravention.

Maximum penalty for tier 1 contraventions

1.453 A tier 1 contravention is a contravention of a civil penalty provision of an SPF principle in Subdivisions C, D, F, or G of Division 2 of Part IVF, being:

- SPF Principle 2: Prevent;
- SPF Principle 3: Detect;
- SPF Principle 5: Disrupt; and

- SPF Principle 6: Respond.

[Schedule 1, item 1, paragraph 58FK(1)(b)]

1.454 The maximum penalty amount for a tier 1 contravention by a body corporate is the greater of the following:

- 159,745 penalty units (which is currently $50,000,185);
- if the relevant court can determine the total value of the benefit that the body corporate and any body corporate related to that body corporate have obtained directly or indirectly and is reasonably attributable to the contravention – three times that total value;
- if the court cannot determine that total value – 30 per cent of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

[Schedule 1, item 1, subsection 58FK(2)]

1.455 The maximum penalty amount for a tier 1 contravention by a person other than a body corporate is 7,990 penalty units (which is currently $2,500,870).
[Schedule 1, item 1, subsection 58FK(3)]

1.456 Despite subsection 82(5) of the Regulatory Powers Act, the pecuniary penalty payable under an SPF civil penalty order and for a tier 1 contravention must not be more than the maximum penalty worked out as outlined above for such a contravention by the person. Subsection 82(5) of that Act would otherwise limit the pecuniary penalty for civil penalty orders.
[Schedule 1, item 1, subsection 58FK(1)]

1.457 The maximum penalty amount of a tier 1 contravention is intended to deter contravention of the provisions and is commensurate to the consequences of contravention of the provision. The penalty also aligns with penalty amounts in other legislative frameworks designed to protect consumers, such as the Australian Consumer Law. Consistent with the Attorney-General's Department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, this penalty is a maximum penalty, and reflects an appropriate deterrence for the worst breach of the SPF provisions, which could contribute to substantial consumer loss.

1.458 High penalties reflect the importance of regulated entities complying with the obligations under the SPF, which is expected to substantially minimise scam losses for SPF consumers. Significant penalties recognise the ongoing damage and loss in the Australian economy, and the role that regulated entities play in preventing and combatting scam activity.

1.459 Further, it is expected that regulated entities will often be large entities that may have little incentive to take steps to combat scams but benefit from the advances in the digital economy that support those scams. Some sectors that are the most significant vectors for scam activity also profit from allowing scammers to use their services. A high maximum penalty is therefore necessary

to achieve an effective and meaningful level of deterrence from breaching the relevant SPF principles.

Maximum penalty for tier 2 contraventions

1.460 A tier 2 contravention is a contravention of a civil penalty provision of:

- an SPF code; or
- an SPF principle in Subdivision B (SPF Principle 1: Governance) or Subdivision E (SPF Principle 4: Report).

[Schedule 1, item 1, subparagraph 58FL(1)(b)(i)]

1.461 The maximum penalty amount for a tier 2 contravention by a body corporate is the greater of the following:

- 31,950 penalty units (which is currently $10,000,350);
- if the relevant court can determine the total value of the benefit that the body corporate and any body corporate related to that body corporate have obtained directly or indirectly and is reasonably attributable to the contravention – three times that total value;
- if the court cannot determine that total value – 10 per cent of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

[Schedule 1, item 1, subsection 58FL(2)]

1.462 The maximum penalty amount for a tier 2 contravention by a person other than a body corporate is 1,600 penalty units (which is currently $500,800).
[Schedule 1 ,item 1, subsection 58FL(3)]

1.463 Despite subsection 82(5) of the Regulatory Powers Act, the pecuniary penalty payable under an SPF civil penalty order and for a tier 2 contravention must not be more than the maximum penalty as outlined above for such a contravention by the person. Subsection 82(5) of that Act would otherwise limit the pecuniary penalty for civil penalty orders.
[Schedule 1, item 1, subsection 58FL(1)]

1.464 The maximum penalty amount of a tier 2 contravention is intended to deter contravention of the relevant provisions and is commensurate to the consequences of contravention of the provision.

1.465 Contraventions of the civil penalty provisions in SPF codes and the SPF principles related to governance and reporting have a lower maximum penalty because these obligations are more systems and process-focused, with more minimal direct consequences for consumers.

Multiple remedies can be sought for a single contravention however civil penalty double jeopardy applies to the same conduct

1.466 A provision of Division 6 does not limit a court's power under any other provision of the CCA or any other Act (for example, under the *Federal Court of Australia Act 1976*). This means that an SPF regulator may seek multiple remedies for a single contravention where appropriate.
[Schedule 1, item 1, section 58FC]

1.467 However, if a person is required under an SPF civil penalty order to pay a pecuniary civil penalty in respect of particular conduct, the person is not liable to a pecuniary penalty for contravening another civil penalty provision of an SPF principle or of an SPF code, or under some other provision of a law of the Commonwealth, in respect of that conduct. In this context, conduct means an act or omission, and is not necessarily tied to a particular scam. This operates to prevent civil penalty double jeopardy.
[Schedule 1, item 1, sections 58FC and 58FM]

1.468 This is intended to avoid the multi-regulator model and tiered structure of the framework leading to an outcome where a regulated entity is penalised twice for the same conduct. However, a court may make other kinds of orders under Division 6 – for example, an order relating to an action for damages – in relation to particular conduct even if the court has made an SPF civil penalty order in relation to that conduct.
[Schedule 1, item 1, note to section 58FM]

Infringement notices

1.469 The infringement notice regime in the SPF is broadly consistent with existing frameworks in the CCA, as well as the Regulatory Powers Act.

1.470 Under this framework, the inspector of the SPF regulator may issue an infringement notice to a person for an alleged contravention of a civil penalty provision of an SPF principle or a civil penalty provision of an SPF code. This power can be used as an alternative to proceedings for an SPF civil penalty order.
[Schedule 1, item 1, subsection 58FN(1)]

1.471 The amendments do not require an SPF regulator to issue an SPF infringement notice for an alleged contravention of a civil penalty provision. Nor does the Subdivision affect a person's liability to proceedings for an SPF civil penalty order in relation to an alleged contravention of a civil penalty provision if an SPF infringement notice is not issued to the person for the contravention or if an SPF infringement notice issued to the person for the contravention is withdrawn or not paid. Further, the amendments do not prevent a court from imposing a higher penalty than specified in the SPF infringement notice if the person does not comply with the notice.
[Schedule 1, item 1, subsection 58FN(2]

1.472 The inspector may issue an SPF infringement notice to a person that the inspector reasonably believes has contravened a civil penalty provision of an SPF principle or a civil penalty provision of the SPF code for a sector. ***[Schedule 1, item 1, subsections 58FO(1) and (2)]***

1.473 Inspectors of an SPF regulator must not issue more than one SPF infringement notice to the person for the same alleged contravention of a civil penalty provision**.** ***[Schedule 1, item 1, subsection 58FO(3)]***

1.474 An infringement notice will not have effect if the notice is issued more than 12 months after the day the relevant contravention is alleged to have occurred or relates to more than one alleged contravention of a civil penalty provision by a person. This supports appropriate regulation of the SPF as it provides the person receiving the infringement notice with clear reasons for the notice. ***[Schedule 1, item, 1, subsection 58FO(4)]***

1.475 An SPF infringement notice must include certain information to ensure traceability and accuracy. This information includes the following:

- a unique number;
- the date on which it was issued;
- the name of the person to which it was issued;
- the name of the inspector issuing the notice with confirmation that the inspector is an inspector of the applicable SPF regulator and how that SPF regulator may be contacted;
- details of the alleged contravention including the day it occurred and the civil penalty provision that was contravened;
- the maximum pecuniary penalty a court could order the person to pay if the court were to make an SPF civil penalty order for the alleged contravention;
- specify the penalty that is payable in relation to the alleged contravention;
- that the penalty is payable within the compliance period;
- that the penalty is payable to the SPF regulator on behalf of the Commonwealth;
- how the payment of the penalty is to be made;
- explain the effects of compliance with the SPF infringement notice, the effects of failure to comply, the compliance period for the infringement notice and withdrawal of the infringement notice.

[Schedule 1, item 1, section 58FP]

1.476 The penalty specified in an SPF infringement notice issued to a person must be a penalty equal to 60 penalty units for a body corporate or 12 penalty units otherwise.
[Schedule 1, item 1, section 58FQ]

1.477 A person will not be regarded as having contravened the civil penalty provision just because they have paid a penalty specified in the notice. This applies if an SPF infringement notice for an alleged contravention of a civil penalty is issued to a person, the person pays the penalty specified in the notice within the infringement notice compliance period and in accordance with the notice and the notice is not withdrawn.
[Schedule 1, item 1, subsections 58FR(1) and (2)]

1.478 No proceedings can be started or continued against the person, by or on behalf of the Commonwealth in relation to the alleged contravention of the civil penalty provision where there has been compliance with the infringement notice.
[Schedule 1, item 1, subsection 58FR(3)]

1.479 However, a person is liable to proceedings for an SPF civil penalty order in relation to the alleged contravention of the civil penalty provision if the SPF infringement notice for an alleged contravention of a civil penalty provision is issued to a person, the person fails to pay the penalty specified in the notice within the infringement notice compliance period, and the notice has not been withdrawn.
[Schedule 1, item 1, section 58FS]

1.480 The infringement notice compliance period for an SPF infringement notice issued to a person is the period of 28 days, beginning on the day after the day that an inspector of an SPF regulator issues the notice.
[Schedule 1, item 1, subsection 58FT(1)]

1.481 The SPF regulator may, by giving written notice to the person, extend the infringement notice compliance period if the SPF regulator is satisfied that it is appropriate to do so. Only one extension may be given, which must not be for longer than 28 days.
[Schedule 1, item 1, subsections 58FT(2) and (3)]

1.482 Failure to give the person notice of an extension to the infringement notice compliance period does not affect the validity of that extension.
[Schedule 1, item 1, subsection 58FT(4)]

1.483 If an infringement notice compliance period for an SPF infringement notice is extended under this section, a reference in this Subdivision to the infringement notice compliance period is taken to be a reference to that period as so extended.
[Schedule 1, item 1, subsection 58FT(5)]

1.484 A person to whom an SPF infringement notice has been issued for an alleged contravention of a civil penalty provisions by an inspector of an SPF regulator

may make representations to the SPF regulator seeking withdrawal of the notice.
[Schedule 1, item 1, subsection 58FU(1)]

1.485 Evidence or information that the person or a representative of the person gives to the SPF regulator in the course of making representations is not admissible in evidence against the person or representative in any proceedings (other than proceedings for an offence based on the evidence or information given being false or misleading).
[Schedule 1, item 1, subsection 58FU(2)]

1.486 An SPF regulator may, by giving written notice to the person, withdraw the infringement notice issued by the inspector if the SPF regulator is satisfied it is appropriate to do so. This withdrawal can be made even if no representations are made by the person seeking withdrawal.
[Schedule 1, item 1, subsections 58FU(3) and (4)]

1.487 The withdrawal notice must state:

- the name and address of the person; and
- the day on which the SPF infringement notice was issued to the person; and
- that the SPF infringement notice is withdrawn; and
- that proceedings for an SPF civil penalty order may be started or continued against the person in relation to the alleged contravention of the civil penalty provision.

[Schedule 1, item 1, subsection 58FU(5)]

1.488 The withdrawal must also be given to the person within the infringement notice compliance period for the SPF infringement notice.
[Schedule 1, item 1, subsection 58FU(6)]

1.489 If an SPF regulator withdraws an SPF infringement notice given to a person after the person has paid the penalty specified in the SPF infringement notice, the SPF regulator must refund to the person an amount equal to the amount paid.
[Schedule 1, item 1, subsection 58FU(7)]

Enforceable undertakings

1.490 Enforceable undertakings are a common feature in regulatory regimes across Australia as they are an effective and efficient way to address non-compliance without court proceedings.

1.491 The ACCC, as the SPF general regulator, may accept a written enforceable undertaking from a person in connection with compliance with an obligation under the SPF principles.
[Schedule 1, item 1, subsection 58FV(1)]

1.492 Similarly, an SPF sector regulator may accept a written enforceable undertaking from a person in connection with compliance with an obligation under an SPF code for the sector.
[Schedule 1, item 1, subsection 58FV(2)]

1.493 An undertaking by a person may be withdrawn or varied at any time with the consent of the SPF regulator who accepted it.
[Schedule 1, item 1, subsection 58FV(3)]

1.494 If an SPF regulator considers that a person who gave them an undertaking has breached any of its terms, the SPF regulator may apply to a court with jurisdiction for an order:

- directing the person to comply with the terms of the undertaking;
- directing the person to pay to the Commonwealth an amount up to the amount of any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach;
- that the court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach, such as a scam victim;
- the court considers appropriate.

[Schedule 1, item 1, subsections 58FV(4) and (5)]

1.495 Where appropriate, an SPF regulator may accept an enforceable undertaking at the same time as taking other regulatory actions.

1.496 For example, an SPF regulator may accept an undertaking from a regulated entity to take steps to comply with their obligation to take reasonable steps to detect scams and also remediate impacted SPF consumers that they have direct customer relationships with who were impacted by an alleged breach of the relevant SPF obligations. In addition, if the regulated entity breached any term contained in an enforceable undertaking accepted by an SPF regulator, a court may order that a regulated entity compensate any person who has suffered loss or damage as a result of the breach.

Injunctions

1.497 An application for an injunction may be made by an SPF regulator or any other person.
[Schedule 1, item 1, subsection 58FZA(1)]

1.498 The intention is that an SPF regulator will apply to a court with jurisdiction for an injunction for a breach of an obligation under the overarching principle. Similarly, it is intended that an SPF sector regulator may apply to a court with jurisdiction for an injunction for a breach of an obligation under a sector-specific code.

1.499 A court may grant that injunction in such terms as it considers appropriate if it is satisfied that the person has engaged, or is proposing to engage, in conduct that constitutes or would constitute:

- a contravention of a civil penalty provision of the SPF principles or a civil penalty provision of an SPF code; or
- attempting to contravene such a provision; or
- aiding, abetting, counselling or procuring a person to contravene such a provision; or
- inducing, or attempting to induce, whether by threats, promises or otherwise, a person to contravene such a provision; or
- being in any way, directly or indirectly, knowingly concerned in, or party to, the contravention by a person of such a provision; or
- conspiring with others to contravene such a provision.

[Schedule 1, item 1, subsection 58FW]

1.500 A court may grant an injunction restraining a person from engaging in conduct:

- whether or not it appears to the court that the person intends to engage again, or to continue to engage, in conduct of that kind;
- whether or not the person has previously engaged in conduct of that kind; and
- whether or not there is an imminent danger of substantial damage to any person if the first mentioned person engages in conduct of that kind.

[Schedule 1, item 1, subsection 58FX(1)]

1.501 A court may grant an injunction requiring a person to do an act or thing:

- whether or not it appears to the court that the person intends to refuse or fail again, or to continue to refuse or fail, to do that act or thing;
- whether or not the person has previously refused or failed to do that act or thing; and
- whether or not there is an imminent danger of substantial damage to any person if the first mentioned person refuses or fails to do that act or thing.

[Schedule 1, item 1, subsection 58FX(2)]

1.502 A court may grant an injunction by consent of all the parties to the proceedings, whether or not the court is satisfied that a person has engaged or is proposing to engage in conduct described at section 58FW (see above).
[Schedule 1, item 1, subsection 58FX(3)]

1.503 A court may grant an interim injunction pending determination of an application for an injunction.
[Schedule 1, item 1, section 58FY]

1.504 A court may rescind or vary an injunction granted in relation to the SPF.
[Schedule 1, item 1, section 58FZ]

1.505 If an SPF regulator applies for an injunction, the court must not require the application or any other person, as a condition of granting an interim injunction, to give an undertaking as to damages.
[Schedule 1, item 1, subsection 58FZA(2)]

1.506 If a person other than an SPF regulator applies for an injunction and would normally be required to give an undertaking as to damages or costs, and an SPF regulator gives the undertaking, the court must accept the undertaking by the SPF regulator and must not require a further undertaking from any other person.
[Schedule 1, item 1, subsection 58FZA(3)]

1.507 The powers given to a court to grant an injunction by Subdivision F of Division 6 do not affect any powers of the court, whether conferred by the CCA or otherwise.
[Schedule 1, item 1, section 58FZB]

Accessing compensation through an action for damages

General rule

1.508 A person who suffers loss or damage by conduct of another person that was done in contravention of a civil penalty provision of an SPF principle or SPF code may recover the amount of the loss or damage by taking action against that other person. Additional rules apply where there are concurrent wrongdoers.
[Schedule 1, item 1, subsections 58FZC(1) and (4)]

1.509 An SPF regulator may also make a claim on behalf of the victim where there is written consent by the victim. This may occur alongside proceedings initiated by the SPF regulator against a regulated entity for an alleged contravention of a provision of an SPF principle or SPF code, to streamline the process for compensating victims.
[Schedule 1, item 1, subsection 58FZC(2)]

1.510 A claim for loss or damages may be made at any time within six years after the day the cause of action that relates to the conduct accrued. This is consistent with the general principles relating to the statute of limitations.
[Schedule 1, item 1, subsection 58FZC(3)]

1.511 For example, if an SPF consumer is not satisfied with the outcomes of an IDR and/or EDR process, they may pursue action and initiate proceedings in court

to recover an amount of loss or damage suffered as a result of an alleged breach by one or more regulated entities subject to the SPF provisions. A court may find that a regulated entity breached its obligation to take reasonable steps to prevent a scam which led to the SPF consumer suffering financial loss and may make an order in favour of the consumer for an appropriate amount of compensation.

1.512 To avoid doubt, a claim for loss and damages under the SPF cannot be made against an unregulated entity, as these entities do not have obligations under the SPF.

Proportionate liability for concurrent wrongdoers

1.513 Where there are multiple regulated entities involved in a claim brought by a victim for loss or damages, the SPF enables the court to consider the proportionate liability of these entities. These provisions are modelled on the existing proportionate liability provisions that apply to claims for damages relating to misleading and deceptive conduct in the CCA, ASIC Act and Corporations Act.

Meaning of concurrent wrongdoer

1.514 In any claim for loss or damages under the SPF, a concurrent wrongdoer is a person who is one of two or more persons:

- who each contravened a civil penalty provision of an SPF principle or an SPF code (whether or not the same civil penalty provision); and
- whose contraventions caused the loss or damage that is the subject of the claim.

[Schedule 1, item 1, subsection 58FZD(1)]

1.515 As only regulated entities may contravene a civil penalty provision of an SPF principle or an SPF code, only regulated entities may be a concurrent wrongdoer. A concurrent wrongdoer could therefore be a regulated entity who contravened the obligation to take reasonable steps to prevent a scam, and a second regulated entity who contravened the obligation to take reasonable steps within a reasonable time to disrupt the scam, where the contraventions together caused the loss or damage that is the subject of the claim.

1.516 A person may be a concurrent wrongdoer even if the person is insolvent, being wound up or has ceased to exist or died.
[Schedule 1, item 1, subsection 58FZD(2)]

Notifying plaintiff of concurrent wrongdoers

1.517 A defendant in proceedings involving a claim under the general rule that has reasonable grounds to believe that a particular person may be a concurrent wrongdoer in relation to the claim must give the plaintiff, as soon as practicable, written notice of the information the defendant has about the

identity of that person and the circumstances that may make that person a concurrent wrongdoer.
[Schedule 1, item 1, paragraphs 58FZG(1)(a) and (b)]

1.518 The court may order that the defendant pay all or any of the costs unnecessarily incurred by the plaintiff in the proceedings because the plaintiff was not aware that the other person may be a concurrent wrongdoer. The costs may be assessed on an indemnity basis or otherwise.
[Schedule 1, item 1, paragraph 58FZD(1)(c) and subsection 58FZG(2)]

1.519 A reference to a 'defendant' includes any person joined as a defendant or other party in the proceedings (except as a plaintiff), no matter how joined.
[Schedule 1, item 1, subsection 58FZF(5)]

Claims involving concurrent wrongdoers

1.520 In any claim to recover an amount of loss or damage under the general rule, the liability of a defendant who is a concurrent wrongdoer in relation to the claim is limited to an amount reflecting that proportion of the loss or damage that the court considers just having regard to the extent of the defendant's responsibility for the loss or damage. The court may give judgment against the defendant for not more than that amount.
[Schedule 1, item 1, subsection 58FZF(1)]

1.521 If the proceedings involve another claim that is not a claim under the general rule, liability for the other claim is to be determined in accordance with any relevant legal rules.
[Schedule 1, item 1, subsection 58FZF(2)]

1.522 This may occur where there are other causes of action available to the claimant in relation to the same loss or damage, such as breach of contract or negligence.

1.523 In apportioning responsibility between defendants in the proceedings, the court must exclude that proportion of the loss or damage to which the plaintiff is contributorily negligent under any relevant law. The court may also have regard to the comparative responsibility of any concurrent wrongdoer who is not a party to the proceedings. This applies whether or not all concurrent wrongdoers are parties to the proceedings.
[Schedule 1, item 1, subsections 58FZF(3) and (4)]

1.524 The court may give leave for any one or more concurrent wrongdoers to be joined as defendants in proceedings involving a claim under the general rule, except for any person who was party to any previously concluded proceedings in respect of the claim.
[Schedule 1, item 1, subsections 58FZJ(1) and (2)]

1.525 The plaintiff referred to in subsections 58FZC(1) and (2) is the victim or an SPF regulator.
[Schedule 1, item 1, note to subsection 58FZG]

1.526 A defendant against whom judgment is given as a concurrent wrongdoer cannot be required to contribute any damages or contribution recovered from another concurrent wrongdoer in respect of the claim (whether or not recovered in the same proceedings in which judgment is given against the deferent) nor to indemnify any such wrongdoer.
[Schedule 1, item 1, section 58FZH]

Certain concurrent wrongdoers not to have benefit of apportionment

1.527 The liability of a concurrent wrongdoer in proceedings involving a claim under the general rule to recover an amount of loss or damage is not excluded if the concurrent wrongdoer intended to cause the loss or damage, or the concurrent wrongdoer fraudulently caused the loss or damages. The liability of such a concurrent wrongdoer is to be determined in accordance with any relevant legal rules (apart from the proportionate liability framework in this Subdivision). Consequently, these concurrent wrongdoers do not have the benefit of apportionment under the proportionate liability framework in this Division.
[Schedule 1, item 1, subsections 58FZE(1) and (2)]

1.528 The liability of any other concurrent wrongdoer is to be determined in accordance with the proportionate liability framework in this Division.
[Schedule 1, item 1, subsection 58FZE(3)]

Subsequent actions by plaintiff

1.529 A plaintiff (or a victim) who has previous recovered judgment against a concurrent wrongdoer for an apportionable part of any loss or damage is not precluded from bringing another action against any other concurrent wrongdoer for that loss or damage.
[Schedule 1, item 1, subsection 58FZI(1)]

1.530 However, an amount of damages cannot be recovered by or for the victim that, having regard to damages previously recovered for the loss or damage, would result in the victim receiving compensation for the loss or damage that is greater than the loss or damage actually sustained by the victim.
[Schedule 1, item 1, subsection 58FZI(2)]

Application of proportionate liability framework

1.531 The proportionate liability framework in this Division does not prevent a person being held vicariously liable for a proportion of a claim under the general rule for which another person is liable. Nor does it prevent a person being held being severally liable with another person for the proportion of a claim for which the other person is liable. Further, it does not affect the operation of any other provision of the CCA or any other Act to the extent that the provision imposes several liability on any person in respect of what would otherwise be a claim under the general rule.
[Schedule 1, item 1, section 58FZK]

Preference to be given to victim compensation

1.532 There may be some circumstances where a court considers it is appropriate to order a person to pay both a pecuniary penalty under an SPF civil penalty order in relation to a contravention or conduct and compensation to a person who has suffered loss or damage as a result of that contravention or conduct.

1.533 Where this occurs, the court must give preference to making an order for compensation if the defendant does not have sufficient financial resources to pay both.
[Schedule 1, item 1, section 58FD]

1.534 This approach is consistent with the object of the SPF to prevent and respond to scams impacting SPF consumers.

Public warning notices

1.535 The SPF general regulator may issue to the public a written notice containing a warning about the conduct of a person if the SPF general regulator:

- reasonably suspects that the person's conduct may constitute a contravention of a specified provision of the SPF principles; and
- is satisfied that one or more persons has suffered, or is likely to suffer, detriment as a result of the conduct; and
- is satisfied that it is in the public interest to issue the notice.

[Schedule 1, item 1, subsection 58FZL(1)]

1.536 An SPF sector regulator may issue an equivalent notice, under the same conditions stated above, in relation to conduct related to a sector code for which they are an SPF sector regulator.
[Schedule 1, item 1, subsection 58FZL(2)]

1.537 An SPF regulator that issues a public warning notice as outlined above must publish the notice on the SPF regulator's website. The notice is not a legislative instrument. This notice is merely declaratory, and is covered by item 19 of the table in section 6 of the *Legislation (Exemptions and Other Matters) Regulations 2015*.
[Schedule 1, item 1, subsection 58FZA(3), subsection 58FZL(4)]

1.538 Public warning notices allow SPF regulators to inform the public about a person engaged in business practices that may amount to a contravention of the SPF. Such notices are intended to stop or reduce the detriment caused by regulated entities engaging in conduct that may be in breach of the SPF. They provide SPF regulators with an enforcement tool that can be used in a preventative manner to avoid consumers being adversely affected by conduct that may breach the SPF.

Remedial directions

1.539 If the SPF general regulator reasonably suspects that a regulated entity is failing, or will fail, to comply with an SPF principle, it may, by written notice given to the entity, direct the entity to take specified action to comply with that SPF principle.
[Schedule 1, item 1, subsection 58FZM(1)]

1.540 If an SPF sector regulator reasonably suspects that a regulated entity for the regulated sector is failing, or will fail, to comply with a provision of the SPF code it is the SPF sector regulator for, the regulator may, by written notice given to the entity, direct the entity to take specified action to comply with that provision of the SPF code. The direction may relate to one or more failures.
[Schedule 1, item 1, subsection 58FZM(2)]

1.541 For example, an SPF regulator may direct a regulated entity that is a digital platform that it considers has breached its obligation to take reasonable steps detect and disrupt scams under the SPF principles to take down a scam advertisement on its platform or service in order to comply with its obligations in the SPF provisions.

1.542 An SPF regulator may also issue a remedial direction to a regulated entity to comply with its obligation to give reasonable assistance or cooperate with the operator of the SPF EDR scheme if it believes that it is failing to comply with this obligation.

1.543 A regulated entity must take action to comply with the direction in the time specified in the direction. This time must be reasonable. If the direction does not specify a reasonable time, the entity must take action to comply with the direction within a reasonable time. The SPF regulator may also extend the time for complying with the direction by written notice given to the entity.
[Schedule 1, item 1, subsections 58FZM(3) and (5)]

1.544 Failure to comply with these directions is subject to civil penalties. (See the definitions of 'civil penalty provision of an SPF principle', and 'civil penalty provision of an SPF code' in subsection 4(1) of the CCA).
[Schedule 1, item 1, subsection 58FZM(4)]

1.545 It is appropriate for an SPF regulator to specify a time for the regulated entity to take action with reference to the potential severity of negative impact on SPF consumers of a regulated entity failing to act quickly when engaging in conduct that may breach the SPF.

1.546 Prior to giving a regulated entity a direction, an SPF regulator must give the entity an opportunity to make submissions to the SPF regulator on the matter.
[Schedule 1, item 1, subsection 58FZM(6)]

1.547 An SPF regulator may vary or revoke a direction in like manner and subject to like conditions (see subsection 33(3) of the *Acts Interpretation Act 1901*).
[Schedule 1, item 1, subsection 58FZM(7)]

1.548 An SPF regulator must, as soon as practicable after a direction is given, varied or revoked, publish a notice of its action on its website.
[Schedule 1, item 1, subsection 58FZM(8)]

Adverse publicity orders

1.549 A court with jurisdiction may, on application by an SPF regulator, make an adverse publicity order against a person who has been ordered to pay a pecuniary penalty under an SPF civil penalty order.
[Schedule 1, item 1, subsection 58FZN(1)]

1.550 Such an order may require the person to:

- disclose, in the way and to the persons specified in the order, specified information that the person has possession of or access to; and
- publish, at the person's expense and in a specified way, an advertisement in the terms specified in, or determined in accordance with, the order.

[Schedule 1, item 1, subsection 58FZN(2)]

1.551 An application for such an order may only be made by the SPF general regulator if the SPF civil penalty order was for a contravention of a civil penalty provision of an SPF principle.
[Schedule 1, item 1, paragraph 58FZN(3)(a)]

1.552 An application for such an order may only be made by an SPF sector regulator if the SPF civil penalty order was for a contravention of a civil penalty provision of an SPF code for the relevant regulated sector.
[Schedule 1, item 1, paragraph 58FZN(3)(b)]

Non punitive orders

1.553 A court with jurisdiction may on application, make one or more of the following orders in relation to a person who has engaged in conduct contravening an SPF principle or a provision of an SPF code:

- a community service order;
- a probation order for a period of no longer than 3 years;
- an order requiring the person to disclose, in the way and to the persons specified in the order, specified information that the person has possession of or access to;
- an order requiring the person to publish, at the person's expense and in a specified way, an advertisement in the terms specified in, or determined in accordance with, the order.

[Schedule 1, item 1, subsection 58FZO(1)]

1.554 An application for such an order may only be made by the SPF general regulator in relation to conduct contravening an SPF principle.
[Schedule 1, item 1, paragraph 58FZO(2)(a)]

1.555 An application for such an order may only be made by an SPF sector regulator in relation to conduct contravening an SPF code.
[Schedule 1, item 1, paragraph 58FZO(2)(b)]

1.556 The following definitions are applied for the purpose of non-punitive orders of the SPF.

1.557 A 'probation order' is an order made to ensure that a person does not engage in the conduct that resulted in the order, or similar conduct or related conduct during the period of the order. It includes an order directing a person to establish a compliance program, or an education and training program that is for employees or other persons involved in the person's business, and is designed to ensure awareness of responsibility and obligation relating to conduct covered by the probation order. It also includes an order directing a person to revise the internal operations of the person's business that lead to conduct covered by paragraph (3)(a) or (b).
[Schedule 1, item 1, subsections 58FZO(3) and (4)]

1.558 'Community service orders' means an order directing a person perform a service that is specified in the order or relates to the conduct that resulted in the order for the benefit of the community or a section of the community.
[Schedule 1, item 1, subsection 58FZO(5)]

1.559 Conduct 'contravening' an SPF principle or a provision of an SPF code includes conduct that constitutes being involved in such a contravention. For the meaning of 'involved', see subsection 4(1) of the CCA.
[Schedule 1, item 1, subsection 58FZO(5)]

Orders (other than damages) to redress loss or damage

1.560 A court with jurisdiction may, on application, make such orders as the court thinks appropriate against a person who engaged in conduct contravening a civil penalty provision of an SPF principle or a civil penalty provision of an SPF code or is involved in that contravening conduct if that conduct caused, or is likely to cause, a class of persons (the victims) to suffer loss or damage. This power does not include an order to make an award of damages. The amendments set out the orders that the court may make.
[Schedule 1, item 1, subsection 58FZP(1)]

1.561 This power applies even if the victims have not been a party to an enforcement proceeding relating to the contravening conduct.
[Schedule 1, item 1, subsection 58FZP(2)]

1.562 When making such orders as the court thinks appropriate, the court must not make such an order unless it consider that the order will:

- redress, in whole or in part, the loss or damage suffered by the victims in relation to the contravening conduct; or
- prevent or reduce the loss or damage suffered, or likely to be suffered, by the victims in relation to the contravening conduct.

[Schedule 1, item 1, subsection 58FZP(3)]

1.563 An application for such an order may only be made by the SPF general regulator in relation to conduct contravening an SPF principle, or by an SPF sector regulator in relation to conduct contravening an SPF code. The application may be made even if an enforcement proceeding in relation to the contravening conduct has not been instituted but must be made any time within 6 years after the day on which the cause of action that relates to the contravening conduct accrues.
[Schedule 1, item 1, subsection 58FZP(4)]

1.564 In working out whether to make such orders against the person, the court may have regard to the conduct of the person and the victims in relation to the contravening conduct since the contravention occurred. This may include for example, any efforts made by the person to remediate the victims. However, the court does not need to make a finding about which persons are victims in relation the contravening conduct or the nature of the loss or damage suffered, or likely to be suffered by such persons.
[Schedule 1, item 1, subsections 58FZP(5) and (6)]

1.565 If the court makes such an order against a person, and the loss or damage suffered, or likely to be suffered, by a victim that is not a party to the proceeding (non-party victim) in relation to the contravening conduct has been redressed, prevented or reduced in accordance with the order and that has been accepted by the non-party victim, then:

- the non-party victim is bound by the order; and
- any other order made by the court as it considered appropriate, in relation to that loss or damage, has no effect in relation to the non-party victim; and
- despite any other provision of the CCA or any other law of the Commonwealth, or a State or Territory, no claim, action or demand may be made or taken against the person by the non-party victim in relation to that loss or damage.

[Schedule 1, item 1, subsection 58FZP(7)]

1.566 The kinds of orders that a court may make against a person include all or any of the following (but are not limited to the following):

- an order declaring the whole or any part of a contract made between the person and a victim (including a non-party victim), or a collateral arrangement relating to such a contract to be void, including to have

been void ab initio or void at all times on and after such date as is specified in the order. This may be a date before the date on which the order is made;

- an order varying a contract or arrangement in such manner as is specified in the order, and if the court thinks fit—declaring the contract or arrangement to have had effect as varied on and after a date specified in the order. This may be a date before the date on which the order is made;
- an order refusing to enforce any or all of the provisions of a contract or arrangement;
- an order directing the respondent to refund money or return property to a victim (including a non-party victim);
- an order directing a respondent, at the respondent's own expense, to repair, or provide parts for, goods that have been supplied under the contract or arrangement to a victim (including a non-party victim);
- an order directing the respondent, at the respondent's own expense, to supply specified services to a victim (including a non-party victim);
- an order, in relation to an instrument creating or transferring an interest in land, directing a person to execute an instrument that varies or terminates or otherwise affects the relevant instrument, or that has the effect of varying, terminating or otherwise affecting, the operation or effect of the relevant instrument.

[Schedule 1, item 1, subsection 58FZQ(1)]

1.567 An interest in land means:

- a legal or equitable estate or interest in the land; or
- a right of occupancy of the land, or of a building or part of a building erected on the land, arising by virtue of the holding of shares, or by virtue of a contract to purchase shares, in an incorporated company that owns the land or building; or
- a right, power or privilege over, or in connection with, the land.

[Schedule 1, item 1, subsection 58FZQ(2)]

1.568 These powers are mirrored, in part, on existing provisions in the CCA (for example in Part IVB). They are intended to give scope for a court with jurisdiction to make an order compensating a victim (which can also include a non-party victim that was not, for example, an SPF consumer in relation to some other proceeding under Part IVF) for loss or harm suffered as a result of contravening conduct. This ensures there is some form of remedial power in relation to persons who may not have recourse available to them through, for example, the EDR mechanisms in the SPF.

1.569 There may be circumstances when an SPF regulator initiates proceedings against a regulated entity, and the court considers it appropriate, in making certain orders against the regulated entity, to also make orders in favour of a non-party victim (who may or may not be an SPF consumer). This allows for the remediation of loss or damage to be streamlined and save victims the time and cost of pursuing a matter in court or through a dispute resolution process. For example, if a court finds in a proceeding between an SPF regulator and a regulated entity that the entity's contravening conduct resulted in a non-party victim suffering financial loss, the court may consider it appropriate to order the regulated entity to provide a remedy.
[Schedule 1, item 1, subsection 58FZC(2)]

Division 7 – Other provisions

1.570 The amendments include a number of mechanical provisions that ensure a consistent treatment for the purposes of the SPF obligations across different types of entities. These specific provisions provide for the application of the SPF obligations to an entity that is a partnership, unincorporated association, or a trust. This ensures the scope of the SPF is not unnecessarily limited by the structure of a relevant entity.
[Schedule 1, item 1, sections 58GA, 58GB and 58GC]

1.571 The SPF provisions apply to a partnership as if it were a person but with the following changes:

- An obligation that would otherwise be imposed on the partnership by an SPF provision is imposed on each partner and may be discharged by any of the partners.
- Permitted activities may be done by one or more of the partners on behalf of the partnership.
- Despite each partner being accountable to obligations and being permitted to act on behalf of the entity, a change in the composition of a partnership does not affect the continuity of the partnership. This ensures minimum disruption is involved in applying the SPF to a partnership.

[Schedule 1, item 1, section 58GA]

1.572 The SPF provisions apply to unincorporated associations as if they are persons but in a way that reflects their status as unincorporated associations.

- An obligation otherwise imposed on the association by an SPF provision is imposed on each member of the association's committee of management instead but may be discharged by any of the members.
- If an SPF provision would otherwise permit something to be done by the unincorporated association, the thing may be done by one or more

of the members of the association's committee of management on behalf of the association.

[Schedule 1, item 1, section 58GB]

1.573 The SPF provisions apply to a trust as if it were a person with applicable changes.

- If the trust has a single trustee, an obligation otherwise imposed on the trust by an SPF provision is imposed on the trustee, and if an SPF provision would otherwise permit something to be done by the trust, the thing may be done by the trustee.
- If the trust has more than one trustee, an obligation otherwise imposed on the trust by an SPF provision is imposed on each trustee instead, but may be discharged by any of the trustees, and if an SPF provision would otherwise permit something to be done by the trust, the thing may be done by any of the trustees.

[Schedule 1, item 1, subsection 58GC(1) to (3)]

1.574 Where the operation of the SPF results in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution), a person who acquires the property from a person otherwise than on just terms is liable to pay the first person compensation. If there is a dispute as to the compensation, the person to whom compensation is payable may institute proceedings for the recovery of the reasonable amount of compensation from the other person, as determined in the Federal Court or the Supreme Court of a State or Territory.
[Schedule 1, item 1, section 58GD]

The SPF rules

1.575 A Treasury Minister may make SPF rules by legislative instrument. To avoid doubt, the SPF rules may not create an offence or civil penalty, provide powers of arrest or detention or entry, search or seizure, impose a tax, set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in the CCA or directly amend the text of the CCA.
[Schedule 1, item 1, subsections 58GE(1) and (3)]

1.576 The SPF rules are subject to sunsetting and Parliamentary scrutiny through the disallowance process.

1.577 Consistent with section 17 the *Legislation Act 2003*, prior to making the SPF rules, the Minister must be satisfied that there has been appropriate and reasonably practicable consultation. This will include appropriate consultation on aspects of the obligation on regulated entities to share information under SPF Principle 4: Report, including in relation to the kinds of information, timing, manner and form of the report that regulated entities are required to give to SPF regulators.

1.578 The Minister may, in writing, delegate the Minister's power to make SPF rules to another Minister or to an SPF regulator. This would be appropriate where the Minister considers that another Minister or another regulator has the necessary industry knowledge, understanding and information to best address scams in that sector and to make an appropriate SPF rules.
[Schedule 1, item 1, subsection 58GE(2)]

1.579 For example, the Minister may consider it appropriate for the SPF general regulator to make rules relating to reporting arrangements, noting the SPF general regulator will be required manage any information it receives under the SPF.

Statutory review of the SPF

1.580 To evaluate the effectiveness of the SPF, a Treasury Minister must cause a review of the SPF provisions to be conducted as soon as practicable after the end of the three-year period starting on the day the first SPF code is made under section 58CB.
[Schedule 1, item 1, subsections 58GF(1) and (2)]

1.581 This review will examine the operation of the SPF provisions, which include:

- provisions in Part IVF;
- provisions of a legislative instrument made under Part IVF, including the SPF codes and SPF rules;
- another provision of the CCA that relates to a provision in Part IVF or in a legislative instrument made under Part IVF; and
- provisions of the Regulatory Powers Act to the extent it applies in relation to a provision in Part IVF.

1.582 The person who conducts the review must give a written report to the Minister, which must be tabled in each House of Parliament within 15 sitting days after the Minister receives the report.
[Schedule 1, item 1, subsection 58GF(3) and (4)]

Consequential amendments

1.583 Part 2 of Schedule 1 makes consequential amendments to various Acts to accommodate the SPF and related changes.

1.584 The intention is that if the telecommunications sector is designated to be a regulated sector, then ACMA would be the SPF sector regulator for that sector. Accordingly, the ACMA Act is amended to ensure the functions and powers that are conferred on ACMA under the SPF provisions are part of ACMA's

telecommunications functions.
***[Schedule 1, item 2, subparagraph 8(1)(j)(vii) of the ACMA Act)*]**

1.585 To facilitate the multi-regulator model and allow for effective information sharing between regulators, a new section is inserted into the ACMA Act to allow an authorised ACMA official to make authorised disclosures to an SPF regulator or an operator of an SPF EDR scheme for the purpose of the operation of the SPF provisions. The primary law amendments provide for a framework of regulated sectors and their sector regulator. It is the intention that ACMA would be designated as the sector regulator for the telecommunications sector when that sector is designated as a regulated sector.
[Schedule 1, item 3, section 59DB of the ACMA Act]

1.586 The intention is that if the banking sector is designated to be a regulated sector, then ASIC would be the SPF sector regulator for that sector. Accordingly, the ASIC Act is amended to reflect that ASIC will have the functions and powers that are conferred on it under the SPF provisions.
[Schedule 1, item 4, subsection 12A(1) of the ASIC Act]

1.587 The amendments also introduce a number of definitions into subsection 4(1) of the CCA:

- 'ACMA' meanings the Australian Communications and Media Authority.
- 'actionable scam intelligence' has the same meaning given by section 58AI.
- 'associate' of an SPF consumer means an associate within the meaning of section 318 of the ITAA 1936 of an SPF consumer, who is a person who carries on a business having a principal place of business in Australia or is a natural person who:
  - is in Australia; or
  - is ordinarily resident in Australia.
- 'civil penalty provision of an SPF code' refers to the provisions that create civil penalties in the SPF under an SPF code.
- 'civil penalty provision of an SPF principle' refers to the provisions that create civil penalties in the SPF under an SPF principle.
- 'de-identified' information is information which is no longer about an identifiable individual or an individual who is reasonably identifiable.
- 'infringement notice compliance period' refers to this period under section 58FT.
- 'inspector' of an SPF regulator, has the meaning given by section 58FB.

- 'involved' in a contravention of a civil penalty provision (whether of an SPF code or SPF principle) means:
  - aiding, abetting, counselling or procuring a contravention of the provision;
  - inducing, whether by threats or promises or otherwise, such a contravention;
  - being in any way, directly or indirectly, knowingly concerned in, or party to, such a contravention; or
  - conspiring with others to effect such a contravention.
- 'reasonable steps' for the purposes of the SPF principles has a meaning which is affected by section 58BB.
- 'regulated entity' refers to an entity to which the SPF applies. These entities (unless excluded) carry out a business or provide a service under a regulated sector. See section 58AD.
- 'regulated sector' refers to a sector that has been designated for the SPF to apply. This designation is made by legislative instrument. See subsection 58AC(1).
- 'regulated service' has the meaning given by section 58AD.
- 'scam' has the meaning given by section 58AG.
- 'SPF civil penalty order' means a civil penalty under Part 4 of the Regulatory Powers Act (as that Part applies because of section 58FJ).
- 'SPF code' refers to sector-specific codes that apply to regulated entities of a regulated sector. SPF codes are legislative instruments. See section 58CB.
- 'SPF consumer' has the meaning given by section 58AH. They are generally those who may be provided the regulated services of a regulated entity, and thus, be exposed to scams in that sector. An SPF consumer must also be a natural person, or small business in Australia.
- 'SPF EDR scheme' for a regulated sector means an EDR scheme authorised under subsection 58DB(1) for that sector.
- 'SPF general regulator' has the meaning given by section 58EB. By default the ACCC is the SPF general regulator with oversight of the SPF.
- 'SPF governance policies, procedures, metrics and targets' refer to a regulated entity's policies and procedures required under paragraph 58BD(1)(a) for the regulated sector and the performance metrics and targets required under paragraph 58BD(1)(c) for those policies and procedures.

- 'SPF infringement notice' means an infringement notice issued under subsection 58FO(1) or (2).
- 'SPF personal information' means personal information, or information relating to a person, that may be used alone or in conjunction with other information to access a service or an account, or funds, credit, or other financial benefits.
- 'SPF principles' means the provisions in Subdivisions B to G of Division 2 of Part IVF. These refer to the overarching principles under the SPF of governance, prevent, detect, report, disrupt, and respond.
- 'SPF provisions' means a provision of Part IVF, a provision of a legislative instrument made under that Part (such as any SPF codes), another provision of the CCA that relates to a provision of Part IVF or a legislative instrument made under that Part and a provision of the Regulatory Powers Act to the extent that it applies in relation to a provision of Part IVF or a legislative instrument made under that Part. See section 58AJ.
- 'SPF regulator' means either the SPF general regulator (by default, the ACCC) or the SPF sector regulator for a regulated sector.
- 'SPF rules' means the rules made under section 58GE. The SPF rules are a legislative instrument.
- 'SPF sector regulator' refers to the sector regulator that has been designated for a regulated sector. See section 58ED. It is intended that for the banking and telecommunications sectors (once designated as regulated sectors):
  - ASIC would be the SPF sector regulator for the banking sector; and
  - ACMA would be the SPF sector regulator for the telecommunications sector.
- 'senior officer' of a regulated entity means an officer or a senior manager of the entity, within the meaning of the Corporations Act.

[Schedule 1, item 5, subsection 4(1)]

1.588 Consequential amendments are made to repeal definitions of 'ACMA' in the CCA because ACMA is now defined in subsection 4(1) of the CCA (the interpretation provision). Accordingly, a reference to 'Australian Communications and Media Authority' in section 155AAA of the CCA has also been updated to 'ACMA'.
[Schedule 1, items 6, 7, 8 and 12, sections 52A, 151AB and 152AC and paragraph 155AAA(12)(b))

1.589 Consequential amendments are made to section 155 of the CCA, which relates to the ACCC's information gathering powers, to ensure these powers can be

used for the purposes and operation of the SPF.
[Schedule 1, items 9, 10 and 11, subsection 155(9AC)]

1.590 The amendments provide for the ACCC as SPF regulator to exercise its existing powers under section 155 of the CCA in relation to obtaining information, documents and evidence, for the purposes of the SPF.

1.591 Specifically, the ACCC as an SPF regulator may exercise its powers under section 155 to the extent a matter constitutes, or may constitute, a contravention of an SPF code or is relevant to a 'designated scams prevention framework matter', as defined by subsection 155(9AC.
[Schedule 1, items 9 and 10, subparagraph 155(2)(b)(i) and paragraph 155(2)(a)]

1.592 A 'designated scams prevention framework matter' in section 155 is a reference to the performance of a function, or the exercise of power, conferred on the ACCC, as the SPF general regulator, by or under Part IVF (being the SPF), a legislative instrument made under that Part or the Regulatory Powers Act to the extent that it applies in relation to a provision of that Part.
[Schedule 1, item 11, subsection 155(9AC)]

1.593 Consequential amendments are made to subsection 1051(2) of the Corporations Act to insert a legislative note which clarifies that a law, instrument or condition requiring entities to be members of the scheme need not be a law, instrument or condition regulating providers of financial products or services. The constitutional basis for that law, instrument or condition would need to support the contention that those entities are required to be members of the scheme.
[Schedule 1, item 13, section 1051 of the Corporations Act]

1.594 Consequential amendments are made to section 1052A of the Corporations Act to insert a legislative note which clarifies that ASIC's power to issue regulatory requirements extends to any application of the AFCA scheme in relation to members of the scheme who are not providers of financial products or services.
[Schedule 1, item 14, section 1052A of the Corporations Act]

1.595 Consequential amendments are made to subsection 1052B(1) to omit "Note" and substitute "Note 1".
[Schedule 1, item 15, section 1052B of the Corporations Act]

1.596 Consequential amendments are made to subsection 1052B(1) to insert a legislative note which clarifies that ASIC's power to give directions extends to any application of the AFCA scheme relating to members of the scheme that are not providers of financial products or services.
[Schedule 1, item 16, section 1052B of the Corporations Act].

1.597 Consequential amendments are made to subsections 1052BA(1) and 1052C(1) to insert a legislative note which clarifies that ASIC's power to give directions extends to any application of the AFCA scheme relating to members of the scheme that are not providers of financial products or services.

[Schedule 1, item 17, section 1052BA and section 1052C of the Corporations Act]

1.598 Consequential amendments are made to subsection 1052D(1) to omit "Note" and substitute "Note 1".
[Schedule 1, item 18, section 1052D of the Corporations Act]

1.599 Consequential amendments are made to subsection 1052D(1) to insert a legislative note which clarifies that AFCA's right to make a request extends to any application of the AFCA scheme relating to members of the scheme that are not providers of financial products or services. ASIC's power under subsection 1052D(2) to approve a material change requested by AFCA is consequentially extended, to reflect the expanded scope of the request able to be made by AFCA.
[Schedule 1, item 19, section 1052D of the Corporations Act]

1.600 Consequential amendments are made to subsection 1052E(1) to insert a legislative note which clarifies that the referral obligation extends to any application of the AFCA scheme in relation to members that are not providers of financial products or services.
[Schedule 1, item 20, section 1052E of the Corporations Act]

Commencement, application, and transitional provisions

1.601 The Bill commences the day after Royal Assent.

1.602 The amendments apply from commencement.

Chapter 2: Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011.

Scams Prevention Framework Bill 2024

Overview

2.1 The Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Scams Prevention Framework

2.2 Article 17 of the ICCPR provides:

- *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
- *2. Everyone has the right to the protection of the law against such interference or attacks*.

2.3 Article 17 may be subject to permissible limitations where those limitations are provided by law and non-arbitrary. In order for limitations not to be arbitrary, they must be aimed at a legitimate objective and be reasonable, necessary and proportionate to that objective.

2.4 The object of the Bill is to prevent and respond to scams impacting the Australian community. It does so by establishing a whole-of-economy SPF that requires regulated entities to develop and implement processes, procedures and systems to take action to prevent and combat scams. The SPF provides for regulators to enforce these requirements.

2.5 In this regard, the Bill engages the right to protection against unlawful and arbitrary interference with privacy by promoting that right, as it is likely to have a positive and beneficial impact on the privacy of consumers.

2.6 Regulated entities under the Bill provide a business or service that is part of the regulated sector and may include the following types of entities.

- Individuals, bodies politic and bodies corporate (as set out in section 2C of the *Acts Interpretation Act 1901*).
- Partnerships, unincorporated associations and trusts (under Division 7 of the Bill).
- Corporations (as defined in section 4 of the CCA).
- A person who carries on or provides any one of the following businesses or services to the extent that a regulated sector includes any of the following businesses or services:
  - businesses of banking, other than State banking (within the meaning of paragraph 51(xiii) of the Constitution) not extending beyond the limits of the State concerned;
  - businesses of insurance of banking, other than State banking (within the meaning of paragraph 51(xiii) of the Constitution) not extending beyond the limits of the State concerned;
  - postal, telegraphic, telephonic or other like services (within the meaning of paragraph 51(v) of the Constitution).
- A person to the extent that the person is carrying on or providing a business or service that is part of the regulated sector and is either:
  - acting using a postal, telegraphic, telephonic or other like service (within the meaning of paragraph 51(v) of the Constitution); or
  - acting in the course of, in relation to, trade or commerce between Australia and places outside Australia, trade or commerce between the States, or trade or commerce within a Territory, between a State or Territory, or between two Territories (noting this reflects various heads of power under the Constitution).

2.7 This means that individual sole traders, partners, and trustees of trusts may legitimately become subject to the regulatory activity of the ACCC, or an SPF sector regulator, where they provide a business or service that is part of a regulated sector under this Bill.

2.8 The Bill expressly describes the requirements to be complied with as 'civil penalty provisions'. This triggers the application of the Regulatory Powers Act. Division 6 of the Bill sets out details about the regulatory activity that may be undertaken to enforce the SPF. Where a regulated entity contravenes a civil penalty provision under this Bill or an SPF code, or is suspected of contravening such a provision, that entity may also be subject to a range of regulatory activity specified in the Regulatory Powers Act, including

monitoring or investigation by the relevant SPF regulator. The SPF general regulator, the ACCC, as access to their standard monitoring and investigation tool, section 155 of the CCA, as the SPF general regulator.

2.9 Where the ACMA, ACCC or ASIC are authorised as a sector regulator, they will have access to their existing monitoring and investigation tools in the ACMA Act, the CCA and the ASIC Act respectively. The proposed modification is appropriate given each agency is already established and has powers and functions conferred upon them, including monitoring and investigation powers.

2.10 The Regulatory Powers Act constrains the exercise of regulatory power, ensuring there are adequate safeguards against arbitrary limitations on the right to privacy in the issuing of warrants. It protects regulated entities from the arbitrary abuses of power and allows for greater transparency on the use of the powers. The Regulatory Powers Act provides various protections, including:

- The entry, monitoring, search, seizure and information gathering powers provided in it are conditional upon consent being given by the occupier of the premises or prior judicial authorisation (section 18 of the Regulatory Powers Act).
- Where entry is based on the consent of the occupier, consent must be informed and voluntary and the occupier of premises can restrict entry by authorised persons to a particular period (section 25 of the Regulatory Powers Act).
- Additional safeguards are provided through provisions requiring authorised persons and any persons assisting them to leave the premises if the occupier withdraws their consent (section 25 of the Regulatory Powers Act).
- The issuing officer of a warrant to enter premises for the purpose of monitoring or investigation must be a judicial officer (section 44 of the Regulatory Powers Act).
- An authorised person cannot enter premises unless their identity card is shown to the occupier of the premises (section 26 of the Regulatory Powers Act).
- If entry is authorised by warrant, the authorised person must provide a copy of the warrant to the occupier of the premise (section 28 of the Regulatory Powers Act).

2.11 These powers are reasonable, necessary and proportionate to achieve a legitimate objective. Taken together, they provide an adequate safeguard and limit the use of regulatory powers in the Bill. This ensures that such lawful interferences are not arbitrary or at risk of abuse. These powers also protect important common law privileges, notably those described in Articles 14 and 17 of the ICCPR (see above).

2.12 The Bill authorises the use and disclosure of personal information by regulated entities and SPF regulators. This includes provisions that require regulated entities to share information with SPF regulators that relates to scams, which may include personal information of the person suspect of committing a scam and the victim of a scam.

2.13 The Bill protects against arbitrary interference with privacy by including requirements, where appropriate, that information is de-identified prior to being shared unless doing so would not achieve the object of Part IVF (about the SPF), for example when regulated entities are required to share scam reports with an SPF regulator.

2.14 The Bill balances this protection with the overall purpose of the Bill, to prevent and respond to scams impacting consumers, by requiring that personal information is authorised to be shared in circumstances where there is a time critical nature to that sharing. Generally, the personal information that would be shared is the personal information of the person responsible for or involved in the scam. This will enable the scam to be appropriately investigated and disrupted by regulated entities and will also enable law enforcement agencies to take appropriate action against the scammer.

2.15 If a scam victims' personal information is shared, this will be done to support a regulated entity to disrupt the relevant scam, including by identifying and notifying particular consumers that are at risk about how they can take action to prevent loss or harm (including further loss or harm). It may also be done to allow an SPF regulator to seek the scam victim's consent to make a claim for loss or damages on their behalf. This may be done alongside the SPF regulator initiating proceedings against the regulated entity, and allows for the remediation of loss or damage to be streamlined and save scams victims the time and cost of pursuing a matter in court or through a dispute resolution process.

2.16 Therefore, to the extent that the information sharing provisions in the SPF constitute a limitation of a person's right to be protected from interference with his or her privacy, the limitation is justified. The provisions are prescribed by law and are in pursuit of the legitimate objective of preventing and responding to scams impacting consumers.

Right to fair trial

Civil penalties are not 'criminal'

2.17 Civil penalty provisions may engage criminal process rights under Articles 14 and 15 of the ICCPR regardless of the distinction between criminal and civil penalties in domestic law. This is because the word 'criminal' has an autonomous meaning in international human rights law. When a provision imposes a civil penalty, an assessment is required as to whether it amounts to a 'criminal' penalty for the purposes of Articles 14 and 15 of the ICCPR.

2.18 The Bill expressly describes the requirements to be complied with as 'civil penalty provisions' and creates a regime for their enforcement. This triggers the application of the Regulatory Powers Act and its standard provisions. The penalties to be imposed are appropriate and tailored to the purpose of the SPF, which aims to prevent and respond to scams impacting consumers.

2.19 The civil penalty orders provided for in the Bill are pecuniary in nature and operate to create a debt to the Commonwealth. They do not apply to members of the public, but to a cohort of businesses operating within a regulated sector.

2.20 There are two tiers for contraventions under the SPF, with different penalties for each tier. The maximum quantum for a tier 1 contravention is higher as these are reserved for conduct that contravenes certain, fundamental obligations of the SPF principles. The provisions set an amount as the maximum penalty that should apply in the most egregious instances of non-compliance with the Bill.

2.21 A tier 1 contravention is a contravention of a civil penalty provision set out in Table 2.1.

Table 2.1 Tier 1 civil penalty provisions

Provision	***Description of civil penalty***
58BJ	Entity fails to take reasonable steps to prevent scams
58BM	Entity fails to take reasonable steps to detect scams
58BN	Entity has actionable scam intelligence and fails to take reasonable steps to investigate
58BO	Entity has actionable scam intelligence and fails to take reasonable steps within reasonable time to identify consumer
58BX	Entity has actionable scam intelligence and fails to take reasonable steps within reasonable time to disrupt the activity or prevent loss or harm arising from the activity
58BY	Entity has actionable scam intelligence and fails to give a report about actionable scam intelligence to the SPF general regulator
58BZC	Entity does not have accessible mechanism for person to report activity that is or may be a scam
58BZD	Entity does not have accessible and transparent IDR mechanism
58BZE	Entity undertakes IDR and fails to have regard to prescribed process and guidelines
58BZF	Entity fails to make publicly accessible information about rights of SPF consumers under reporting and IDR mechanisms and EDR scheme
58BZG	Entity is not a member of an authorised EDR scheme or fails to give reasonable assistance to or cooperate with the EDR operator or fails to comply with obligation under SPF code for sector that relates to scheme.

2.22 The maximum penalty amount for a tier 1 contravention by a body corporate is the greater of the following:

- 159,745 penalty units (which is currently $50,000,185);
- if the relevant court can determine the total value of the benefit that the body corporate and any body corporate related to that body corporate have obtained directly or indirectly and is reasonably attributable to the contravention – three times that total value;
- if the court cannot determine that total value – 30 per cent of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

2.23 The maximum penalty amount for a tier 1 contravention by a person other than a body corporate is 7,990 penalty units (which is currently $2,500,870).

2.24 A tier 2 contravention is a contravention of a civil penalty provision of an SPF code or a civil penalty provision set out in Table 2.2.

Table 2.2 Tier 2 civil penalty provisions

Provision	***Description of civil penalty***
58BD	Entity fails to document and implement governance policies and procedures relating to scams, and develop and implement performance metrics and targets to measure the effectiveness of those policies and procedures.
58BE	Entity fails to provide annual certification about its governance policies, procedures, metrics and targets.
58BF	Entity fails to meet the record keeping obligations relating to governance
58BG	Entity fails to provide a report about its governance arrangements upon request by an SPF regulator
58BR	Entity fails to report actionable scam intelligence to SPF regulators
58BS	Entity fails to report scams to SPF regulators upon request by an SPF regulator

2.25 The maximum penalty amount for a tier 2 contravention by a body corporate is the greater of the following:

- 31,950 penalty units (which is currently $10,000,350);
- if the relevant court can determine the total value of the benefit that the body corporate and any body corporate related to that body corporate have obtained directly or indirectly and is reasonably attributable to the contravention – three times that total value;

- if the court cannot determine that total value – 10 per cent of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

2.26 The maximum penalty amount for a tier 2 contravention by a person other than a body corporate is 1,600 penalty units (which is currently $500,800).

2.27 The judiciary continues to have discretion to consider the seriousness of the contravention and impose a penalty that is appropriate in the circumstances. The civil courts are experienced in making civil penalty orders at appropriate levels having regard to the maximum penalty amount, considering a range of factors including the nature of the contravening conduct and the size of the entity involved.

2.28 Further, while the civil penalty provisions in the Bill are intended to deter people from non-compliance with the SPF, none of the civil penalty provisions carry a penalty of imprisonment and there is no sanction of imprisonment for non-payment of any penalty.

2.29 Therefore, the civil penalty provisions introduced by the Bill should not be considered 'criminal' for the purposes of Articles 14 and 15 of the ICCCPR.

Reverse evidential burden

2.30 There SPF rules may contain exceptions to the requirement to report actionable scam intelligence to the SPF general regulator under section 58BR. For example, the rules may specify that entities are not required to report actionable scam intelligence it received from the SPF general regulator to avoid duplication. The SPF rules may also specify an entity is not required to share information where doing so would be inconsistent with an overseas privacy law which also applies to the actionable scam intelligence.

2.31 Where such an exception applies, the defendant bears an evidential burden in relation to establishing those matters because this operates as an exception to general obligation of the SPF. This refers to the burden of adducing or pointing to evidence that suggests a reasonable possibility that the exception in the SPF rules apply.

2.32 This is consistent with the operation of the Regulatory Powers Act and is appropriate as the information relating to this matter is peculiarly within the knowledge of the defendant. This limitation is also necessary to avoid costly and difficult investigations by an SPF regulator to enforce the reporting requirement, which play a critical role in achieving the object of the SPF.

Infringement notices

2.33 The Bill also engages the right to a fair and public hearing through the creation of an infringement notice scheme. An infringement notice can be issued by an inspector of an SPF regulator for a contravention of a civil penalty provision that is enforceable under the Bill. Section 58FS operates so that the alleged contravention of the civil penalty provision will be heard by a court where:

- the person does not pay the penalty specified;
- within the compliance period;
- in accordance with the notice; and
- in circumstances where the notice has not been withdrawn by the regulator.

2.34 This ensures the right of a person to a fair and public hearing by a competent, independent and impartial tribunal is preserved by the Bill.

2.35 Additionally, the Bill outlines that the operation of section 58FS must be explained in an infringement notice issued to a person.

2.36 Under section 58FR, neither criminal nor civil proceedings may be brought against a person who has been issued an SPF infringement notice where the person pays the specified penalty in accordance with that notice and within the compliance period. As well as in circumstances in which the infringement notice has not been withdrawn. Further, the contravention alleged in the infringement notice is not proved by the payment of that penalty.

2.37 The ACCC has an existing investigation power under section 155 of the CCA. Section 155 confers power on the ACCC to obtain information, documents and evidence about conduct that constitutes or may constitute a contravention of the CCA. This power may be delegated under new section 58EC to a sector regulator or a member, SES employee, or other employee of the sector regulator acting at an SES level, and the sector regulator has agreed to the delegation in writing.

2.38 In addition, the Bill provides for the regulators to have certain other enforcement powers relating to monitoring or investigating compliance with an SPF code. Generally, regulated entities are to be subject to monitoring and investigation under Part 2 of the Regulatory Powers Act, except where: either the ACCC, ASIC or ACMA is the sector regulator; or a declaration is in force under subsection 58FI(2) (which declares that particular monitoring powers are to apply). Within Part 2 of the Regulatory Powers Act, sections 24 and 54 make it an offence to fail to answer questions of an authorised officer. Conduct constituting an offence under either provision is subject to a penalty of 30 penalty units. Sections 17 and 47 of the Regulatory Powers Act affirm that the privilege against self-incrimination and legal professional privilege are not abrogated. These protections guarantee the fair trial rights protected in Articles 14(3)(d) and (g) of the ICCPR by limiting the operation of the questioning powers provided by the Regulatory Powers Act.

2.39 To the extent the Bill engages Article 14 of the ICCPR, it does so appropriately. It is regulatory and disciplinary in nature and limited to achieving the measure's purpose. A higher penalty may be imposed on individuals amounting to a criminal penalty if their value exceeds the maximum amount allowed by the civil penalty law.

Conclusion

2.40 The Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the Human Rights (Parliamentary Scrutiny) Act 2011. Where the Bill may limit human rights, including where the provisions of the Regulatory Powers Act have been triggered, those limitations are reasonable, necessary and proportionate for the regulators to carry out their functions and to achieve the object of the SPF, which is to prevent and respond to scams impacting the Australian community.

Attachment 1: Impact Analysis

Executive summary

Scams are a growing issue in Australia inflicting significant harms on Australians. There are a range of impacts of scams including harms to consumers, reputational damage for businesses, withdrawals from the digital economy and undermining public trust.

Current industry initiatives lack a coordinated cross-sector approach to protect Australians from scams. Without government action, industries providing services that are vectors of scam activity are unlikely to be sufficiently incentivised and coordinated to respond to the rising cost of harms from scams.

The core objectives of the government's policy response would be to both reduce scam harms and align the benefits and costs of scam prevention. These objectives are supported by secondary goals to uplift industry actions to prevent, detect, disrupt, and report scam activity and to better support Australians who experience a scam.

Treasury has considered two options:

- Option 1: Maintain the status quo.
- Option 2: Establish the Scams Prevention Framework (SPF), implementing the Government's election commitment to introduce a mandatory framework for industry codes on scams initially applying to banks, telecommunications providers and certain digital platforms.

Option 2 would involve regulatory costs for banks, telecommunications, and certain digital platforms to uplift their anti-scam activities, information sharing and dispute resolution capabilities. Option 2 has been assessed as likely to involve a net benefit through reducing scam exposure, losses and redress. The SPF would improve the regulatory framework for industry scam prevention activities, improve sharing of actionable scam information across the economy and improve dispute resolution systems and outcomes for scam victims.

Treasury undertook public consultation on policy options from November 2023 to January 2024. Targeted consultation with industry continued in mid-2024 and draft legislation underwent public consultation from September to October 2024. Consultation has informed the design of the SPF under option 2 as well as the level of regulatory burden it would involve.

Option 2 is the preferred option to implement the government's objectives to both provide benefits in reducing scam harms and improve the alignment of the costs and benefits of scam prevention activity. Implementing the SPF is preferable to the status quo, under which there would not be an overarching framework to enable uplift in industry's scam prevention activities.

The SPF would be implemented through legislating a framework for industry codes, designating relevant services of banking, telecommunications and certain digital platforms, and developing sector codes to prescribe further specific obligations.

Upon implementation the SPF would be evaluated by the government through several measures using data from government and industry sources. These include consumer and industry reports about scams, agency monitors of consumer victimisation and evaluation of industry compliance with mandatory obligations.

Background

Scams are a significant source of financial crime that inflict unacceptably high harm to Australian consumers and industry. Scams target a wide range of people by exploiting the social and technological vulnerabilities in the way Australians interact and do business online. Scams are often linked to other crimes, including identity theft and cybercrime.

Scams are attempts, directly or indirectly, to deceive a consumer into obtaining financial benefits or personal information. The scope of 'scam' activity is not currently defined in legislation. Most scams aim to induce an individual to act to initiate payments to the scammer or disclose account or security credentials. Scams can be carried out through a wide range of communication channels, including phone, text message, social media, and email.

In response to the rising impact of scams, the Government made an election commitment to introduce tough, new mandatory industry codes for banks, telecommunication providers and social media companies to combat scams. Policy options considered in this Impact Analysis (IA) would build on $58 million in funding to launch the National Anti-Scam Centre (NASC) on 1 July 2023.[1] The NASC co-ordinates efforts to prevent scams by improving intelligence sharing across Government and the private sector, raising public awareness about scams and making it easier for consumers to report scams to a single agency. These efforts have contributed to a 13 per cent annual decrease in scam losses in 2023, the first downward trend since combined reporting on scam losses began in 2015.

At the 2024-25 Budget, a draft version of this IA was provided to inform a Budget decision on developing mandatory industry codes for regulated businesses to address scams on their platforms and services. Subsequently, a full IA was developed alongside finalisation of policy, informed by public consultation on the draft legislation in September 2024, to support the Government's final policy decision in October 2024.

[1] Budget 2023-2024, *Budget Paper No. 2 – Budget Measures*, page 211.

1. Policy problem

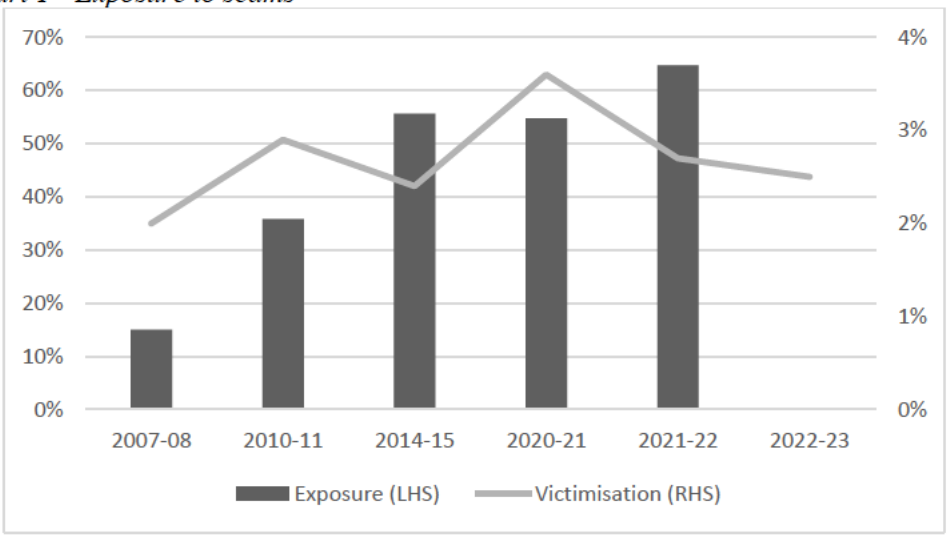
1.1 Scams are a significant issue of growing concern

1.1.1 The recent growth in scam activity

The impact of scams on Australians has risen sharply and has accelerated since 2020. High-value losses, driven by the growth in investment scams, have led to billions being stolen from Australians, peaking at $3.1 billion in 2022.[2] Most, if not all Australians, have been targeted by a scam attempt.

The Australian Bureau of Statistics (ABS) has periodically surveyed Australians in the Personal Fraud report (see Chart 1) to estimate the annual incidence of scam exposure and victimisation.[3] ABS figures estimate that 2.5 per cent of Australians (514,300) were victimised by a scam in 2022-23, only slightly higher than the rate of 2.0 per cent in 2007-08. Scam exposure rates have risen from 15 per cent in 2007-08 to 65 per cent of the population in 2021-22.[4] Australian Institute of Criminology (AIC) surveys that found 13.6 per cent of those surveyed were scammed in their lifetime, and 3.6 per cent were scammed in the year 2023.[5]

Chart 1 - Exposure to scams[6]



[2] ACCC, *Targeting Scams* 2022

[3] Data attempts to measure the impact of scam attempts through exposure and victimisation rates. Exposure to scams includes all incidences where a scammer uses a contact method to target a consumer, regardless of its impact on them. Victimisation rates only capture experiences of scams where the victim has been defrauded and experienced a loss.

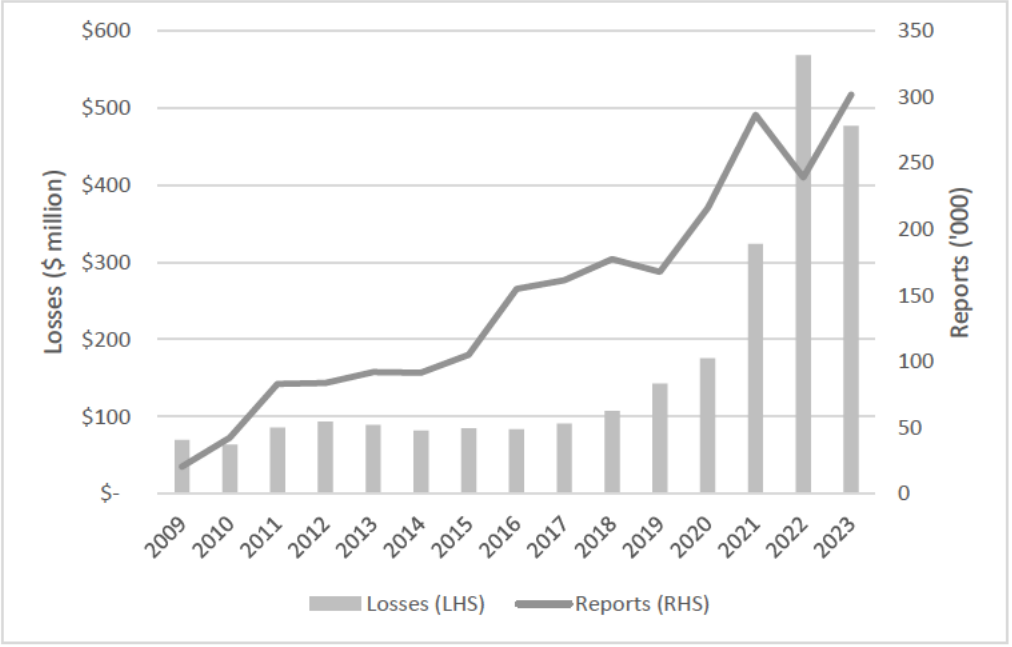
[4] ABS, *Personal Fraud, 2022-23*, 20 March 2024. A person was considered to have been exposed to a scam if they had received an unsolicited invitation, request, notification or offer, and read, viewed, or listened to the material.

[5] AIC, *Cybercrime in Australia 2023*, 27 June 2023 p. 30-32

[6] ABS, *Personal Fraud, 2022-23*, 20 March 2024

The increasing prevalence in scams is also shown in the rapid rise of reports through reporting portals including Scamwatch. Scamwatch reports provide details on a scam from individuals who have encountered or been affected by a scam, allowing the Australian Competition and Consumer Commission (ACCC) and the NASC to co-ordinate responses. Although reporting of scams to Scamwatch has steadily risen over time, annual losses abruptly increased from 2020 (see Chart 2). Australians have reported over 164,000 scams totalling $160 million losses in the year to September 2024.[7]

Chart 2 - Consumer reports to Scamwatch[8]



In 2023, business made 4,933 scam reports to Scamwatch, an increase of 27.9 per cent from 2022.[9] Scams on businesses resulting in the most losses involved false billing and investments. Of the $29.5 million in reported scam losses for businesses $17.3 million were reported by small and micro businesses.

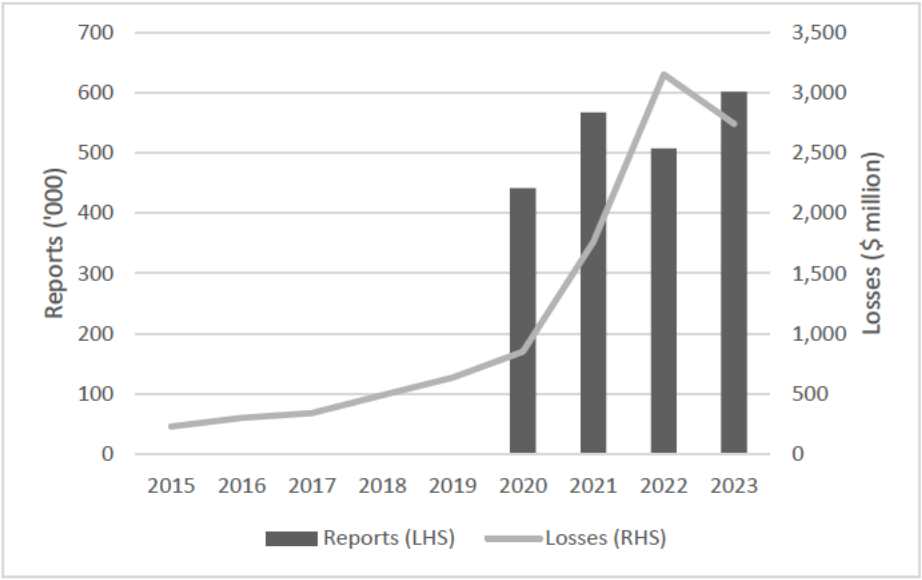
In recent years, the information sharing infrastructure of the ACCC has been enhanced to enable reporting on 'combined' figures from consumers and industry. This includes data sourced from Scamwatch, ReportCyber, the Australian Financial Crimes Exchange (AFCX), IDCARE, and the Australian Securities and Investments Commission (ASIC).

Combined data shows a consistent trend with Scamwatch reports, depicting a rapid rise in losses from 2020 as shown in Chart 3. Annual reported losses to scams made by Australians increased from $634 million in 2019 to $1.8 billion in 2021, and further

[7] ACCC, Scamwatch online data dashboard
[8] ACCC, Scamwatch online data dashboard
[9] Ibid.

increased to a peak of $3.1 billion in 2022.[10] In 2023, reported scam losses declined for the first time since 2016 to $2.7 billion. Although, expanding combined reporting infrastructure could be impacting the growth in figures.

Chart 3 - Combined industry and consumer reports[11]



In 2023, Australians made over 601,000 reports about scams to combined data sources, including 302,000 reports to Scamwatch. In the 29,000 reports to Scamwatch involving losses to a scam, the average loss was $16,000 and the median was $500.[12] The largest reported losses and the driver of growth in scams are largely from investment scams, which form around half or $1.3 billion in combined losses. Individuals often lose their entire savings or have their accounts drained from investment schemes. The median loss is much lower than the average as many of the more reported scam types, including phishing or buying and selling scams, are lower, one-time fraudulent payments.

1.1.2 Scams inflict a broad range of harms

While not quantifiable, ongoing trends of elevated losses to scams arising from insufficient consumer protections and inconsistency in industry approaches can cause broader societal costs.[13] Beyond the financial losses, scams can have a devastating impact on victims' lives, causing significant psychological, emotional and social distress to the individual and their families. The prevalence of scam activity also reduces confidence in digital commerce, communication and government authorities. A selection of these and broader costs are outlined in Table 1.

[10] ACCC, *Targeting Scams*, 2023

11 ACCC, Targeting Scams, 2015 to 2023 reports. Combined figures for the number of consumer reports are not comparable prior to 2020 due to changes in data sources and methodology.

[12] ACCC, Targeting Scams report 2023.

[13] International Public Sector Fraud Forum, *Guide to Understanding the Total Impact of Fraud,* 2023.

Table 1 – Broader impacts inflicted by scams

Personal	• The increased need for diligence and caution by consumers imposes costs for individuals, including through the time to assess or verify legitimacy of sources. These self-imposed costs by consumers add to frictions industry puts in place to prevent scam activities. Heightened diligence and caution could also drive withdrawals of participation in the wider digital economy. • The prominence and frequency of exposure to scams attempts on communications platforms such as social media, chat services and telecommunications inflict nuisance costs on individuals. These exposures to scams result in wasted time and effort by individuals. • Australians invest in personal administrative or external security measures to help them avoid falling victim to a scam. This may include the time and cost involved in considering changing service providers, establishing alternate contact details, or changing how they manage their banking to minimise the potential for scam activity. • Losses from scams inflict emotional, and psychological impacts upon victims, potentially creating long-term burden and costs. Financial losses to scams reduce the financial independence and wellbeing of victims. • Those affected by a scam may face the resulting additional time, cost and psychological burden associated with seeking support to recover. This arises from a lack of clarity on responsibility for industry to respond to reports of scams and provide support to victims.
Business	• Scams can create financial and reputational risks for businesses. Businesses that provide services which are vectors of scam activity may choose to invest in systems or processes to minimise the exposure of their brand or may otherwise need to devote additional resources to rebuild public trust. • Businesses which are vectors of scam activity or that are impersonated by scammers may suffer loss of revenue as consumers disregard legitimate dealings or look to minimise risk by avoiding interacting with them.
Broader economic	• Managing scam-related risks requires industry to absorb greater costs, staffing and resources into detecting, investigating and responding to scams, affecting competitiveness. Some of these costs may be passed onto consumers through higher prices. Activities to reduce the harm of scams impose inefficiencies for economic activity. • The frequency of scam activity can change consumer behaviour or create inefficiencies in digital transactions. • If costs of managing scams are inequitably distributed across the scams ecosystem, it may result in inefficient allocation of capital

	or labour across the economy and detract from productivity outcomes. • The erosion of trust in digital interactions damages the reputation and economic standing of impersonated businesses or government agencies, potentially unwinding efficiency of digital interactions and if not addressed may lead to withdrawal from digital technology by parts of Australian society.
Security	• Scams often intersect with other fraud and cybercrime offences, including data breaches and identity theft. The increased proliferation of scams affects the privacy and information security of businesses and their consumers.
Social	• The behaviour of scammers acts to undermine public trust in the brands and services which are being impersonated or co-opted by the scam, causing inefficiency and reducing confidence in online commerce and digital communication. • Scams may lead to risk aversion or undermine trust and confidence in essential functions of the economy, including the reliability of communications and transactions and the capacity of industry and government to protect consumers.
Government	• Government revenue collection and expenditure required to deliver programs may be impacted due to distrust of government communication channels and institutions. • The erosion of trust damages the reputation of impersonated businesses and government agencies which, if not addressed, may lead to withdrawal of digital technology from government administration.

Inaction to combat scams will see these problems increase over time, with consequential increases in the cost and time required to rectify them in the future.

1.2 Drivers of scams

Australia, as with many other countries, is experiencing spikes in losses. A list of several underlying factors as to why this has occurred is outlined in Table 2. This section examines some of these factors in detail below.

Table 2 – Drivers of recent growth in scam losses

Drivers of recent scam losses	
Cybersecurity threats	As more data is collected about consumers, high-profile data breaches and cyber threats have compromised consumer security and personal details that can be used by malicious actors to target scam victims and carry out scams.

Drivers of recent scam losses	
Increased digitalisation of the economy	The pandemic created abrupt shifts across the economy towards remote work and communication, leading to increased uses of digital services in ways that were unfamiliar or at a far higher rate than before. The efficiency gains and speed of transactions, from communication to payments channels, have enabled significant acceleration of interactions between parties.
Use of crypto and digital assets	The emergence and increasing uptake of unregulated digital assets such as cryptocurrencies, unfamiliar to many consumers and of increasing interest to others, has been exploited by scammers as an exit channel to direct funds out of the control of the victim.[14]
New technologies	Scammers have become increasingly sophisticated in their efforts due to the take up of newer technologies at their disposal, such as chat bots and artificial intelligence, that allow them to impersonate legitimate entities with far greater accuracy and deploy communications to a wide audience.[15]
Economic pressures	Economic pressures during and after the pandemic have led to greater financial pressure on consumers, increasing the panic of responses to scam demands for unpaid fees or the allure of profiting from scam investments.

1.2.1 Growth of low-cost frequent consumer contact

Low barriers to entry and costs to initiate digital communication and commerce (including via online and social media) allow scammers to initiate direct consumer contact at high frequency. The high volume and prevalence of unsolicited offers or communication from scammers works on the basis that a proportion of those targeted will pursue the illegitimate offer. Scam tactics can be seen as lucrative activity for criminals as they succeed due to these high volumes of communications creating many opportunities propagating illegitimate offers.

Growing use of digital communication and media channels by industry and governments have generally not been supported by robust and readily available means for the public to validate the identity and legitimacy of the source, or to authenticate commerce offers. Requirements for customer identity validation, such as those which exist in the financial sector, are not universal in all sectors. Consumers also lack easy methods to verify whether communications are from a legitimate business or a scammer.

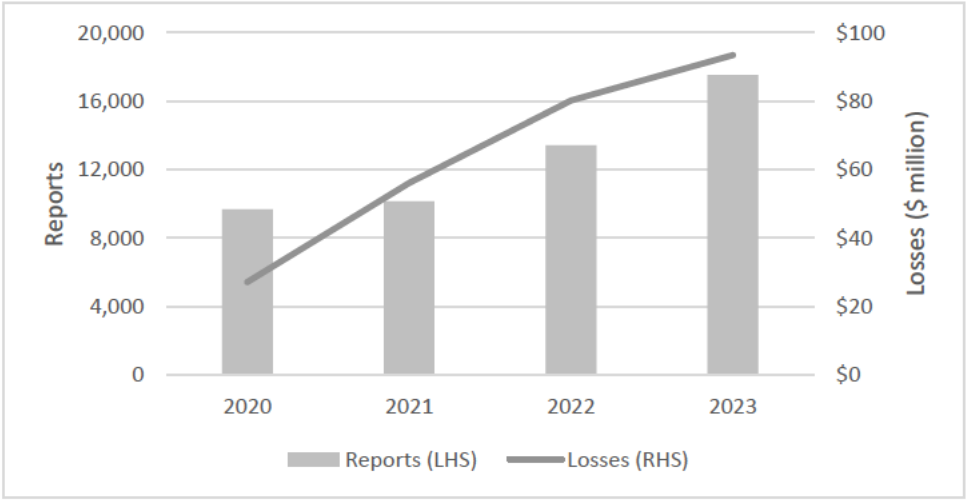
[14] ACCC, *Targeting Scams 2021,* p. 1, 27, 69
[15] ACCC, *Targeting Scams 2022*, p. 14

The 2023 Scamwatch consumer reporting data[16] provides information on the major channels used by scammers including:

- contact methods most commonly reported were text message (36 per cent), email and phone.
- contact methods most frequently associated with financial losses were phone (24 per cent), social networking and online forums and email.
- phishing scams were the most common scam approach, representing 36 per cent of all reports. Despite the inconvenience of their prevalence, only 2 per cent of phishing reports were associated with a financial loss.
- investment scams, while only 3 per cent of all reports, were associated with $292 million or 61 per cent of all reported losses. Additionally, investment scams were associated with a high average loss of $81,300.

Digital platform service providers are a rapidly expanding conduit for scammers to target consumers. In particular, social media is over-represented as a source of losses to scams, accounting for 6 per cent of reported contact methods in 2023, but is the second most common source of scam losses. Chart 4 illustrates the consistent rise in consumer reports on social media scams to Scamwatch, leading to $93.5 million in losses reported in 2023.

Chart 4 – Social media and online forum scams reported to Scamwatch[17]



1.2.2 Awareness and response lags evolution in scam tactics

It can be very hard to spot a scam. Scammers are sophisticated and may interact with a target over multiple communication platforms to build a false connection. Scammers rapidly adapt their approach to take advantage of modern technology, products, services, and major events to convince everyday Australians that a scam is a legitimate offer.

[16] ACCC, Scamwatch online data dashboard
[17] ACCC, Scamwatch online data dashboard

Scammers also take advantage of the immediacy of online transactions by using urgency and psychological pressure to motivate targets to act without further consideration or investigation. Scammers' demands for real-time financial transfers or the use of difficult to trace forms of payment (such as gift cards and crypto assets) reduce the opportunity for those targeted to stop payments or seek recovery of financial losses.

Consumers play an important role in detecting and preventing scams, but can also be affected in ways that diminish their ability to disclose, report and seek help when they have been scammed. Shame and social stigma associated with falling victim to a scam is a disincentive for reporting and can prevent discussion of experiences to help consumers understand that anyone can get scammed. Although communication and education activities are important prevention activities, these alone are not likely to be impactful as scammers continue to change strategies and adapt to new technologies and trends.

1.3 Industry responses to scams activity

1.3.1 Lack of clear responsibility and accountability for mitigating scam harms

A successful scam will often involve illegitimate activity across multiple sectors to engage the consumers. The sectors scammers most used as a conduit for consumer harm are banks, telecommunications providers and digital platform service providers. For example, a scam may be initiated via a fraudulent advert on a social media platform, which leads to engagement via phone before payment being made by the victim via a bank transfer.

Businesses and industry associations in these sectors have recognised the growing prevalence of scams and have independently begun to take steps to mitigate the impact and harm scams have on Australians. However, businesses that are co-opted by scammers currently have differing approaches in how they respond to reports of potential scam material. In some cases, businesses are perceived to prioritise direct commercial or economic outcomes for their business over investigating the potential harm, disruption, victimisation, and financial losses to their consumers. Poor or sluggish responses to potential scam reports perpetuates the exposure and likelihood of success of a scam.

A successful scam often involves illegitimate activity across multiple sectors in the scams ecosystem, leading to an array of challenges for consumers, industry and government such as:

- which sector the consumer contacts to report the scam and seek support or redress,
- how to share relevant information between industry, law enforcement agencies and regulators to investigate scam reports and improve disruption of scams by sharing intelligence of evolving scam patterns,

- how to determine the specific actions or failures by sectors in the scams ecosystem which contributed to the compromise of consumer protection,
- what regulatory avenues can be used to pursue illegitimate scam activity, and
- how to determine the appropriate and proportional accountability and responsibility for failures in consumer protections, and related liability for losses and appropriate penalties.

The involvement of many sectors means there are inconsistent views across the scam ecosystem regarding the responsibility and accountability of each sector to mitigate harms and to provide support or pathways for redress to consumers. Sectors, which are by their nature at differing points in consumers experience of a scam, face differing reputational detriment and incentives to disrupt scam activity or to help consumers to verify the legitimacy and identity of digital commerce and communication.

The regulatory landscape needs to evolve to better protect consumers from scams in an environment where multiple sectors play a role. Consumers can experience frustration in seeking action, investigation, or support from entities at different stages of the scam life cycle. These issues are compounding as scams increase in complexity and sophistication over time. Clear and effective regulation is needed to balance the competing interests of establishing co-ordinated responses and consumer protections for scams while not limiting industry competition or innovation.

1.3.2 Inconsistent dispute resolution processes for scams

Dispute resolution arrangements vary in the banking, telecommunications, and digital platforms sectors, resulting in inconsistent outcomes for scam victims seeking redress. Industry-specific internal dispute resolution (IDR) and external dispute resolution (EDR) arrangements are currently required to be in place for banks and telecommunications providers. The Australian Financial Complaints Authority (AFCA) is the EDR body for complaints against banks and the Telecommunications Industry Ombudsman (TIO) for telecommunications-related complaints. There are no existing industry-specific IDR or EDR arrangements operating for digital platforms. As a result of these varying arrangements across the ecosystem, there is often confusion for consumers in how to report scams, or seek support and redress. Industry-specific EDR arrangements mean scam victims may find themselves lodging complaints with multiple EDR schemes and be bounced between different EDR schemes This results in additional time and psychological burden when dealing with the financial and emotional harm of scams.

Further, industry specific EDR arrangements mean there is no holistic consideration of the role multiple entities in different sectors play in a scam complaint. The realisation by a consumer they have been scammed often occurs after payment has been made, meaning payment providers such as banks are frequently the point of the ecosystem where consumers report a scam and seek assistance to recover the financial loss. Where there is a dispute between a bank and a consumer, and a satisfactory outcome could not be reached through IDR, the consumer may escalate a complaint to AFCA. However, AFCA is only able consider the conduct of the bank involved, and not other industry

sectors which may have been involved in the scam chain (e.g. digital platforms) and could have acted to prevent the financial loss or scam.

1.3.3 Piecemeal and slow industry action

Industry self-regulation is occurring in some sectors, but not at the pace consistent with growth in scam activity.

Some individual businesses or areas of industry sectors have made efforts to address scams, such as the introduction of the Reducing Scam Calls and Scam Short Messages (SMs) industry code for telecommunications providers, the Australian Banking Association (ABA) and Customer Owned Banking Association's (COBA) Scam-Safe Accord, and the Digital Industry Group Inc. (DIGI) Australian Online Scams Code (AOSC). Of these only the Reducing Scam Calls and Scam SMs industry code is compulsory with enforcement by ACMA.[18]

Several banks, telecommunications and digital platforms providers, participate in the AFCX (an industry-led information sharing and reporting regime) where members can use an online platform to identify and analyse suspicious transactions and alert other members.[19] In 2023, the AFCX expanded the platform to build a Fraud Reporting Exchange that enables members to send and receive near real-time reports to co-ordinate and halt multiple transactions in the chain of a single scam. However, as these information sharing arrangements are not supported by legislative provisions, participants face legislative constraints in sharing information which may contain personal identifiers between member organisations. The scope of the Fraud Reporting Exchange is also limited to organisations which voluntarily participate and invest in information sharing.

The current voluntary approach to addressing and introducing anti-scam measures by industry has been inconsistent and slow relative to the sharp rise in scam activity. Industries across the scam ecosystem have taken a piecemeal approach to addressing the scams threat, with the result that efforts have been misaligned and haphazard.

See **Appendix 1** for further detail on industry actions to date.

2. Need for Government action

2.1 Need for government action

Government action is required to ensure effective coordination, and a whole-of-ecosystem response to reduce financial losses from scams and restore trust in digital commerce and communication. Without government action, it is unlikely the cost of harms will be adequately considered by industries which are vectors of scam activity.

[18] ACMA carries enforcement powers to issue warnings and directions to participating entities to comply with relevant industry codes, and can issue infringement notices and penalties if these are not met. See Part 6 of the *Telecommunications Act 1997.*

[19] Full membership of the AFCX is not publicly disclosed, however participants include the four founding major banks, Macquarie and Bendigo Bank, and COBA.

As a result, there will not be consistent and effective anti-scam protection measures implemented by industry across the entire scam ecosystem and the costs will fall inequitably across society.

2.1.1 Economy-wide coordination of anti-scam activity

Clear and consistent standards for preventative action across all high priority sectors in the scam ecosystem are needed to ensure gaps in consumer protections are minimised. Effectively achieving this outcome will depend on action by those who have the best opportunity and most appropriate resources to address scams. Voluntary action by industry has not proven sufficient to date.

Effective and coordinated action across the economy is limited by the absence of an overarching regulatory framework that sets clear roles and responsibilities for government, regulators, consumers and the private sector. The current piecemeal and fragmented voluntary approach has made it easier for scammers to exploit regulatory gaps across the ecosystem. It has also made it difficult for consumers and victims of scams to understand the role and responsibility of a business in combatting scams and providing clear responses to scam reports.

Prevention actions must be taken across all sectors in the ecosystem that are high-risk for scam activity. In the absence of action across the ecosystem, scammers will shift their activity to the sectors which have weaker practices relating to scam protections. This would leave Australians exposed to sophisticated scam activity.

2.1.2 Improving alignment of costs and benefits of action

Reliance on voluntary market action is unlikely to be effective as losses and detrimental reputational impacts are inequitably distributed across the scam ecosystem between government, industry and consumers. Incentives for comprehensive voluntary action are lacking for key sectors as the business and reputational cost of scam activity are misaligned with the relative roles sectors' play as vectors of scam activity. For example, although digital platforms encounter reputational risks and potential loss of users from the presence of scams hosted on their platforms, this content persists on many platforms. Scams reported to Scamwatch originating on social media led to the largest growth in losses from 2022 to 2023 (16.5 per cent from $80.2 million to $93.5 million), while losses have been decreasing for scams perpetrated using most other contact methods (e.g. 17.7 per cent decrease in losses from scam phone calls).[20]

Government action is required to create consistent incentives and obligations for action to minimise harm from scams across the scam ecosystem. Government action is needed to ensure that the treatment of consumers who report scams or seek redress is not determined predominately by the service providers through which the scam occurred.

[20] ACCC, *Targeting Scams 2023*. p. 14

2.1.3 Providing a consistent message

There are currently many competing voices in the scam disruption space, with various perspectives creating confusion and inconsistent messaging for Australians. The Government can provide a consistent voice of authority that Australians could rely on to improve consumer protections. Government can establish expectations for how businesses respond to scams, support victims and establish pathways for equitable redress where a business has failed to meet these expectations.

Government action to set expectations across the entire ecosystem would reduce confusion and inconstant messages, allowing consumers to:

- feel more confident engaging with the digital economy without being overly exposed to scams;
- increase trust in communications from government and industry and feel better protected from scams;
- be less disrupted by scam activity, and the time required to assess or verify the validity of digital communication or commerce; and consequentially result in fewer reports of scams;
- increase confidence that industry and government will respond to scam reports; and
- incur less financial, psychological, emotional and social distress from scam activity.

2.1.4 Co-ordination with international anti-scam initiatives

Government action is needed to ensure scam prevention activities are co-ordinated economy-wide, in alignment with international activities and commitments. Internationally, government-initiated actions are being taken to establish pathways for consumers to report scams, and for policies to tackle scams economy-wide which inform the policy approaches in Australia. In the United Kingdom there are voluntary sector charters for fraud between the government and industry sectors to address scams.[21] In Singapore, proposals have been put for adoption of a Shared Responsibility Framework to allocate liability for scams across sectors. [22]

In March 2024, the Government participated in multilateral dialogue at the inaugural Global Fraud Summit hosted by the United Kingdom Government. The outcomes of the Summit included a communique establishing an agreed global framework for addressing fraud, including commitments to co-ordinate and strengthen international government and industry collaboration on scam prevention. These commitments have been supported by bilateral dialogue with countries, including Singapore, the United Kingdom and New Zealand.

[21] United Kingdom Finance, *2023 Half-Year Fraud Update;* United Kingdom Home Department, *Online Fraud Charter 2023.*
[22] Monetary Authority of Singapore, *Consultation Paper on Proposed Shared Responsibility Framework,* 20 December 2023.

2.2 Successful government action

2.2.1 Improvements have been associated with Government action

The work by Government to date has had an impact on reducing scam activity and losses. For example, ASIC's takedown capability removes or limits access to fraudulent and malicious websites on the internet to disrupt scam activity, which has led to takedowns of more than 7,300 investment scam and phishing websites between July 2023 and August 2024.[23] The takedown service has mostly targeted fake investment platforms appearing to offer high-risk products like foreign currency derivatives and crypto assets. ASIC is also targeting impersonation scams where legitimate businesses are cloned to trick consumers, and fake celebrity endorsements used to fraudulently promote financial products.[24] These actions have helped drive investment scam losses down by around 60 per cent in the second quarter of 2024 compared to the same quarter in 2022.[25]

Following the introduction in July 2022 of the Reducing Scam Calls and Scam SMs industry code, telecommunications providers have blocked 1.5 billion scam calls and 668 million scam SMS.[26] Between April and June 2024, telecommunications providers reported blocking over 156 million scam calls and over 134 million scam SMS.[27]

Government provided $10.9 million over four years to launch[28] a SMS Sender ID Register to combat scammers impersonating key industry or government brand names in text message headers. The voluntary pilot, commenced by the Australian Communications Media Authority (ACMA) in December 2023[29], consolidates existing provider-level initiatives to protect participating alphanumeric sender IDs from impersonation by scammers. Following an extension of the pilot,[30] and a consultation on the design of a mandatory Register,[31] the legislation amending the *Telecommunications Act* to establish the SMS ID Register received royal assent on 22 August 2024.[32]

While Australian Government initiatives to combat scams are showing initial signs of reducing the acceleration of scam losses and exposure, scam harms remain unacceptably high. Despite positive signs, consistent and integrated economy-wide action is hindered by the lack of incentives some sectors have for robust voluntary action.

[23] ASIC, *Online investment trading scams top ASIC's website takedown action ,* 19 August 2024.
[24] The Hon Stephen Jones MP, Assistant Treasurer and Minister for Financial Services, *Thousands of scam investment websites removed in takedown blitz,* 2 November 2023.
[25] ACCC Scamwatch, *Scam Statistics* data dashboard
[26] Calculated from ACMA's "Action on telco consumer protection" quarterly reports from the July to September 2022 to April to June 2024.
[27] ACMA, *Action on telco consumer protections* April to June 2024, 12 August 2024.
[28] The Hon Michelle Rowland MP, Minister for Communications, *Albanese Government acts to disrupt illegal text message scams,* 23 April 2023.
[29] ACMA, *The SMS Sender ID Registry*
[30] ACMA, *Action on Scams, Spam and Telemarketing January to March 2024*, 31 May 2024.
[31] DITRDCA, *SMS Sender ID Registry Fighting SMS Impersonation Scams*, 18 February 2024.
[32] *Telecommunications Amendment (SMS Sender ID Register) Bill 2024*

2.2.2 Objectives for scam prevention policy

Further government action is needed to make Australian consumers and small businesses harder targets for scammers. Australia needs the ecosystem targeted by scammers to be as robust as possible to prevent, detect, report, disrupt and respond to scam activity, and provide flexibility to adjust as scammers adapt to responses by authorities and exploit gaps in protections.

The government has two core objectives to address the rising impact of scams on the economy:

1) **Reduce scam harms**: Reduction of the rates of reported exposure and victimisation of consumers from scam activity occurring in sectors which are key vectors targeted by scammers. Success can be measured by a sustained reduction in the number and size of reported scam losses by consumers.
2) **Align benefits and costs of scam prevention**: Alignment of industry responses as appropriate to the presence of scam activity on platforms and services across the ecosystem. Greater symmetry and co-ordination of anti-scam responses will contribute to reducing the exposure of business activities open to exploitation by scammers. Success can be measured by reductions in scams taking place across services as opposed to an aggregate reduction in one area of the economy.

The government aims to facilitate improved outcomes against these core objectives through:

- Improvements to the consistency, quality, and timeliness of industry responses to scam activity. Uplift in scam prevention action across the ecosystem is required to minimise gaps in the responses and protections provided by businesses, with the weakest links in the ecosystem often exploited by scammers. The impact of actions would be measured through analysis of business practices and the quality of anti-scam policies, procedures, and resourcing.
- Greater levels of industry collaboration, reporting and information sharing between businesses and to regulators about scam activity. Information sharing improves the capability of parties in the scams ecosystem to quickly detect and disrupt scam activity as it arises or prevent similar activity by the same perpetrator. Collaboration would be measured through volume, quality, and use of reporting data.
- Increased accessibility and transparency of pathways for consumers to report and seek support when experiencing a scam. The impact of scams on consumers can be mitigated when they are able to quickly report scam activity and receive support through dispute resolution and redress arrangements. Improvements to consumer experience would be measured by factors, including timeframes, consumer satisfaction, and the outcomes of reporting and dispute resolution.

Government commitments have not set a timeframe for achievement of these objectives. However, the Government aims to reduce the impact of scams as a priority due to the unacceptably high losses experienced to scams in Australia. These objectives are in line with the aim of the NASC to make Australia the world's hardest

target for scammers by improving co-operation between government, industry and law enforcement to prevent scams and empower Australians to avoid scams.[33]

For more information about the objectives and evaluation of outcomes, see Appendix 3.

3. Policy options considered

Consistent with guidance from the Office of Impact Analysis (OIA) on election commitments, Treasury has considered two policy options. The options considered are:

- Option 1: Maintain the status quo.
- Option 2: Implement the Government's election commitment to introduce economy-wide, mandatory scams codes by establishing the Scams Prevention Framework (SPF).

Further industry-led initiatives have not been considered in this IA. While beneficial, existing industry-led actions are not capable of delivering consistent and co-ordinated ecosystem wide preventions for scam activity. Current voluntary codes do not deliver comprehensive coverage of the vectors of scam harms, and have limited ability to hold signatories to account creating gaps which can be exploited by scammers.

Mandatory and pre-determined bank liability is not considered in this IA because it is inconsistent with the policy problem of determining an appropriate sharing of responsibilities and incentivising a system-wide improvement in scam prevention. Compensation mechanisms that cover multiple sectors, not just banking, are considered in Option 2.

Additionally, a non-regulatory option has not been considered in this IA, as the government is separately implementing non-regulatory responses to the policy problem, including through the implementation of the NASC and a public awareness campaign.

3.1 Option 1 – Status quo

Without further government action, Australians will continue to rely predominately on voluntary responses by industry to combat scams. Those efforts would be complemented by existing Government initiatives introduced to address scams and the current regulatory oversight and enforcement powers of regulators relating to more general consumer or financial protections.

Protections in Australia for consumers and businesses would comprise of the following initiatives with limited reach to address and manage scam threats:

- the NASC in receiving scam intelligence and convening Fusion Cells to target solutions to emerging threats;
- ACCC/NASC and ASIC engaging with takedown providers to identify and taken down investment scams and phishing websites;

[33] NASC, *Quarterly Update, January to March 2024,* 21 May 2024

- the voluntary approaches of industry sectors, including the ABA/COBA Scam-Safe Accord and the DIGI Australian Online Scams Code;
- the SMS Sender ID Registry protecting participating sender IDs from impersonation;
- ACMA enforcing the *Reducing Scam Calls and Scam SMs* industry code; and
- existing non-targeted consumer protection regulatory and enforcement powers to respond where those laws have been breached.
- existing consumer dispute and ombudsman schemes for complaints in the telecommunications and banking industries.

There would be no change to the fragmented response to voluntary anti-scam activity, where the protections and outcomes for victims could differ greatly depending on the sectors involved in their specific scam experience and processes of their service providers. Industry would be engaged further by government where they offer to take voluntary actions to contribute to national anti-scam measures, such as expanded information sharing with the NASC.

3.2 Option 2 – Scams Prevention Framework

Under Option 2, the government would introduce new mandatory industry codes to outline the responsibilities of the private sector in relation to scam activity under an overarching SPF. If the entities in these industries fail to comply with their obligations, they may be subject to penalties or be liable to compensate consumers for losses experienced due to these failures.

A new framework that creates mandatory obligations for sectors targeted by scammers would provide appropriate guardrails to reduce the scam threat activity across key sectors and make Australia a less attractive target for scammers.

The introduction of an overarching regulatory framework, supported by sector-specific mandatory codes, will deliver the Government's 2022 election commitment of introducing tough, new mandatory industry codes for banks, telecommunication providers and social media companies to combat scams.[34]

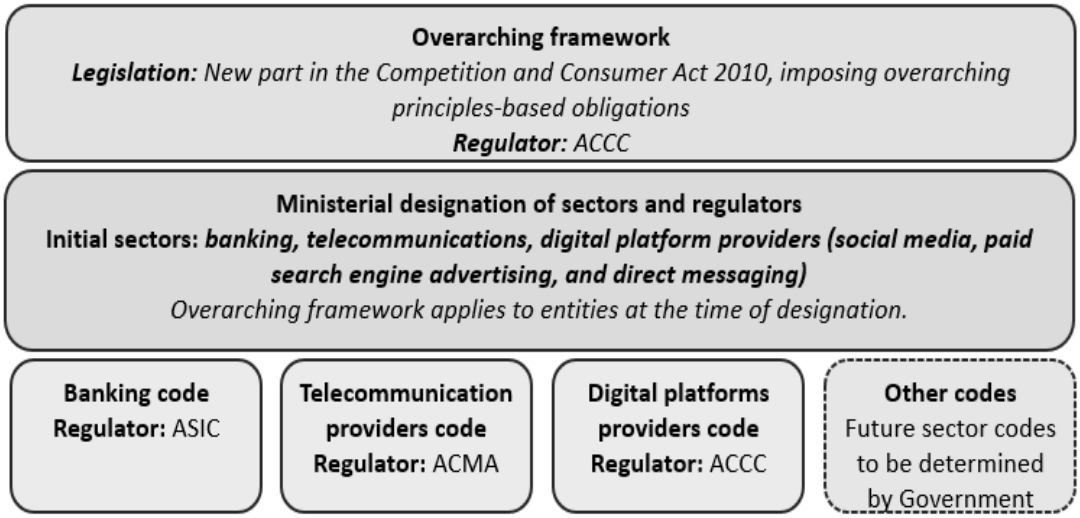
This option would have a two-tiered regulatory design that enables an overarching legislation of the SPF in the *Competition and Consumer Act 2010* and subordinate legislation to introduce sector-specific obligations (Figure 1). This option would promote a whole-of-ecosystem approach to scams by directly legislating minimum standards that are enforceable in the designated sectors where scammers are prevalent.

The SPF design will enable flexibility to designate additional sectors as future challenges arise. This approach will fulfil the Government's election commitment as it would enable the development and enforcement of sector specific codes on banks, telecommunication providers, and digital platform service providers, which at the

[34] The Hon Stephen Jones MP, Assistant Treasurer and Minister for Financial Services, *Fighting back against scammer scrouge – Government announces new anti-scams centre,* 15 May 2023

outset, would cover social media, direct messaging and paid search advertising services.

Figure 1 – The Scams Prevention Framework



Overarching framework

The SPF establishes an overarching framework to set principles-based obligations that would be adaptable to the various operating models of regulated businesses. The SPF would enable an increase in baseline requirements commensurate with the size and risk profile of the entity targeted by scams and allow for consideration of future sectors to be designated by government. The SPF would drive consistency in expectations and responses across sectors.

Under the SPF there would be 6 types of obligations for regulated entities:

- Prevent: Implementation of responsive anti-scam processes, procedures and/or systems, and make information available to consumers in relation to the steps they can take to minimise the risk of scams.
- Detect: Taking proactive steps to detect scam activity on its platform and/or service, and act in a timely manner on scam intelligence received to prevent further loss to impacted consumers.
- Disrupt: Taking proactive and timely steps to disrupt scam activity identified on its platform and/or service and share relevant scam intelligence with impacted consumers in a timely manner.
- Respond: Having an accessible mechanism for consumers to report a scam, an IDR mechanism for a consumer to make a complaint, and membership of the prescribed EDR scheme for their sector.
- Report: Sharing scam intelligence with a government regulator in real-time and responding to information requests from regulators within a specified timeframe. Government regulators would also be expected to share scam

intelligence with other entities, government agencies and people who may be able to respond to the scam activity.
- Governance: Documentation of policies and procedures for managing the risk of scams on their platform and/or service and regularly review their effectiveness against established performance metrics and targets.

IDR and EDR requirements would apply consistently across all designated entities. Where a consumer has experienced loss due to a scam, they would first approach a relevant regulated entity for redress through the entity's IDR mechanism. If a consumer complaint is not resolved or if the consumer is not satisfied with the outcome at the IDR stage, they will have an option to escalate their complaint to EDR. All entities that provide a service that is regulated by the SPF would be required to become a member of an authorised EDR scheme. An EDR mechanism would provide pathways for redress (including compensation) where regulated entities have not met their SPF obligations. AFCA would become the single EDR body for the three sectors initially designated under the SPF. Consumers would be able to raise scam complaints related to banks, telecommunication providers and certain digital platforms, ensuring a holistic 'no wrong door' approach to seek redress.

The SPF would also establish a network for reporting intelligence to protect against scams. By requiring entities which detect scam activities to share information with a government regulator, and establishing systems for such intelligence to be shared with relevant entities across the scam ecosystem; anti-scam activities can be coordinated across multiple entities, industry sectors and potentially with international partners.

Certain requirements around scam disruption and response action will be framed as principles-based obligations, leaving open the potential for more prescriptive details in sector-specific codes.

The SPF would introduce a responsive and adaptable framework that allows the Government, industry and regulators to respond to changes in scam activity in the economy, by allowing for additional sectors or services of the economy to be regulated, and for sector-specific codes to be made and enforced for that sector.

Mandatory sector-specific codes

In addition to the principles-based obligations, the SPF would introduce mandatory sector-specific codes, setting out more specific obligations for each sector.

Sector-specific codes would ensure measures are appropriate for each industry, as well as providing flexibility for obligations to be developed in further detail as scams evolve. This design is intended to enable rapid response to evolving scam patterns, without requiring changes to the primary law.

Sector-specific codes may incorporate prescriptive expectations on businesses to:

- Document policies and procedures setting out their approach to managing scam-related risks in their business;
- Comply with certain obligations related to IDR and EDR, including timeframes for response to consumer complaints at the IDR level, and

cooperating and providing reasonable assistance to the prescribed EDR scheme; and
- Act on scam intelligence, supported by guidance on the actions expected of businesses.

The mandatory sector-specific codes will initially apply to sectors designated to be covered under the SPF (banks, telecommunication providers and digital platform service providers). Consideration of designating additional sectors and introducing sector-specific codes would be available under the proposed SPF model where there is a constitutional basis to do so.

4. Net benefit of each option

The net benefit of each option is assessed through analysis of expected:

- Regulatory costs Regulatory costs incurred by:
  - Banks
  - Telecommunication providers
  - Digital platforms
  - Consumers
- Government costs
- Benefits of:
  - Reducing exposure to scams
  - Reducing scam losses
  - Improving redress for victims of scam losses

The net benefit of options 2 has been assessed using a break-even analysis. This method is chosen as the benefits of each policy option are highly uncertain and not fully unquantifiable.

The following evaluation establishes the threshold break-even level of reduction in scam losses required to achieve a net benefit, considering the expected costs of each option. Although there are other monetary and non-monetary benefits from reducing scam harms (see section Scams inflict a broad range of harms), the dollar amount of losses to scams is a clear measure of the level of benefit related to each option.

The likely effectiveness of each option reducing scam losses to outweigh its overall costs is assessed to establish which option would achieve the greatest net benefit. Expected change in the volume of amounts reimbursed to scam victims from relevant entities has not been considered as the primary objective of anti-scam actions and are not considered as benefits or costs of each option. The dollar amounts paid as reimbursements are equally a benefit to victims and a cost to regulated entities.[35]

As quantification of the benefits of anti-scam activities is not possible a cost-benefit analysis is not appropriate in this case. As policy options 2 would be an innovative approach to strengthening protections from scam activity, there is a lack of evidence on the level to which these approaches would be effective.

[35] These payments represent a transfer of monies between entities and consumers rather than a benefit to society overall.

The broad reach of benefits, including non-monetary impacts in areas like consumer confidence or businesses' reputational damage, also means it is not possible to make a quantitative assessment of all benefits. Benefits would apply to a diverse group of Australian society, including individual consumers, sectors in the scams ecosystem and legitimate businesses at risk of impersonation. These broader benefits would be result from improvements in the 3 types of benefit assessed.

Details of the assumptions used in calculations of regulatory costs are included in **Appendix 2 – Regulatory cost calculations**.

4.1 Regulatory costs

4.1.1 Banks

Option 1 – Status quo

Under the status quo, banks would maintain current commitments to address scams on their services, including implementation of the Scam-Safe Accord.

Banks currently dedicate significant resourcing to fraud prevention and account verification activities. In recent years, individual banks have introduced measures in response to the rising impact of scams, including new measures to detect scams, verify accounts, and share and receive intelligence. An overview of current sector uplift across various banking sector initiatives is provided below at Table 3**.**

Most domestic banks are members of industry associations ABA and COBA, who have co-ordinated sector-wide commitments under the Scam-Safe Accord to commit members to anti-scam measures. The Scam-Safe Accord includes a confirmation of payee system with an industry-estimated cost to the sector of $100 million.[36] More information on the Scam-Safe Accord and relevant commitments for banking sector members is at **Appendix 1**.

Table 3 – Banking sector initiatives

Activities	Examples of sector initiatives
Detection measures	Some banks have announced the use of new technologies, including artificial intelligence, to detect suspicious and unusual behaviour on its platforms and use analytics to predict the risk level of potential scam activity, including a *Scam Scoring* model announced by ANZ in April 2024.
Payee verification	Some banks have announced additional checks and warnings for payments, including account name matching measures including CommBank *NameCheck* and Westpac *Verify* initiatives in March 2023.

[36] Australian Banking Association, *Banks unite to declare war on scammers*, 24 November 2023.

Activities	Examples of sector initiatives
High-risk transaction controls	Banks have announced a series of new holds, declines and limits on high-risk transactions, including changes for payments to high-risk cryptocurrency exchanges announced by all major banks over 2023-24.
Caller identification and verification	Some banks have announced in-app communications and partnered with telecommunications providers to verify bank calls, including CommBank *CallerCheck* in February 2023 *and Westpac Safecall* in July 2024.

Under status quo arrangements, industry voluntary information sharing arrangements will continue to develop, with all Scam-Safe Accord signatories committing to join the AFCX. In May 2023, the ABA reported that 14 of its 20 members were, or were in the process of, entering membership with the Fraud Reporting Exchange of the AFCX. Under the Scam-Safe Accord, participating banks committed to join the AFCX by mid-2024 and its Fraud Reporting Exchange over 2024-25.

Banks play a pivotal role in economy-wide information sharing arrangements and have developed more standardised sets of data and processes compared to other sectors. However, banks have less visibility of intelligence relating to contact or communication methods for scams beyond self-reported information from consumers, which is highly useful for early identification.

Under the status quo, banks would be subject to existing requirements to have appropriate IDR mechanisms in place and be a member of AFCA. Both of these obligations are set out in section 912A of the *Corporations Act 2001*. However, certain branches of foreign-owned authorised deposit-taking institutions (ADIs) that generally service wholesale clients and ADIs that provides services to industry (e.g. the Australian Settlements Ltd) do not hold an AFCA membership.

Being a member of AFCA includes paying AFCA's annual membership fee (~$389 for FY 2024-25), complaint handling fees and an annual proportionate user charge that is calculated based on prior year's AFCA dispute handling data. AFCA does not charge for the first five complaints against a member in a financial year. After that, the complaint handling fees vary on a case-by-case basis, depending on the stage the complaint is closed. Under status quo, AFCA would maintain its current jurisdiction as the EDR scheme for financial sector firms, including in relation to complaints involving scams.

Option 2 – Scams Prevention Framework

The impact of the SPF on the banking sector would result in a consistent standard of measures to prevent, detect, report, disrupt, and respond to scams additional to voluntary commitments or industry self-regulation. The uplift approach to the initial SPF would see the most changes in its capture of banks that do not participate in or meet current industry standards relating to scams as all businesses would be mandated to adopt new policies and procedures.

Under the SPF, the banking sector may be required to undertake additional activities to demonstrate compliance with its principles-based obligations, including the following:

- **Prevention activities**, including the design of appropriate banking in-app communications and warnings to consumers to reduce the risk that consumers will be exposed to a scam attempt.
- **Detection activities**, including information sharing and improving responsiveness to trace and action credible intelligence from consumer and industry reports of reasonably suspected scam activity.
- **Disruption activities**, including ensuring appropriate frictions are in place for transactions reasonably at risk of being a scam, which may include placing holds, delays and limits on accounts or transactions.

To document and review these activities, banks would also have overarching governance obligations to develop and implement governance policies, procedures, metrics and targets to combat scams. Whilst compliance costs for industry to perform governance obligations will vary based on the maturity of existing internal governance arrangements. Most banks have or have already voluntarily committed to implementing anti-scam activities under the Scam-Safe Accord, reducing the anticipated impacts.

Assuming existing strategies are in place, governance impacts additional to status quo governance activities may include capability and staffing to ensure the following functions can be performed:

- annual review of anti-scam policies and procedures by a senior officer within the entity,
- maintenance and record-keeping of documents relating to anti-scam policies and procedures,
- drafting and publication of information on how businesses are protecting consumers, as well as ensuring information is available to consumers on rights and available complaints avenues.

Information sharing requirements would create additional impacts relevant to new policies and procedures relating to escalating actionable scam intelligence. However, the costs of these arrangements are mitigated due to existing Accord banking sector commitments to join in the AFCX.

The extent to which banks would be required to incur additional costs is mitigated by the considerable extent of independent and self-regulated activity in the sector, and parallel regulatory obligations for similar harms, including those relating to money laundering offences covered under the *Anti-Money Laundering and Counter Terrorism Financing Act*.

The SPF will capture businesses in the banking sector by designating all ADIs overseen by the Australian Prudential Regulation Authority (APRA). As outlined in Table 4, this would capture some businesses that are and are not a member of industry bodies and would potentially be subject to additional obligations. Depending on the

size and complexity of these entities, regulatory capture may impose expectations for new activities and associated costs.

It is expected that the implementation of SPF obligations and associated costs will differ depending on the size and complexity of the entity. As of June 2024, APRA monitors 126 ADIs. Of the $1.469 trillion in deposits managed by these ADIs, 73 per cent are held by the major four banks.[37] The remainder of deposit-taking activity in Australia is managed by a range of smaller entities: including medium-sized banks, credit unions, building societies and neobanks, each with a variable customer base, resourcing and presence in the Australian financial system.

Table 4 – Potential regulated entities under the Banking Code[38]

REGULATED SECTOR	POTENTIAL KNOWN ENTITIES	EXAMPLES	INDUSTRY REPRESENTATION
BANKS **DEFINED AS *AUTHORISED DEPOSIT-TAKING INSTITUTIONS***	**4** major banks	ANZ Banking Group, Commonwealth Bank of Australia	All **4** are members of ABA
	73 other domestic banks, credit unions, building societies and neobanks	Bendigo and Adelaide Bank, Newcastle Permanent Building Society	**64** are members of ABA or COBA
	7 Australian subsidiaries of foreign-owned banks	Bank of China (Australia), HSBC Bank Australia	**6** are members of ABA
	48 Australian branches of foreign-owned banks	Citibank, ING Bank	**2** are members or have subsidiaries that are members of ABA

The SPF would also impose obligations on regulated entities to have in place an accessible and transparent IDR mechanism for consumers to make complaints in relation to scams, and to be a member of a prescribed EDR scheme. AFCA would operate a single EDR scheme for scam complaints in relation to the three initial sectors subject to the Framework.

[37] APRA, *Monthly Authorised Deposit-Taking Institution Statistics Table 4, Deposits on Australian books of selected individual ADIs* (June 2024)

[38] Further details in Appendix 2. This list is illustrative and is not intended to represent the intended scope of the definitions for the designation of these services, which would require further development after the SPF is legislated. Providers of purchased payment facilities and restricted ADIs have been assumed to be out of scope of SPF obligations.

As indicated above, banks are already required to have appropriate IDR mechanisms in place, and most are a member of AFCA under section 912A of the *Corporations Act 2001*. The SPF requirement to be a member of AFCA would apply to all ADIs, including those that might not have existing membership with AFCA (such as branches of foreign-owned banks). This is because these entities could also be involved in a scam and their customers are not invulnerable to the threat of a scam. The number of scams complaints requiring EDR would be expected to increase initially because of improved complaints procedures and uplifted obligations resulting in greater benefit to consumers from taking complaints to AFCA. However, the number of complaints is likely to fall as the rate of scam victimisation reduces because of the SPF.

Areas where there would be uplift beyond current initiatives of entities in the banking sector are summarised in Table 5.

Table 5 – Banking sector initiatives and uplift required for the Scams Prevention Framework

Obligation	Current initiatives	Uplift required
Anti-scam activity	Voluntary Scam-Safe Accord standards for ABA and COBA members	Anti-scam activity improvements, governance operations
Information sharing and reporting	ABA/COBA members committed to participation in AFCX	Higher standards of information sharing would be required, including beyond the banking sector
Dispute resolution	AFCA membership and IDR requirements for consumer banking	Likely increase in complaints, required membership of AFCA for branches of foreign banks

As outlined in Table 6, the estimated regulatory costs of Option 2 additional to the status quo for the banking sector would be $100.9 million in the initial year, and $31.8 million on an ongoing basis each following year. Most of this regulatory cost would be on banks which are not affiliated with the ABA or COBA, which would be required to invest in capabilities to meet the Scam-Safe Accord level of anti-scam activity and additional requirements of the proposed option. However, there would also be a need for investment in improvement of capabilities for Scam-Safe Accord signatories. While almost all ADIs are members of AFCA, banking EDR costs are expected to increase due to an initially increased number of scam complaints each year.

Table 6 – Option 2 Estimated annual regulatory burden on banks ($m)

Entity type	Entities	Initial cost	Ongoing cost
Major banks	4	$6.2	$1.0
Other ABA/COBA	72	$22.9	$2.7
Non-affiliated/AFCA	40	$51.1	$20.0
Non-affiliated/non-AFCA	16	$20.6	$8.1
Total	**132**	$100.9	$31.8

4.1.2 Telecommunication providers

Option 1 – Status quo

Telecommunications providers are already subject to mandatory obligations under their existing industry code. The 2022 *Reducing Scam Calls and Scam SMs* industry code requires telecommunications providers to:

- provide up-to-date guidance for consumers on how to manage and report scam calls and texts;
- monitor, identify, trace and block phone calls and SMS from recognised scammers; and
- report identified scam calls and SMS to the ACMA and any involved telecommunications providers.

These actions demonstrate providers have the infrastructure and are responding to existing expectations that businesses in the sector lift consumer protections.

Information sharing arrangements in the telecommunication sector are progressing. Major telecommunications providers participate in the AFCX Intel Loop. The AFCX has expressed interest in expanding inclusion of non-banking sector entities such as the telecommunications and payments system providers, with Optus and Australian Payments Plus already AFCX members. In July 2023, Optus announced its Call Stop technology to automatically block calls to scam numbers, linking to intelligence gained in partnership with the banking sector and AFCX.[39]

Telecommunications providers would maintain their existing mechanisms in relation to IDR and EDR, which includes compliance with complaints handling requirements under the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018* and membership with the TIO. The TIO receives and manages all complaints in relation to the telecommunications sector, including scam complaints.

Option 2 – Scams Prevention Framework

Under Option 2, there are unlikely to be significant additional costs for telecommunications providers who are compliant with current obligations. Actions previously taken or planned to be taken to implement anti-scam activities in response

[39] Optus, *Optus Call Stop to fight off SMS scams*, 17 July 2023.

to *Reducing Scam Calls and Scam SMs* industry code obligations would mitigate the costs required for meeting the SPF's regulatory requirements.

All telecommunication providers would have additional governance obligations to document and review their anti-scam activity, as detailed in the section for banks. Although the industry does not have an explicit sector-wide commitment to specific governance activities related to scams, impacts are similarly likely to be variable and mitigated by existing governance activities.

Telecommunications providers would need to invest in their capabilities to share scam information potentially more frequently and in new formats. This burden would be mitigated by the current capabilities required to share data with ACMA and other providers under the *Reducing Scam Calls and Scam SMs* and involvement by the major telcos in AFCX.

Telecommunication service providers would largely be able to leverage existing complaints handling processes to meet IDR requirements under the SPF. In relation to EDR, telecommunication service providers would be required to join an AFCA-led single EDR scheme for the purposes of scam complaints, in addition to maintaining their existing required membership with the TIO for non-scam complaints.

The requirement to join AFCA would also apply to transit carriers and carriage service providers (CSPs) that may currently be exempt from the requirement to join TIO because they do not have individual or small business customers. This is because transit carriers and CSPs could be responsible for carrying scam calls and texts between two providers prior to reaching a consumer.

Under Option 2, most telecommunication service providers would be required to maintain membership of two EDR schemes – TIO and AFCA. In addition to costs associated with TIO's EDR process under the status quo, telecommunication service providers would incur costs to join and participate in AFCA's EDR processes.

Areas where there would be uplift required additional to current initiatives of entities in the telecommunications sector are summarised in Table 7*Table 7 – Telecommunications sector initiatives and uplift required for Scams Prevention Framework Table 7*.

Table 7 – Telecommunications sector initiatives and uplift required for Scams Prevention Framework

Obligation	Current initiatives	Uplift required
Anti-scam activities	Mandatory *Reducing Scam Calls and SMs* Code obligations	Mainly new governance processes, and possible uplift in obligations
Information sharing and reporting	AFCX for major telcos, sharing with ACMA under *Reducing Scam Calls and SMs* Code	Higher standards of information sharing would be required, including across sectors
Dispute resolution	TIO membership and IDR requirements, except for transit carriers and CSPs	AFCA membership, likely increase in complaints

As outlined in Table 8, the estimated additional regulatory costs of Option 2 for the telecommunications sector would be $22.0 million in the initial year, and $14.1 million on an ongoing basis each following year. There would be a need for investment to comply with new governance, information sharing and EDR arrangements. There would also be costs associated with an increased number of scam complaints each year, with a higher level of fees required by AFCA.

Table 8 – Option 2 Estimated annual regulatory burden on telecommunications providers ($m)

Entity type	Entities	Initial cost	Ongoing cost
Major telcos	4	$5.4	$4.5
Medium CSPs	18	$1.8	$1.4
Small CSPs	150	$5.2	$2.8
Very small CSPs	241	$8.3	$4.6
Transit carriers / CSPs[40]	32	$1.3	$0.8
Total	**445**	**$22.0**	**$14.1**

4.1.3 Digital platforms

Option 1 – Status quo

Some major digital platforms in Australia have agreed to voluntary measures to address online scams through the AOSC. DIGI, the industry body representing the digital industry in Australia, has voluntary industry anti-scams standards and is developing internal dispute standards in response to a request from the government.

[40] Transit carriers/CSPs are included in this entity type category, and not under the other categories above.

Under the status quo the AOSC would see a voluntary uplift in anti-scam activities in signatory digital platforms. It would encourage progress on anti-scam measures including verification measures for advertisers, mechanisms for user reporting of scam content, and agreements to co-ordinate actions with the NASC.

As a voluntary code, industry actions are not enforceable and there are no obligations if signatories fail to meet commitments under the AOSC. Other observed limitations to the application of the AOSC include that:

- There are no defined timelines for full implementation of commitments or details on how DIGI will monitor and evaluate the effectiveness of actions taken by signatories to consider compliance with the AOSC, beyond processes for AOSC review and amendment.
- The AOSC contains principles limited by other terms of use, policies or conduct rules of the entity. Whilst signatories are also committed to address initiating scams in these instruments, it gives latitude to industry to define what content would attract the operation of the AOSC.

Information sharing arrangements across industry to address scams in Australia is nascent, with some digital platform membership of the AFCX and Intel Loop. The AOSC provides a general commitment to work with relevant stakeholders to share information and respond to information requests with Government agencies, law enforcement and industry. However, due to limited details on these commitments including specifics on the nature of collaboration and information sharing, the AOSC may leave inconsistent ways in which digital platforms are interacting with them.

While options for a mandatory IDR and EDR regime for digital platforms are being developed for future consideration by Government, currently the sector is not subject to any such mechanisms. As a result, the status quo options would leave consumers with limited options to seek support or redress from digital platforms where they have been subject to a scam on their service.

Option 2 – Scams Prevention Framework

The SPF would designate digital platform services, initially offering social media, direct messaging and paid search advertising services, comply with principles-based obligations. A snapshot of potentially regulated digital platforms is outlined in Table 9.[41]

[41] Further detail on assumptions used to estimate the number of relevant services is included in Appendix 2 – Regulatory cost calculations.

Table 9 – Potential regulated digital platform services[42]

KNOWN SERVICES	EXAMPLES
~10 SOCIAL MEDIA SERVICES	Facebook, Instagram, YouTube, TikTok, Pinterest, Twitter, Reddit, LinkedIn, BeReal
~19 DIRECT MESSAGING SERVICES	Facebook Messenger, WhatsApp, SnapChat, Signal, iMessage, Zoom, Slack, Discord, WeChat
~2 PAID SEARCH ADVERTISING SERVICES	Google Search, Bing Search

Due to the broad range of regulated services in this sector, and that sector-wide action to combat scams has not been as co-ordinated to-date as in other sectors, greater uplift can be expected to meet compliance with the SPF. Whilst the voluntary AOSC would encourage the uplift of anti-scam activities in relation to services covered by the AOSC that are offered by the signatories, the SPF would mandate a stronger uplift to address scam activity in designated services provided by digital platforms. In addition to general obligations relating to governance and information sharing, businesses may undertake the following actions to demonstrate compliance with the SPF:

- **Prevention activities**, including greater verification of user accounts, and clear information and warnings to service users about scam activity and providing users with the options to manage their exposure to content at a higher risk of being a scam, such as receiving messages from unknown accounts.
- **Detection activities**, including the use of appropriate tools and technologies to proactively identify accounts, content and advertisements that are likely to be associated with scam activity.
- **Disruption activities**, involving greater content moderation including suspension of accounts, content and advertisements reported by users, other entities, and regulators, and removing those accounts and content within a reasonable period if verified as a scam.
- **Responses to scams**, including to have an accessible mechanism for consumers to report scams, an accessible and transparent IDR mechanism and membership of an EDR scheme.

Under Option 2, designated digital platforms would be required to have in place an IDR mechanism that is accessible and transparent for users, and comply with any requirements related to IDR set out in the sector codes (including timeframes for response to a consumer complaint). Designated digital platforms would be required to become a member of AFCA if they are providing a service that is regulated by the SPF.

Areas where there would be uplift required additional to current initiatives of entities in the digital platforms sector are summarised in Table 10.

[42] This list is illustrative and is not intended to represent the intended scope of the definitions for the designation of these services, which would require further development after the SPF is legislated. These definitions would involve further consultation before designation of the sector by the Minister.

Table 10 – Digital platforms sector initiatives and uplift required for Scams Prevention Framework

Obligation	Current initiatives for AOSC signatories	Uplift required
Anti-scam activities	Voluntary AOSC commitments to develop internal anti-scams strategy and procedures	Develop anti-scams activities, with oversight and governance measures for continuous improvement
Information sharing and reporting	Commitments to share information and respond to requests under the AOSC and engage with the NASC	Higher standards of information sharing would be required, including with other sectors
Dispute resolution	No mandatory requirements	Accessible and transparent IDR mechanism available to consumers and AFCA membership

As outlined in Table 11, the estimated regulatory costs of Option 2 additional to the status quo for the digital platforms would be $106.0 million in the initial year, and $42.1 million on an ongoing basis each following year. Most of this regulatory cost burden would be on the major digital platforms offering social media, paid search advertising and direct messaging services. Digital platforms would be required to undertake investment in anti-scam activities to comply with new obligations under the SPF, beyond activities committed to under the AOSC including governance, information sharing, IDR and EDR arrangements. Digital platforms which are not signatories to the AOSC would be expected to incur a higher level of costs to implement anti-scam activity improvements.

Table 11 – Option 2 Estimated annual regulatory burden on digital platforms ($m)

Entity type	Entities	Initial costs	Ongoing costs
Major platforms - AOSC	5	$43.7	$16.8
Major platforms - non-AOSC	2	$21.8	$9.6
Medium platforms - AOSC	2	$5.0	$1.8
Medium platforms - non-AOSC	12	$35.4	$14.0
Total	**21**	$106.0	$42.1

4.1.4 Consumers

Consumers need to engage with new or changed processes that entities often introduce in their services to strengthen protections from scams.

These processes, referred to as frictions, are intended to make services safer or slow the pace of services to make it more difficult for scammers to succeed in causing harm to consumers. For example, for the banking sector frictions involve the use of limits, holds, and delays to reduce risk in transactions, including those to new payees. For digital platforms, such similar process which create frictions for consumers could include account holder verification, two-factor account identification and delays in sending messages, posting advertisements or social media content.

There are known inconveniences and issues regarding frictions as not all consumers will perceive the value or benefit of the friction. These frictions can create costs for doing business through the introduction of inconvenience and delays in using regulated services or platforms, including administrative impost for users and may reduce the efficiency of urgent digital interactions. However, survey responses from Treasury and Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA)'s public consultation and industry sentiment suggests that consumers may be willing to accept additional frictions in order to be better protected from scams.

Option 1 – Status quo

Under the status quo, the accountability for scam activity would fall inequitably across the scam ecosystem with banks and payment providers (the point where the financial loss is most frequently recognised) giving rise to greater risk-aversion in undertaking banking with customers or introducing more excessive frictions in their consumer services.

Absent clear obligations or controls, entities may use measures at their disposal to mitigate risks in ways undesirable to consumers in terms of access to and efficiency of their services more generally, but particularly in banking services. This may involve banking and other services imposing higher costs on higher risk consumers and businesses, including additional fees and in some cases stricter limitations on service offerings.

Option 2 – Scams Prevention Framework

The costs on consumers of frictions may increase due to entities uplifting their anti-scam activities to comply with their SPF obligations under option 2. Such anti-scam actions may result in additional time, cost, resources and effort required to use services of banks, telecommunications providers and digital platforms. However, the relative impact compared to frictions expected under the status quo is uncertain and difficult to quantify.

Frictions may be affected in each sector as follows:

- In banking services there could be minimal impact given the prominence of existing anti-scam measures. In comparison to the status quo option 2 may lead to either an increase or reduction in prominence of frictions; as a result of

clearer accountability and coordination across the ecosystem altering the need for delays and verification in banking activities.
- In telecommunications services there may only be minor impacts on consumers compliance costs given the current and planned levels of anti-scam actions.
- For digital platform services in social media, paid search advertising and direct messaging there may be a greater level of frictions for consumers, potentially relating to obligations to improve identification verification processes or user verification requirements on platforms which do not currently have these in place.

Many services which would be directly regulated by the SPF such as digital platforms and bank transaction accounts do not involve direct prices on consumers. Regulated entities may pass on a share of the costs of complying with increased regulation potentially through higher consumer prices or onto other users of the service such as businesses. As costs would be spread across various entities and industries the overall effect on prices experienced by consumers may be negligible, and outweighed by lower burden on consumers to engage in their own administrative or external security measures to help them avoid falling victim to a scam.

Given the high level of uncertainty over whether the net change in consumer costs would be an increased or decreased burden, they are assumed to be negligible under option 2.

Under option 2, consistent with status quo, consumers would not be charged any fees for taking their scam complaints to AFCA and would not incur costs for EDR.

4.1.5 Overall regulatory costs

Option 1 – Status quo

As Option 1 represents the status quo it does not involve additional regulatory costs relative to current commitments across industry.

Option 2 – Scams Prevention Framework

In the initial year implementing Option 2 would involve $228.8 million in regulatory costs including $100.9 million for banks, $22.0 million for telecommunications providers and $106.0 million for digital platforms. Each following year ongoing these regulated entities would incur $88.0 million of regulatory costs including $31.8 million for banks, $14.1 million for telecommunications providers and $42.1 million for digital platforms.

Table *12* outlines the overall regulatory costs expected to be involved in implementation of Option 2. On average over the first 10 years industry would be expected to incur $102.1 million in annual regulatory costs across the 3 sectors

designated under the SPF (($228.8 million + 9 x $88.0 million)/10). Individuals and community organisations would not be expected to incur a net change in costs as these impacts are assumed to be negligible.

Regulatory burden estimate (RBE) table

Table 12 – Annual regulatory costs (from business as usual) over first 10 years of implementation

Change in costs ($ million)	Business	Community organisations	Individuals	Total change in costs
Total, by sector	$102.1	Nil	Nil	$102.1

4.2 Government costs

Option 1 – Status quo

As Option 1 represents the status quo it does not involve additional costs for government relative to the current arrangements. However, from the government's perspective, as the scams problem grows, the resources required to address issue at a later point in time will also grow.

Option 2 – Scams Prevention Framework

As announced in the 2024-25 Budget, the government would provide $37.3 million for the introduction of mandatory industry codes to be established under a SPF over four years from 2024–25.[43] This includes $8.6 million per year ongoing for government regulators to administer and enforce mandatory industry codes for regulated businesses to address scams on their platforms and services, initially targeting telecommunications, banks and digital platforms services relating to social media, paid search engine advertising and direct messaging.[44]

To implement a single EDR scheme for scam disputes for the three initial regulated sectors under the SPF would involve seed funding of $14.7 million over two years from 2024-25 for AFCA to expand its jurisdiction and establish its capacity to handle SPF disputes. There would no ongoing government costs. Once established, AFCA would recover its operating costs from its members.

[43] Treasury (2024) Budget 2024-25 Paper 2, Part 2: Payment Measures, Page 180

[44] Prior expenditure announced in the Budget 2023-24 for Fighting Scams (Budget Paper 2, page 211) included "$58 million over years from $86.5 million to establish the NASC within the ACCC to improve scam data sharing across government and the private sector and to establish public-private sector Fusion Cells to target specific scam issues." Although this prior investment would facilitate information sharing and coordination activities under the SPF, these activities are not wholly dependent on the SPF being implemented and therefore not calculated as a direct government cost related to implementing the SPF.

As outlined in Table 13, government costs for the initial year would be $26.2 million for establishing the SPF and AFCA's expanded jurisdiction, followed by $8.6 million each year to administer the SPF.

Table 13 – Annual government costs ($ millions)

	Initial	Ongoing
Administering and enforcing SPF obligations	$11.5	$8.6
AFCA – establish single EDR scheme for 3 initial sectors[45]	$14.7	$0.0
Total	**$26.2**	**$8.6**

4.3 Benefits

4.3.1 Reducing exposure to scams

Option 1 – Status quo

There would be two key factors limiting future reductions in exposure to scams under the status quo policy settings: lack of clear industry obligations and lack of co-ordination across the economy.

Option 2 – Scams Prevention Framework

Clear obligations on regulated entities

The primary objective of the SPF is to set clear roles and responsibilities for the Government, regulators, and the private sector in combatting scams. The key benefit of the SPF is that mandatory and consistent standards across industry sectors will uplift anti-scam activities and in turn reduce exposure to scams for consumers.

Uplifting these anti-scam activities to a consistent standard across the designated sectors of banking, telecommunications and digital platforms would result in more consistent consumer protections across the Australian economy. This would result in lower frequency of scam activity reaching consumers and reduced losses to scams, as has been demonstrated by industry activities including:

- Under the Reducing Scam Calls and Scam SMs industry code telecommunications providers have blocked 1.5 billion scam calls and 668 million scam SMS between July 2022 and June 2024.[46]
- Google reported blocking or removing 206.5 million advertisements which violated their misrepresentation policy in 2023, including many scams.[47]

[45] AFCA will receive $14.7 million over two years from 2024-25. That is, $5.2 million in 2024-25 and $9.2 in 2025-26.
[46] Calculated from ACMA's "Action on telco consumer protection" quarterly reports from the July to September 2022 to April to June 2024.
[47] Google 2023 Ads Safety Report, 27 March 2024

- Meta conducted a targeted search for scam investment ads in July 2024 which resulted in nearly 20,000 such scam ads being identified and removed.[48]

Ensuring consistency across the sectors in which scams operate would also reduce the potential movement of scam activity to other sectors. The use of mandatory obligations would deliver a benefit over the status quo as there are recognised gaps in existing anti-scam policies and procedures.[49]

Coordination of anti-scam actions

The SPF would enhance information sharing arrangements to enable more efficient and timely sharing of information critical to support government regulators and industry to effectively protect consumers against scams. Sharing information would enable regulators and businesses to act quickly to prevent and disrupt the scam occurring, to mitigate the impact of the scam and/or prevent future scams. This would also include information sharing with law enforcement and government agencies via the government regulator.

For example, the SPF would enable a bank that is notified it has facilitated the transfer of funds through a scam into an account at another bank to report details about both the sending and receiving account holders to the regulator. The information would then be provided to other regulated entities so that prompt action can be taken to disrupt other transfers to the scammers receiving account and attempt to recover the funds. Sharing scam information across the ecosystem could also enable a social media service provider to quickly remove an advertisement or suspend an account suspected to be associated with scam activity reported by the bank to prevent further consumers from being impacted.

These capabilities would build on other coordination activities which have been effective in reducing scam exposure, including the following:

- ASIC's website takedown service has worked with other government agencies and industry to coordinate the removal of over 5,530 fake investment platform scams, 1,065 phishing scam hyperlinks and 615 cryptocurrency investment scams between July 2023 and August 2024.[50]
- The Optus 'Call Stop' program targets call back scams by diverting calls to scam phone numbers identified by banks and their customers, operated through the AFCX.[51]
- The NASC investment scam Fusion Cell brought together 43 organisations to identify and block investment scams including banks, social media platforms, payment platforms, trading platforms, investment services, telecommunications providers and government agencies. Between August 2023 and February 2024, the Fusion Cell's information sharing activity resulted in 1,000 instances of scam advertisements, advertorials, and videos

[48] Meta's Submission on the Scams Prevention Framework Bill 2024, 4 October 2024.
[49] An outline of these identified gaps in regulator investigations into industry practices in the banking and digital platforms sector is included in **Appendix 1.**
[50] ASIC, *Online investment trading scams top ASIC's website takedown action,* 19 August 2024.
[51] Optus, *Optus Call Stop to fight off SMS scams,* 17 July 2023.

being removed by digital platforms, takedown of 220 scam websites and diversion of 113 call back scams.[52]

- Between April and May 2024 Meta engaged in an intelligence sharing initiative with the banking industry through the Fraud Intelligence Reciprocal Exchange, via the AFCX. Meta was able to act on 102 scam reports to conduct a wider investigation, resulting in the removal of over 9,000 pages and over 8,000 AI-generated celeb-bait scams.[53]

4.3.2 Reducing scam losses

Option 1 – Status quo

Inaction from Government to close gaps in the ecosystem targeted by scams would continue to expose Australians to vulnerabilities and high volumes of scam activity and resulting financial, psychological and social detriment.

Option 2 – Scams Prevention Framework

Reducing exposure to scams under option 2 would result in reduced scam losses. In addition to the benefit of Option 2 in reducing exposure to scams resulting in reduced losses to scams, there are particular actions related to the SPF principles which would result in lower amounts being lost to scams once a consumer has been exposed to a scam or a scam is underway. Option 2 would uplift the capability of regulated entities across the chain of services involved in a scam, improving the likelihood scam activity can be prevented, disrupted and potentially amounts recovered. This would result in reduced losses in the Australian economy.

There is evidence that uplifts to anti-scam activities consistent with potential obligations under the SPF have resulted in measurable benefits to industry and consumers, indicating that creating consistent standards for these uplifts in capacity through mandatory obligations would result in further reductions in scam losses. In the banking sector, major banks have announced that their existing measures have diverted millions of dollars from being lost to scams and fraud.[54] Table 14 outlines a summary of reported scams losses prevented due to anti-scam activities in the banking sector.

[52] NASC, Investment scam fusion cell, Final report, May 2024.
[53] Meta, *Meta partners with the Australian Financial Crimes Exchange (AFCX) and Australian banking sector to combat scams,* October 2024. https://medium.com/meta-australia-policy-blog/meta-partners-with-the-australian-financial-crimes-exchange-afcx-and-australian-banking-sector-to-7b7b26227360
[54] ANZ, *The price of security is vigilance,* 2023; Commonwealth Bank, *Annual Report 2023*

Table 14 - Reported banking sector savings due to disruption of payments to scammers

Bank	Measure	Description	Value
ANZ	Overall	Jan 2023 – Oct 2023	$100-120 million[55]
Bendigo Bank	Blocks	2022 – 2023	$39 million[56]
Commonwealth Bank	Customer verification	Mar 2023 – May 2023	$11 million[57]
NAB	Overall	Jan 2023 – Apr 2023	$270 million[58]
Westpac	Blocks	Jan 2022 – May 2023	$131,000[59]
Westpac	Customer verification	Mar 2022 – May 2023	$250,000[60]

As an example, the Commonwealth Bank introduced a NameCheck confirmation of payee system in February 2023[61] which diverted 10,000 scam payments valued at over $38 million between March to September 2023.[62] This technology, which is licensed to other entities, has led to benefits reflected in reducing customer losses by a third over 6 months.[63]

There is also evidence that Government and regulator intervention is reducing the trajectory of scam losses as outlined in section 2.2.1.

4.3.3 Improving redress of scam losses

Option 1 – Status quo

This option would not achieve an economy wide understanding or agreement on responsibilities in responding to scams. As a result, consumers will continue to be subject to the imbalance of power they face in requesting a service provider investigate or accept a proportion of accountability for a scam loss.

Option 2 – Scams Prevention Framework

The SPF would impose clear obligations on regulated entities, provide clear pathways for consumers to seek redress and ensure consistency in consideration of scams complaints. Under the SPF, responsibility for redress will sit with all regulated entities

[55] ANZ, *We are in the fight against scammers together* (26 October 2023); *The price of security is vigilance* (27 November 2023)
[56] Bendigo Bank, *Bendigo Bank says collaboration is key to fight against scams and fraud* (24 November 2023)
[57] Commonwealth Bank, *CBA steps up national battle against scams* (30 May 2023)
[58] NAB, *NAB's scam alerts intervene in $270 million worth of payments* (17 June 2023)
[59] Westpac, *Westpac trials new cryptocurrency blocks to prevent scam losses* (18 May 2023)
[60] Ibid
[61] Commonwealth Bank of Australia, *New scam detection, prevention and education initiatives to keep more customers safe,* 2023
[62] Commonwealth Bank of Australia, *CBA extends scam disruption technologies as part of whole of ecosystem' national approach,* 2023.
[63] Commonwealth Bank of Australia, *Research shows Australians are more scam-aware than 12 months ago as losses fall,* 2023.

where they have not taken appropriate action. This would ensure the liability for scam losses is appropriately allocated across the ecosystem.

Mandatory IDR

Under the SPF, regulated entities operating designated digital platforms would be required to have an accessible and transparent IDR mechanism for consumers to complain about scams on its services (including the entity's conduct relating to such scams) consistent with standards for banks and telecommunications providers. Effective IDR mechanisms benefit both consumers and businesses by providing regulated entities an opportunity to assess its conduct and resolve the complaints in a timely and efficient manner. The IDR obligation would encourage the early resolution of complaints, including for compensation or other remedies to be provided to consumers where there has been a breach of their obligations under the SPF.

Mandatory EDR

Entities that are providing a service that is regulated by the SPF will be required to become a member of the EDR scheme for their sector. An EDR scheme offers a no-cost, independent and fair mechanism for consumers to escalate their complaint when they are not resolved at the IDR stage or if the IDR outcome is unsatisfactory. An effective ombudsman also incentivises regulated entities to meet their obligations, knowing that consumers have an accessible pathway to seek redress.

As scammers often operate across multiple entities and sectors in their deception of consumers, a single EDR scheme offers SPF consumers a holistic experience where there are multiple regulated entities involved in complaints. It would also bring consistency in consideration of complaints and be less burdensome for SPF consumers and industry when compared with multi-scheme alternatives.

4.4 Comparison of benefits and costs

Assessment of the of Options 2 is based on both break-even analysis and assessment of the expected relative level of benefits from each option. As previously discussed, the status quo would involve persistence of harmful costs of scams associated with personal data breaches, financial losses, psychological damages with broader socioeconomic consequences. Therefore, the net benefit is an assessment of whether their implementation costs are outweighed by the level to which they reduce these scam harms.

Option 2 – Scams Prevention Framework

Break-even analysis

As outlined in the **Overall regulatory costs** and **Government costs** sections, the average annual costs to implement Option 2 over the first 10 years will be $112.5 million ($102.1 million in regulatory costs plus $10.4 million in government costs).

Given the average scam victim in Australia reported losing $16,000 in 2023,[64] for Option 2 to result in a net benefit to society (based on reduced financial losses to scams alone) the number of instances of consumers experiencing a scam loss would need to reduce by 7,028. This is equal to 4.6 per cent reduction of the $2.7 billion of reported scam losses in 2023.[65]

Likelihood of achieving a net benefit

As Option 2 would substantially improve the regulatory framework for industry anti-scam activities and improve industry practices in responding and sharing scam information, it would be broadly expected to reduce instances of scam losses by at least 7,028 resulting in the benefits of this option outweighing the costs associated with its implementation.

As outlined above, there is evidence that uplifts to anti-scam activities have resulted in reduced measured scam losses. Although the level of further scam losses which could be avoided is uncertain, it is reasonable to assume that strengthening of scam protections, including coordination across the scam ecosystem, would result in further reductions in scam losses. Therefore, although quantification of the level of benefit is not possible given the current level of evidence available, it would be more than that likely Option 2 would result in a net gain for Australian society.

In addition, Option 2 is highly likely to reduce exposure to scams, improve redress of scam losses and provide benefits in addition to those directly related to reducing scam losses. Although these additional benefits are also unquantifiable for the purposes of this analysis, they would likely substantially increase the level of net benefit associated with Option 2.

5. Consultation

Extensive consultation was undertaken to inform the design, objectives and challenges policy interventions on scams may encounter, as well as to gauge industry and civil society's attitudes toward the proposed options.

5.1 Initial public consultation

Treasury and DITRDCA consulted on a comprehensive scams framework from 30 November 2023 to 29 January 2024.[66] Consultation involved seeking feedback on a paper that outlined a Scams Code Framework with proposed principles, features and sector-specific obligations for banks, telecommunication providers and digital platforms to adhere to in an effort to combat scams. To complement the consultation

[64] ACCC, Targeting Scams report 2023.
[65] Note the of scam losses in Australia may be expected to change in the future under Option 1 - status quo. If the number of scam victims would rise under the status quo (as is likely given assessment outlined in the Section 1) this percentage represents an overestimate of the reduction in scam losses required to result in a net benefit.
[66] The Department of Treasury, *Scams – mandatory industry codes,* 30 November 2023 – 29 January 2024

paper, a survey was released to seek feedback from members of the public on their personal experience with scams, as an alternative to providing a written submission.

As part of consultation, roundtables and bilateral meetings were held with key stakeholders. This included digital platforms, telecommunications, consumer and banking roundtables; and a regulator workshop with the ASIC, the ACCC and the ACMA.

There were 67 written submissions received (including 13 confidential submissions) from banks and financial services, digital platforms, telecommunication providers, consumer and other advocacy organisations, external dispute resolution bodies and regulators. Non-confidential submissions are published on Treasury's website. The public survey received 203 responses.

In response to consultation, businesses did not provide estimates of the quantum for anticipated costs to meet the standard of the proposed policy. Reasons for this include a reluctance to provide estimates or commit funding without greater detail on expectations from Government and guidance from regulators.

Key themes and findings

Consultation paper

Stakeholders generally supported the policy intent and design of the Framework. This included general support for a two-tiered model characterised by an overarching framework with principles-based obligations and mandatory sector-specific codes. Stakeholders generally agreed the definition of a 'scam' and 'consumer' should be legislated, with suggestions for refinement in order to capture the appropriate consumer and scam activity.

Stakeholders agreed that banks, telecommunication providers and digital communication platforms be captured in the initial scope, noting it will be expanded to other sectors later and suggesting rapid integration of several further sectors. Given the complexity of multiple regulators enforcing different sector-specific codes, stakeholders noted how regulation and enforcement across the ecosystem may differ. Banks and telecommunication providers supported an anti-scam strategy requirement and other stakeholders recommended making certain changes to the obligations, to reduce the reporting burden on businesses. Digital platforms expressed a desire for the creation of industry-developed codes and suggested voluntary approaches. Through DIGI, entities expressed encouragement for further engagement to clarify the scope of services relevant to the framework and associated definitions.

Industry stakeholders welcomed dispute resolution processes, particularly banks and telecommunication providers with existing EDR regimes. Some stakeholders including digital platforms noted further work would be required on determining the requirements on businesses and scope for stakeholders to seek redress, as well as determining an appropriate external dispute resolution body. Consumer advocates generally supported the intent of dispute resolution processes, although expressed a desire to streamline the consumer journey through dispute resolution and avoid

complexity or delay with disputes. In terms of penalties and enforcement, stakeholders largely supported a consistent approach to enabling regulators with appropriate tools and penalties for non-compliance.

Consumers and consumer advocates recommended obligations on banks be introduced for mandatory reimbursement of consumer losses in addition to the proposed framework of mandatory and enforceable industry codes. The recommendation was proposed as a way to incentivise primarily the banking industry to take greater steps to reduce scam-related risks in the banking and payments system to mitigate the impacts of losses stolen from Australians by scammers. For instance, a joint submission by the Consumer Action Law Centre, CHOICE and The Australian Communications Consumer Action Network recommended a strong presumption of reimbursement for consumer losses by the bank apply, with a corresponding mechanism for banks to seek to recover a portion of these costs from other regulated entities where those entities' actions have contributed to the scam occurring. This recommendation was considered in the policy development process, particularly as a partially related model has been adopted in the United Kingdom. The recommendation to introduce mandatory reimbursement by banks as an additional component to the framework of mandatory industry codes is not appropriate to be assessed as an additional component to option 2 in this IA as it would predominantly place an additional presumption of liability of scam losses and costs for resolution of redress apportionment onto one sector, with minimal corresponding additional incentives for other sectors to recognise liability for not meeting their obligations. This approach would not effectively address the key policy objectives to align industry responsibilities for scam prevention with the presence of scam activity on platforms and services across the economy and would not further incentivise co-ordination of anti-scam responses (see section 2.2.2). The design of the redress arrangements in government's framework will consider consumer advocates feedback to look to make the dispute resolution and redress process as consumer focused as possible, while maintaining the objective of aligning responsibility for liability and obligations for scam prevention across the economy.

Consumer survey

Respondents broadly expressed their challenges with reporting and managing scam complaints to businesses, such as delays in responses and poor visibility of actions taken by the businesses. Respondents were most exposed to and were victimised by phishing, false billing and online shopping scams. Phone calls and text messages were the most common medium for scams.

Respondents supported the need for greater industry accountability and suggested improvements in access to reporting, account authentication and verification and information sharing. Respondents support the current regulatory action, including the centralised approach to data reporting, compliance activities and co-ordination via the NASC. To supplement existing action, respondents recommended measures to improve consumer education and digital literacy and greater law enforcement.

In terms of sector-specific obligations, respondents called for banks to improve methods to create and verify new accounts and improve processes to recall user funds;

for telecommunication providers to address scam texts and calls and prevent the registration of scam numbers; and for digital platforms to restrict reported accounts, such as accounts with false and misleading advertisements, and improve customer service responses.

5.2 Targeted consultation

Post-consultation in January, Treasury and the DITRDCA continued to lead the policy development process and sought feedback on the proposed features of the policy for the public consultation. The ACCC, ASIC and ACMA were also regularly engaged with Treasury in developing the regulatory and administrative aspects of the proposed SPF under option 2.

Treasury also engaged with key private sector stakeholder groups including the Communications Alliance, AFCX, ABA, COBA and DIGI on key aspects of the policy development throughout 2024.

Key themes and findings

Targeted discussions informed the policy development process. They represented opportunities for entities and representative bodies to explore initiatives in relation to the development of standards to prevent, detect, disrupt and respond to scams.

Input was specifically sought on the regulatory costs which were likely to be incurred by regulated entities in complying with new obligations under the SPF. Responses were received with reference to investments previously undertaken to initiate anti-scam procedures and information sharing systems, as follows:

- Obligations for information sharing with the government regulator were identified to be similar in nature to those required under the Consumer Data Right, which is also administered by the ACCC. However, the likely level of cost burden from information sharing for regulated entities was indicated to be of a smaller scale given the scope for information to be shared would be more limited to scam activity, in comparison to information on customers.
- Stakeholders noted the likely level of regulatory cost would be highly dependent on prior or planned investments in anti-scam activities. In particular, entities which are already constructing information sharing arrangements such as through the AFCX would have a lower administrative burden.

5.3 Consultation on draft legislation

Treasury and DITRDCA undertook consultation on the exposure draft of legislation that established the SPF from 13 September to 4 October 2024. This process involved direct engagement through roundtables and meetings with regulators, consumer groups, industry associations and banks, telecommunication providers, digital

platforms (providing social media, direct messaging and paid advertising search services) and other relevant stakeholders.

To inform analysis of the regulatory impacts of option 2, consultation materials included a paper outlining consultation questions for stakeholder,[67] including the following requested input from stakeholders:

"If possible, please include a breakdown of the following including upfront and ongoing impacts:

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

Key themes and findings

Direct engagement identified the following key issues with the design of the proposed SPF policy:

- Concern about the interaction between obligations under the SPF principles and sector specific codes, and coordination between the regulators.
- The legislative structure may not allow for adequate tailoring of obligations to specific sectors.
- Industry representatives discussed a desire to align obligations with existing industry codes or instruments, such as the Scam-Safe Accord, Reducing Scam Calls and SMs Code, and DIGI's AOSC.
- Concern that reporting obligations would drive a high volume of reports which in turn may not be useful to support disruption activities.
- Concern that consumer warning obligations may lead to a high volume of warnings and be ineffective.
- A lack of clarity regarding liability for compensation, including apportionment between regulated entities.
- Concerns about the effective operation of dispute resolution, including how regulated entities may work together at the IDR stage.

Stakeholders did not provide estimates of additional regulatory costs expected to be incurred by regulated entities or consumers. However, they provided qualitative feedback including:

- Expect to have increases in reporting and compliance costs for regulated entities. These costs would include implementing the new annual certification

[67] Treasury, Scams Prevention Framework – exposure draft legislation, Summary of reforms document, page 12.

regime, system enhancements, additional resources for IDR, staff training and change management costs.
- Participants in existing industry initiatives were expected to have a lower level of regulatory burden. Entities that already have information sharing arrangements such as through the AFCX and ACMA would already be developing the infrastructure to support it under the SPF.
- There would be substantial burdens on smaller entities to implement SPF obligations, which have more limited personnel and technology resources. There were concerns this would put smaller entities at a competitive disadvantage.
- Entities may face overlapping obligations with existing IDR/EDR requirements, the Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) regime and existing industry codes.
- Increased costs are likely to be passed onto consumers, making it important initiatives are efficient and proportionate to scam risk. Stakeholders suggest existing frameworks be recognised to reduce inefficiencies and minimise additional compliance costs.
- Digital platforms discussed that completely new obligations, such as the development of pathways for dispute resolution arrangements, would have a disproportionately higher impact on the sector to develop and implement than other sectors with existing systems.
- Transitional arrangements would be required to enable entities to undertake uplifts in capabilities prior to obligations being enforced.

5.4 Future consultation

To proceed with option 2, following the finalisation of the legislation there would be several consultation processes undertaken to further refine the policy design:

- consultation on the instruments to designate the initial target sectors;
- consultation on the design and implementation aspects for EDR to be operated by AFCA to deliver whole-of-ecosystem external dispute escalation approach, and integrated with IDR processes;
- consultation on the obligations in the banking sector code;
- co-development between ACMA and the Communications Alliance of obligations in the telecommunications sector code, informed by experience with the current *Reducing Scam Calls and Scam SMs* code; and
- consultation on the obligations in the digital platform sector code.

5.5 Evaluation of the consultation process

How feedback was incorporated into policy design

In response to general support from stakeholders, key design aspects of the SPF under option 2 have been retained. Namely, the two-tiered model with its initial designated sectors (along with the intention of expanding of the framework to future sectors). Certain aspects of the SPF were modified in consideration of stakeholders' suggestions, for instance, stakeholders noted the importance information sharing and reporting and encouraged consideration of how to remove duplication between the multiple sectors and regulators involved in implementation of the SPF. As a consequence, the option has been adjusted to establish a streamlined overarching principles-based obligation for reporting and information sharing, with further details to be clarified outside of primary legislation.

The digital platforms sector has expressed concerns that the proposed definition[68] of "digital communication platforms" was too broad and may capture entities, such as news, music, audiobooks or podcast aggregators, on which scams may not occur. The SPF has been subsequently modified to capture social media, messaging and search advertising services.

Concerns about risks of burdens on smaller regulated entities identified by stakeholders are to be mitigated by enabling the SPF the flexibility to tailor obligations to the size, structure and operations of the entities. Differences in capabilities would be accounted for when providing further detail on obligations under the SPF principles and sector-specific code obligations. Similarly, transitional arrangements for penalty provisions across the framework would also be considered, noting the uplift that is required in capability and infrastructure to adhere to obligations. This must be balanced against the need for immediate and coordinated action to respond to the threat of scam activity and protect SPF consumers.

Feedback on the primary areas for expected additional regulatory costs has been checked against IA assumptions. Stakeholder feedback broadly aligns with assumptions used for costs for regulated entities.

Limitations

The design of the public consultation paper was high-level in nature as it aimed to assess the capabilities of and sought broad advice on a comprehensive model. Similarly, consultation on exposure draft legislation focused on the over-arching design of the SPF legislation. Subsequently, the opportunity to ask more specific questions to refine details on certain elements, like sector-specific codes' details and their impacts, was limited. Regulatory costs estimated in this IA were not able to be

[68] It was initially proposed for digital communication platforms to cover content aggregation, connective media and media sharing services.

tested with stakeholders and industry was also not able to quantify their compliance costs which may be a result of the range of questions raised that diverted capacities.

The public consultation begun on 30 November 2023 and concluded on 29 January 2024 which coincided with major holiday celebrations that may have influenced stakeholder capacities. Likewise, the consultation on exposure draft legislation ran for 3-weeks due to time constraints in the legislative development process.

6. Preferred option

6.1 Comparison of options

Option 2 is preferred. The benefits of implementing a coordinated approach to mandatory industry codes, information sharing and a single EDR scheme under option 2 have been assessed as making it the preferred option in comparison to the status quo under option 1. Option 2 is preferred as it has been assessed to result in better outcomes for the 2 core objectives of government action outlined in section 2.2.2: reduce scam harms and align benefits and costs of scam prevention.

1) Reduce scam harms

The key benefit of option 2, is that mandatory and consistent standards across industry sectors will uplift scam prevention activities and in turn reduce exposure to scams for businesses and consumers.

Under the status quo there may be some improvement in actions from entities to reduce exposure to scams, but inaction from Government to close gaps in the ecosystem targeted by scams would continue to expose Australians to vulnerabilities and high volumes of scam activity.

Option 2 would provide substantial improvement toward creating clear obligations on regulated entities and coordination of scam prevention activities. Option 2 would uplift the capacity for regulated entities across the chain of services involved in a scam, improving the likelihood scam exposure does not lead to financial loss. Uplifts to scam entity disruption activities and information sharing between entities would result in more scam activity being circumvented before amounts are transferred to a scammer.

While there may otherwise be continued progress on voluntary information sharing and anti-scam activities, the status quo would not involve the level of uplift or coordination of option 2. Similarly, under the status quo there would not be the benefit of ecosystem-wide improvements and it may involve risks of such a system being exploited by scammers.

The proposed SPF under option 2 addresses a variety of socioeconomic challenges which arise from scams through introducing a cohesive overarching structure to Australia's response to scam activity supported by government. Establishing a coherent government framework would provide a consistent message in relation to consumer

protections for scams (see section 2.1.3). This would assist in improving confidence for engaging in communications and economic activity, and understanding there are structures in place for acting on evolving scam activity into the future.

2) Align benefits and costs of scam prevention

Given the role of different types of entities offering services vulnerable to scams across the Australian economy, it is preferable to pursue an approach which does not inequitably burden one sector with the regulatory burden of complying with scam prevention and response obligations. Allocation of incentives across the scams ecosystems associated with option 2 make it preferable to the status quo Option 1 would not result in alignment of the benefits of anti-scam activity as protections, with incentives currently more concentrated on banking services and major entities rather than across entities in the scam ecosystem.

Option 2 involves aligning the imposition of costs across the economy with where there would be benefit from scam prevention activity. Option 2 would involve regulatory burden improving anti-scam activities and complying with mandatory obligations spread across the initially designated sectors of banking ($38.7 million average over the first 10 years), telecommunications ($14.9 million) and digital platforms ($48.5 million), and then potentially onto designated future services where scams are occurring. Within these sectors, costs are expected to be aligned with the extent there are opportunities for certain categories of entities to uplift their anti-scam activities and engage in improved information sharing arrangements and EDR.

The single EDR scheme proposal under option 2 takes a whole-of-ecosystem approach. This ensures responsibility for redress will sit with all entities regulated under option 2 where they have not taken appropriate action. This would ensure the liabilities for redress for scams are allocated across the ecosystem, including digital platforms who currently do not have EDR arrangements in place and remain a point of vulnerability in the scams ecosystem.

6.2 Implementation of Option 2 – Scams Prevention Framework

To implement option 2 legislation would need to be passed to establish the legal status of the SPF and enable the establishment of mandatory industry codes for scam prevention. The SPF would introduce mandatory requirements to combat scams in all sectors in the economy, initially applying to designated sectors in telecommunication providers, banks and digital platform services relating to social media, paid search engine advertising and direct messaging. Future sectors will be considered as scam methods and trends adapt and the SPF matures.

The SPF would be introduced as part of a broader effort to modernise Australia's laws for the digital age, including reforms to Australia’s privacy, money laundering and cyber settings, the modernisation of the payment system, introduction of online safety

measures, as well as the rollout of Digital ID and eInvoicing infrastructure for businesses.

Detailed obligations relating to scam prevention activities, governance, reporting and dispute resolution would be further refined to ensure compatibility with other regulatory regimes and industry initiatives. Obligations would be designed to minimise inefficiencies and regulatory burdens where appropriate.

Designation of sectors

With the SPF legislation, a designation instrument would be issued to outline the scope of entities providing services in the banking, telecommunications and certain digital platforms (social media, direct messaging and paid search advertising services) which would be obligated to comply with the SPF. This would introduce mandatory anti-scam obligations on services through which most scam activity is occurring.

Designation instruments for the first three sectors would be developed by Treasury and DITRDCA, in collaboration with industry stakeholders and other government agencies. Public consultation on the designation instruments would occur prior to instruments taking effect, to minimise risk the scope of entities covered under the SPF does not match the policy intent. The instrument may specify an application or a transition period before the SPF comes into effect to manage implementation risks.

The SPF's flexible design would enable additional sectors to be designated in the future. Prior to designating a sector, there would be consideration by Treasury and the Government of the scam activity in the sector, effectiveness of existing industry initiatives to address scams, interests of SPF consumers of the service, consequences and any other matters such as regulatory costs.

Sector-specific codes

Sector-specific codes would be developed to outline sector-specific prescriptive obligations for each sector that are consistent with the principles-based obligations. This would enable the codes to provide specific obligations tailored to the scam activity in different sectors. The codes would also provide flexibility to adapt to new and emerging scams, reflecting the fast changing and dynamic nature of scam activity in the digital economy.

Code-making may be conducted by a Minister or a government regulator, to provide flexibility for appropriate responsibilities across relevant sectors. Consultation would be undertaken on the specific obligations in the sector-codes before they are made mandatory to ensure they are appropriately designed.

Treasury would develop the codes for banks and digital platforms. The Treasury Minister intends to delegate code making for the telecommunications sector to ACMA.

ACMA would work closely with the telecommunication industry on the telecommunications sector code with DITRDCA being the relevant policy agency.

Enforcement of the code

The tiered regulatory design of the SPF would be administered and enforced via a multi-regulator model. This would deliver a whole-of-ecosystem approach to enforcement, and leverage existing regulatory relationships, monitoring and investigation frameworks already established by regulators.

The intent is that ACCC will enforce the obligations in the primary law of the framework and the digital platform service provider code; the ACMA will enforce the telecommunications code; and the ASIC will enforce the banking code.

The ACCC as facilitators of information sharing would develop appropriate guidance for reporting by regulated entities, to align with their systems, operational objectives and capabilities. Sector regulators would also develop guidance appropriate for each sector in relation to obligations under the sector codes.

Transitional arrangements for penalty provisions across the framework would be considered to enable uplift in regulated entities capabilities to be conducted. Consideration of transitional arrangements would be balanced against the need for immediate and coordinated action to respond to the threat of scam activity and protect SPF consumers.

7. Evaluation

As outlined in the need for Government action (see section 2.2.2), the objectives of the SPF are to uplift industry efforts to address scams by mandating improvements in business practices, policies, and procedures to address scams. The intended outcomes are that improvements in industry standards will reduce the impact of scams on Australians and improve industry responses and scam supports.

Evidence to inform evaluation of the SPF and success measures will include information from Government and industry sources. Industry sources include existing reporting and monitoring mechanisms undertaken by agencies and regulators to monitor of scams on regulated platforms. Metrics for success will include information through the following mechanisms:

- The NASC regularly monitors and publishes information on consumer and industry reports about scams under the Quarterly Report and Targeting Scams report.
- Agencies monitor consumer victimisation to scams, including the Australian Bureau of Statistics Personal Fraud report and Australian Institute of Criminology Cybercrime in Australia report.
- Under the current industry codes regime, the ACMA is already monitoring and evaluating telecommunications industry compliance under the Reducing Scam Calls and Scam SMs code. The SPF will enhance the current evidence base by

providing greater regulatory oversight and compliance reporting that provides transparency on measures businesses are undertaking to address scams. Regulators will monitor and evaluate how regulated entities in their sector implement mandatory obligations.

Reports from government regulators including many of these metrics are published annually or quarterly which would enable evaluation of the intended objectives to reduce scam harms to be undertaken and analysis to be conducted on areas for improvement. More details on these measures and their value for evaluation of the SPF is provided in ***Appendix 3***.

Due to the multi-faceted, changing nature of scams, there are risks that the above metrics for success may not be reflected by the evidence base used to evaluate the SPF. There are many factors that underpin changes in consumer reporting and losses that require proper recognition and analysis. As the lead regulator and overarching agency operating the NASC program, the ACCC has experiencing in monitoring and interpreting changes in the scams ecosystem and is best placed to consider these factors when using data and evidence to evaluate the outcomes of the SPF.

Glossary of Acronyms

ABA	Australian Banking Association
ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ADI	Authorised deposit-taking institution
AFCA	Australian Financial Complaints Authority
AFCX	Australian Financial Crimes Exchange
AIC	Australian Institute of Criminology
APRA	Australian Prudential Regulation Authority
AOSC	Australian Online Scams Code
ASIC	Australian Securities and Investments Commission
CDR	Consumer Data Right
COBA	Community Owned Banking Association
CSP	Carriage Service Provider
DIGI	Digital Industry Group Inc.
DITRDCA	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
EDR	External dispute resolution

FTE	Full-time equivalent
IA	Impact Analysis
IDR	Internal dispute resolution
NASC	National Anti-Scam Centre
OIA	Office of Impact Analysis
RBE	Regulatory burden estimate
SMs	Short messages
SMS	Short message service
SPF	Scams Prevention Framework
TIO	Telecommunications Industry Ombudsman

Status during policy development

Point in policy development	Timeframe	Status of the IA
Government elected with commitment to implement mandatory industry codes for scam prevention	May 2022	Undeveloped.
Public consultation on a mandatory industry code framework	November 2023 - January 2024	Began collating information for analysis in IA.
Government allocates funding in the 2024-25 Budget to establish a scams code framework	May 2024	Decision informed by Draft IA. OIA reviewed the Draft IA, providing comments which were addressed prior to the decision. An OIA assessment of the Draft IA was not required.
Ongoing targeted consultation with stakeholders	May 2024 - September 2024	Further collation of information for policy design and analysis in IA. Draft IA not used as basis for this consultation.
Internal interim decision on draft legislative design	September 2024	Draft of IA sent to OIA for comments.
Consultation on exposure draft legislation for the SPF	September 2024 - October 2024	Questions related to policy design and regulatory impacts outlined in consultation documentation. Further collation of information for analysis in IA. Draft IA not used as basis for this consultation.
OIA 1st Pass Final assessment	October 2024	1st pass assessment IA completed and presented to OIA.

Point in policy development	Timeframe	Status of the IA
OIA 2nd Pass Final assessment	October 2024	OIA 1st pass assessment comments addressed. 2nd pass assessment IA completed and presented to OIA.
Final policy decision to proceed with proposal	October 2024	To be informed by IA that has been through final assessment by OIA.

Appendices

Appendix 1 – Recent anti-scam actions and dispute resolution arrangements

Banks

Examples of initiatives announced by major banks include improved approaches to confirmation of payee such as account matching and consumer alerts; new technologies and analytics to detect and disrupt unusual behaviours; and the introduction of new holds, limits and declines on payments to cryptocurrencies. Banks are also monitoring scam activity and providing consumers with pathways to report and seek support from scams.

ASIC has periodically reviewed the anti-scam policies and procedures of banks, producing two reports: the first in April 2023 reviewing the four major banks, and the second in August 2024 reviewing fifteen non-major banks.[69] In its analysis, ASIC identified that the approach to scams strategy and governance were variable between the banks. There were inconsistencies in detecting and stopping scam payments and determining liability and that victims were not always well supported.

ASIC's findings indicate areas for improvement for both major and non-major banks, but highlight the asymmetry of scam-related supports for consumers, including dispute resolution, outside the major banks.

As an industry, there has also been collective action to addressing scams. On 24 November 2023, the ABA and the COBA launched the Scam-Safe Accord[70]. The Scam-Safe Accord has six priority initiatives based on the principles of 'disrupt', 'detect' and 'respond' (outlined in Table 15) and aims to align the banking industry's approach to addressing scams. The Scam-Safe Accord applies to all members of the ABA and COBA including large commercial Australian banks, building societies and credit unions.

[69] ASIC, *Scam prevention, detection and response by the four major banks, Report 761,* April 2023; *Anti-scam practices of banks outside the four major banks, Report 790*, August 2024.
[70] ABA, *Banks unite to declare war on scammers*, 24 November 2023.

Table 15 – Priorities for the Scam-Safe Accord

Disrupt
Banks will deliver an industry-wide confirmation of payee solution to customers – All banks will roll out this name-checking technology so their customers know who they are dealing with, mitigating the possibility of people being manipulated into paying a scammer when the name does not match. – Design of the new system to check names is to have commenced, with rollout to occur over 2024 and 2025.
Banks will take action to prevent misuse of bank accounts via identity fraud – All banks will adopt further technology and controls to help prevent identity fraud, including major banks using at least one biometric check for new individual customers opening accounts online by the end of 2024. – These checks will use behaviour detection or involve a check of a customer's face or fingerprint, enabling banks to use these characteristics to verify their customer's identity.
Banks will introduce warnings and payment delays to protect customers – If a customer is transferring money to someone they haven't paid before or raising payment limits, banks will ask more questions, and provide warnings and delays to reduce the risk of customers falling victim to a scam. It will act as a mitigant when scammers put customers under pressure to act quickly to transfer funds. – Banks will work to introduce enhanced warnings and delays by the end of 2024.
Detect
Banks will invest in a major expansion of intelligence sharing across the sector – All ABA and COBA members will join the AFCX to be ready to use scams intelligence to fight scams from mid-2024, and to the Fraud Reporting Exchange over 2024-25 to help customers recover money faster. – This will allow scams intelligence to be shared at speed between banks, helping banks prevent more scams and recover funds for customers faster where possible.
Respond
Banks will limit payments to high-risk channels to protect customers – Banks will make these risk-based decisions when they identify high-risk getaway vehicles being used by scammers to move money out of Australia. – More banks will limit payments to high-risk channels such as some crypto currency platforms to protect customers from possible theft.
Banks will implement an Anti-Scams Strategy – All banks will implement an anti-scams strategy to enhance oversight of the bank's scams detection and response.

Under section 912A of the Corporations Act 2001, banks are required to have in place IDR procedures that meet certain requirements and procedures approved by ASIC (see ASIC's Regulatory Guidance 271[71]), and additionally to be a member of AFCA. Having an IDR mechanism in place allows consumers to make a complaint to a bank (including where the consumer has been subject to a scam). Where a complaint involving a scam is not resolved at the IDR stage or the IDR outcome is unsatisfactory, consumers can escalate their complaints to AFCA.

Telecommunication providers

The telecommunications industry has taken a number of steps in developing codes to reduce the frequency and impact of scam SMS and telephone calls. The networked nature of telecommunications means that scam calls and SMS usually travel across multiple networks owned by multiple telecommunications providers - both compliant and non-compliant - to reach their target. Scammers are able to exploit vulnerabilities in the ecosystem via providers who are not compliant with the rules.

The first *Reducing Scam Calls and Scam SMs* industry code was developed by Communications Alliance, the peak body for the Australian telecommunications industry and registered by the ACMA in December 2020. In 2022, the Communications Alliance led revision of the *Reducing Scam Calls and Scam SMs* industry code, which was registered by the ACMA in July 2022.[72] The revised Code features improved tracing and reporting measures, along with a new section dealing with the identification, tracing and blocking of numbers associated with Scam SMs.

The 2022 *Reducing Scam Calls and Scam SMs* industry code requires telecommunications providers to:

- provide up-to-date guidance for consumers on how to manage and report scam calls and texts;
- monitor, identify, trace and block phone calls and SMS from recognised scammers; and
- report identified scam calls and SMS to the ACMA and any involved telecommunications providers.

Telecommunications providers who are found to be in breach of the code can be issued with a direction to comply by ACMA in the first instance. This is the strongest enforcement outcome currently available to the ACMA for initial breaches of the code. Telcos may face penalties of up to $250,000 for breaching ACMA directions to comply with the code.

In addition to the code, telecommunications providers are subject to other rules introduced by the ACMA to combat scams, including:

- stronger identity verification processes before mobile numbers can be transferred between providers – aimed at stopping scammers from hijacking

[71] ASIC RG 271: https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-271-internal-dispute-resolution/

[72] Register of telco in...~https://www.acma.gov.au/register-telco-industry-codes-and-standards

mobile phone numbers for the purpose of gaining access to other people's personal accounts including bank accounts and social media accounts, and
- authorisation processes for sensitive transactions via the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* to provide a high level of assurance to prevent malicious actors gaining access to a device and the personal information held on it.

The ACMA regularly conducts audits and investigations to test industry compliance with the code. Since 2023, the ACMA has acted against seven telcos that send bulk SMS for failing to comply with multiple anti-scam and public safety rules. In 2023, the ACMA reported that despite the significant inroads made by the new code rules, some telcos were not conducting sufficient checks to ensure customers using text-based sender IDs have a legitimate right to do so. The ACMA noted there are strong indications scammers have used these vulnerabilities to send SMS scam campaigns[73].

Individual telecommunications providers are also continuing to implement new technologies and processes to protect consumers. Several larger telecommunications providers have developed their own internal processes, such as 'trusted source' arrangements to protect phone numbers associated with well-known Australian companies.

The telecommunications sector has a mature external dispute resolution scheme, administered by the TIO. The TIO has jurisdiction to handle complaints about phone and internet services and can handle a complaint about a scam if part of the complaint related to the actions (or inactions) of a telecommunications provider who is a member of TIO. The TIO can also consider a telecommunication service provider's compliance with the *Reducing Scam Calls and Scam SMs* Code. However, there are certain matters the TIO cannot consider (e.g. contents of a scam calls or text, situations where a scammer pretends to be acting for the telecommunication service providers).[74] Certain transit carriers and CSPs may be exempt from the requirement to join TIO as they do not have individual or small business customers.

The TIO can also only take action against a consumer's contracted telecommunications provider. A common scenario is where a consumer receives a scam SMS or phone call that originated from a non-compliant provider and was transmitted to their device via a network operated by a compliant provider. In this scenario, the consumer has no right of action against their own telecommunications provider or the non-compliant originating provider.

In relation to IDR, a carriage service provider that is offering to supply a telecommunications goods or service is required to establish and implement a complaint handling process that meets certain minimum requirements set out in the *Telecommunications (Consumer Complaints Handling) industry Standard 2018.* This provides an avenue for consumers to make complaints to telecommunication service providers about their products and services (including a scam on their service).

[73] ACMA, *Action on scams, spam and telemarketing January to March 2023,* 15 May 2023.
[74] TIO's Submission to the Department of Treasury, 1 February 2024.

Digital platforms

In 2022, the ACCC identified the failure of digital platforms to take sufficient steps to prevent online harms as a key consumer harm throughout its digital platform inquiries. The ACCC recommended that digital platforms be required to implement measures to prevent and remove scams, including a notice and action mechanism (for businesses to take timely action on reports). At a minimum, the ACCC recommended these measures be applied to search, social media, online private messaging, app store, online retail marketplace and digital advertising services.[75]

On 8 December 2023, the Government provided in-principle support for the recommendations made by the ACCC in its fifth interim report of the Digital Platform Services Inquiry that aim to address competition and consumer harms on digital platforms.[76] As part of the response, the Assistant Treasurer and Minister of Communications wrote to digital platforms to develop a voluntary IDR code by July 2024. Digital platforms are not currently subject to industry-specific mandatory IDR or EDR requirements in relation to their services in Australia.

DIGI is an industry association representing twelve large digital platforms with a presence in Australia. The digital sector also includes companies in the technology sector, represented by the Tech Council of Australia. DIGI has previously led self-regulated industry codes to address online harms, including development of the Australian Code of Practice on Disinformation and Misinformation in response to the Government's response to the ACCC's 2019 Digital Platforms Inquiry[77].

In February 2024, DIGI expressed interest in developing a voluntary scams code of practice for the digital industry and launched the AOSC on 26 July 2024. The AOSC, signed by 9 DIGI members to date,[78] proposes several voluntary measures for signatories to implement when providing online services. The code applies to the provision of services including social media, peer-to-peer marketplaces, email, messaging, video sharing and paid advertising on digital platforms.

The AOSC sets out guiding principles to inform commitments to undertake specific measures, depending on the applicable services operated by the signatory. These guiding principles include consideration of the diversity of services, proportionality, the protection of user privacy and freedom of expression, and the need for collaboration and co-operation among all relevant stakeholders. *Table 16* details the specific commitments set out under the AOSC for signatories (outlined in Table 16)

Table 16 – High-level summary of key priorities under the Australian Online Scams Code

Priority	Services

[75] Australian Competition and Consumer Commission, Digital Platform Services Inquiry, *Interim report No. 5 – Regulatory reform,* September 2022
[76] The Hon Stephen Jones MP, Assistant Treasurer and Minister for Financial Services, *Government's response to the ACCC's major competition and consumer recommendations for digital platforms,* 8 December 2023
[77] Treasury, *Regulating in the digital age Government response and implementation roadmap for the Digital Platforms Inquiry,* 12 December 2019.
[78] Signatories include Apple, Discord, Google, Meta, Snap, TikTok, Twitch, X and Yahoo.

Blocking	
Deploy measures to detect and block suspected scams, including to ensure scams are addressed as non-compliant activity in community standards, guidelines or terms of service, have or adopt effective internal processes to detect, flag or remove content suspected to be a scam, block or terminate users for creating new accounts when the original accounts were removed for scams, offer appropriate login authentication methods and encourage the adoption of strong security measures such as two-step verification.	Social media services, peer-to-peer marketplaces and video sharing services
Provide guidance to users on how to stay safe when buying and selling items from other users, and commit or move towards introducing reasonable and targeted measures for the verification of users using peer to peer marketplaces.	Peer-to-peer marketplaces
Reporting	
Have a simple and quick route to report possible scams, including having or adopting simple in-product mechanisms for users to report suspected scam content, action those reports as swiftly as possible if suspicious, have or adopt a simple and direct process for law enforcement and agencies to report suspected scam activity, and indicate to users that they may report scams to law enforcement and their bank.	Social media services, peer-to-peer marketplaces and video sharing services
Provide or develop appropriate protections, which may include displaying warnings or allowing users to control or block messages.	Social media services
Takedowns	
Take quick action against verified scam content and scammers, including to expeditiously remove scam content once found by the signatory that violates applicable terms or service or policies, take appropriate enforcement action against users that post, send or share scam content, once found to be in violation, and have a clear process for users to request reinstatement of access following account takeover or scam.	Social media services, peer-to-peer marketplaces and video sharing services
Advertising	
Deploy measures to protect people from scam advertising, including to offer or develop verification or authentication measures for new advertisers, commit or move towards	Paid advertising services

introducing measures to confirm advertisers hold necessary financial services, have or introduce measures to screen advertisements, deploy processes to combat URL cloaking, and commit to or move towards a simple scam reporting mechanism.	
Email and messaging	
Deploy specific measures to protect people from scams in email and messaging, requiring service providers to make guidance available to users on scams, clarifying standards, guidelines and terms of service to ensure initiating scams is a breach of them, and have systems or processes in place to monitor for and identify scams, take appropriate action and identify trending or changing behaviour associated with scams.	Email and messaging services
Law enforcement	
Engage with law enforcement efforts to address scams, including responding to valid Australian law enforcement requests for user information or to provide information on persistent and prolific serious and organised crime as soon as practicable, and considering other ways to support crime prevention such as the provision of training, law enforcement reporting channels or public-private partnership initiatives.	All entities
Intelligence sharing	
Contribute to public-private and cross sectoral initiatives to address scams, including working with the NASC, regulators and industry partners to contribute to the work of the NASC, explore data and share best practice, as well as responding to valid regulator information requests.	All entities
Communications	
Provide information about scam risks and support counter-scam efforts., including committing to the NASC and ACCC to share information and learnings, support regulator and consumer organisation communications campaigns, and continue engaging users with messaging on risks, such as through in-product messages, help pages or links to third-party resources.	All entities
Strategy and future proofing	
Contribute to strategy development and future proofing exercises to stay ahead of the threat, including developing an	All entities.

internal anti-scam strategy, analyse established and emerging scam types on relevant services, undertake internal co-ordination to assess risks of future technologies on those services, share findings with the NASC and appropriate entities.	

Appendix 2 – Regulatory cost calculations

Under options 2 regulated entities would need to implement new systems or improve existing systems to adhere to mandatory industry codes. These changes would impose implementation and ongoing costs on businesses in adhering to obligations and respond to changed levels of liability related to scams.

For the purposes of this IA, the types of activities undertaken by entities incurring regulatory costs due to implementation of option 2 are grouped into three categories:

1. **Anti-scam activities -** Activities needed would include scam prevention, detection, disruption and response, based on its assessment of its risk in the scams ecosystem. This includes complaints handling and IDR obligations, and would also include governance operations to comply with new regulations.
2. **Information sharing and reporting** – Sharing, receiving and acting on information, to ensure that entities within the scams ecosystem have information to enable detection and prevention of scams.
3. **External dispute resolution** – Engagement in schemes to provide pathways for redress to consumers.

Increased regulatory costs from these activities are assumed to be either incurred for administrative improvements or technology, as outlined in Table 17.

Table 17 – Regulatory cost implications for relevant entities

Potential business costs in compliance with options 2	
Administrative improvements	Entities would need to make changes in administrative procedures to give effect to new mandatory obligations and improve anti-scam activity in response to changed incentives. This may include detecting patterns of potential scam activity, responding to reports or complaints from consumers and establishing procedures for sharing information and engaging with regulators and other businesses to respond to scams. Training may need to be provided to operational and executive staff in terms of their compliance and reporting responsibilities. New policies, procedures and risk analysis may need to be completed to give effect to new anti-scam activities. Businesses may be required to resource greater operational staffing or engage third party service providers to perform anti-scam activities, including for internal and customer-facing roles.

Technology	New or improved technology builds may be required to implement measures to facilitate detection, analysis and disruption activities, or set up infrastructure for data and information sharing.

Compliance costs would vary depending on several factors, including the maturity of voluntary protections being taken in a sector or individual business. The size and complexity of a business, its services, customer base, nature of the scam-related risks, and current and potential staffing and anti-scam infrastructure would also each shape expected costs. Across each activity, the assessment of regulatory costs for this IA has been based on benchmarks applied to the number of entities classified into categories across these factors.

Costs assumptions

Anti-scam activity

Uplifts in anti-scam strategy have been estimated based on benchmark assumptions for entities at different stages of capacity, assumed to be linked to their current participation in anti-scam initiatives such as industry codes, information sharing systems and EDR schemes. Entities whose existing or planned policies and procedures are better aligned with optimal practice are expected to incur lower additional costs compared to those that are not.

In constructing these assumptions, we have considered that regulated entities have already invested resources into similar or consistent consumer protection activities. These entities are likely to make further investments under the status quo. Uplifts would involve enhancements and managing higher volumes of activity for existing system and processes.

Table 18 outlines the benchmark regulatory cost assumptions for a medium sized entity. These estimates are based on assumptions of the required staff resources required to achieve a type of uplift, in terms of full-time equivalent (FTE) or weeks work required from staff.

Table 18 – Benchmark assumptions for required anti-scam activity uplift – for a medium sized entity

Uplift needed	Types of entities	Technology ($m)		Administration ($m)		Estimation assumptions
		Initial	**Ongoing**	**Initial**	**Ongoing**	
Minor anti-scam activity improvements	ABA/COBA member banks	0.22	0.00	0.02	0.00	Technology: 1.0 FTE technology staff in initial year, none ongoing Administration: 0.1 FTE admin staff in initial year, none ongoing
Moderate anti-scam activity improvements	AOSC signatory digital platforms	0.45	0.04	0.21	0.10	Technology: 2.0 FTE technology staff in initial year, 0.2 FTE ongoing Administration: 1.0 FTE admin staff, then 0.5 FTE ongoing staff.
Material anti-scam activity improvements	Non-affiliated banks, non-AOSC digital platforms	0.67	0.22	0.42	0.21	Technology: 3.0 FTE technology staff in initial year, 1.0 FTE ongoing Administration: 2.0 FTE staff, 1.0 FTE ongoing staff
SPF Governance operations	All regulated entities	0.00	0.00	0.02	0.01	Administration: 0.1 FTE admin staff in initial year, 0.05 FTE ongoing
Initiating IDR processes	Digital platforms	0.00	0.00	0.83	0.42	Administration: 4.0 FTE admin staff, 2.0 FTE ongoing

Full-time equivalent is assumed as 37.5 hours per week and 52 weeks per year, with labour costs at the rates per hour outlined in Table 19. Different labour cost rates are assumed for technology staff and administrative staff. These are calculated as per OIA guidelines with a 1.75 multiplier[79] applied to Australian Bureau of Statistics average earnings figures.[80]

Table 19 – Hourly labour cost assumptions

[79] OIA - regulatory burden framework, page 13

[80] ABS Employee Earnings and Hours, Australia, Data cube 13, May 2023. Full-time non-managerial employees paid at the adult rate.

	Rate/hr	ABS category
Administrative staff	$106.75	224 Information and organisation professionals
Technology staff	$115.33	261 Business and systems analysts, and programmers

Large entities are assumed to require 5 times the resources of medium entities, and small entities are assumed to require half the resources of medium entities.

These uplift cost assumptions can be interpreted in comparison to past industry activity, such as domestic banking sector members of ABA and COBA that have previously invested in a confirmation of payee system with total sectoral costs estimated at $100 million, around $1.3 million per bank.[81] This is comparable to the assumed regulatory costs incurred by a medium sized entity to initiate anti-scam activities over 2 years.

Information sharing and reporting

Regulatory costs of information sharing arrangements under option 2 are challenging to estimate due to uncertainty of the required systems for entities to communicate with the government regulator and other factors such as the frequency of communication and the information required.

However, expected entity investments for compliance with information sharing obligations under the consumer data right (CDR) are a comparable basis for estimated regulatory costs. Although, the SPF information sharing arrangements would be less complex and lower in volume and frequency than required under CDR.

Regulatory costs of CDR by type of entities regulated were conducted in 2021 for coverage of the telecommunications sector[82] and in 2022 for the non-bank lending sector.[83] Table 20 outlines the estimated annual regulatory costs in the first year and ongoing, by type of entity from these previous reports, which have been inflated to current dollar values to use as benchmarks for regulatory costs under option 2.[84]

Table 20 – Estimated annual CDR compliance costs by types of entity (in 2024 dollars)[85]

Type of entity	Year 1	Ongoing	Source
Small telco	$394,000	$186,000	CDR telecommunications sectoral assessment (Treasury 2021)
Large telco	$4,986,000	$1,484,000	

[81] Australian Banking Association, *Banks unite to declare war on scammers*, 24 November 2023.
[82] Treasury (2022) Consumer Data Right – Telecommunications Sectoral Assessment, available on the OIA website: https://oia.pmc.gov.au/published-impact-analyses-and-reports/consumer-data-right-telecommunications-sectoral-assessment
[83] Treasury (2022) CDR – Non-bank lending sectoral assessment, available on the OIA website: https://oia.pmc.gov.au/published-impact-analyses-and-reports/cdr-non-bank-lending-sectoral-assessment
[84] Using Consumer Price Index values for Australia from the Australian Bureau of Statistics, from September 2021 to June 2024 for telecommunications estimates and from June 2022 to June 2024 for non-bank lender estimates.
[85] Rounded to the nearest $1,000.

Type of entity	Year 1	Ongoing	Source
Medium non-bank lender	$826,000	$330,000	CDR non-bank lending sectoral assessment (Treasury 2022)
Large non-bank lender	$3,302,000	$1,101,000	

As information sharing for option 2 under the SPF would be less resource intensive than the CDR, it is assumed a regulated entity would incur 20 per cent of the CDR benchmark costs if needing to develop information sharing capabilities with the government regulator without similar prior or intended activities. Given many entities are already undertaking information sharing without the SPF, such entities would only be assumed to need to incur around 5 per cent of the CDR cost benchmark.

External dispute resolution costs

Costs to regulated entities for engaging in EDR programs are estimated based on the fee structures and experiences of entities engaged with AFCA's EDR process.[86]

AFCA is a not-for-profit body and recovers its cost from members. It relies on three funding streams to support its business operations:

- annual membership fees,
- fees collected from members subject to a complaint (complaint fees), and
- a proportionate charge to members who have had six or more complaints brought against them during the period (user charge).

AFCA's annual membership fee for financial firms is expected to be around ~$389 in FY2024-25. Complaint fees and an proportionate user charges are calculated based on prior year's AFCA dispute handling data.

AFCA's fee schedule incentivises early resolution of disputes by regulated entities. EDR costs will be minimised if they meet their mandatory obligations, resolve complaints directly with their customers at the IDR stage or resolve complaints early where they are escalated to EDR. AFCA does not charge for the first five complaints in a financial year against a member. After that, AFCA's complaint fees depend on where in the process that the relevant complaint gets resolved. Fees are smaller at the earlier stages and increase if the complaint requires a decision. The fee schedule encourages earlier resolution of complaints and for firms to improve their IDR process, which decreases the need for the complaints to come to AFCA.

The user charge is a proportionate annual charge which is calculated at the start of the financial year and is based on AFCA's prior year dispute handing data. More frequent users of AFCA's service pay higher user charges.

In 2023-24, AFCA received 10,928 scam complaints, with 67% of the complaints closed at the 'registration and referral' stage.[87] Under the 2024-25 fee schedule, AFCA has a complaint fee of $96 for cases at the 'registration and referral' stage.[88]

[86] AFCA Complaint Fee Guide.
[87] AFCA Annual Review 2022-23, Scam complaints, https://www.afca.org.au/annual-review-scams
[88] AFCA Fee Structure FY25, https://www.afca.org.au/members/funding-model/fee-structure

As a conservative estimate of regulatory costs for the purposes of this IA it is assumed that entities which are not currently a part of an EDR scheme would incur approximately costs of $924 per complaint (inclusive of GST). This is based on AFCA 2023-24 data on distribution of the stage AFCA scam complaints are closed and the approximate 2024-25 fee associated with complaints at that stage.

The annual AFCA fees for scam complaints per entity is estimated by apportioning the approximately 11,000 complaints received each year across types of banks and other ADIs according to the market share of total residential deposits.[89] These estimates are outlined in Table 21 (covers major banks, non-major ABA member banks and other ADIs) and are used as benchmarks for EDR costs for regulated entities in the banking sector, as well as telecommunications and digital platforms.

Table 21 – Estimated annual EDR costs for scam complaints by type of entity[90]

Type of entity	Number	Market share	Assumed scam complaints per entity	AFCA fees for scam complaints per entity
Major banks	4	73.6%	2,025	$1,818,000
Non-major ABA member banks[91]	16	17.5%	121	$109,000
Other ADIs - AFCA members	115	8.8%	8	$8,000

For telecommunications providers which are currently members of the TIO, enrolment in a single EDR scheme under the SPF would involve an uplift in fees given they would need to be members of two EDR schemes. TIO would continue to operate its existing EDR jurisdiction in relation to non-scam complaints about telecommunications service providers. However, as there is no publicly available data on TIO fees for complaints involving scams it is not possible to estimate current levels of TIO fees which are expended by TIO members on scam complaints.[92] For the purposes of this analysis, it is assumed the increase in EDR fees from the Framework would be 50 per cent of the estimated fees of similar scale entities in the financial sector.

Under option 2, demand for EDR would be higher as consumers seek to take action to exercise their rights to protection under the Framework or mandatory reimbursement. This is assumed to be a 10 per cent uplift from the current volume of scam complaints

[89] APRA, Monthly Authorised Deposit Taking Institution Statistics, Key Statistics, July 2024. Although some complaints may not be related to ADIs, the market share of scam complaints have been calculated based on the assumption all complaints are made to ADI members in the proportion equivalent to their market share of total residential deposits. This benchmark may be conservatively higher than AFCA fees actually incurred.
[90] Rounded to the nearest $1,000.
[91] Identified based on Australian Banking Association website list of 20 members, as at September 2024, https://www.ausbanking.org.au/about-us/aba-members/
[92] According to the 2023 TIO Financial Report "funding requirement is allocated to members based on the percentage of the number of complaints (referrals) the member had in the previous calendar year compared to the total complaints (referrals) received in that year." However, data on the number of complaints by member is not available.

made against AFCA members (with the uplifted cost assumption carried across to telecommunications and digital platform sector entities).

It is assumed other internal costs and resources required to undertake EDR obligations in addition to AFCA fees are incorporated costs of overall anti-scam activity. Costs incurred by regulated entities in paying redress to scam victims are not accounted for as a cost of either option 2, as these payments represent a transfer from the entity to the consumer with no overall net cost or benefit.

Assumptions on number of regulated entities

Banking

Full membership of the AFCX is not publicly disclosed, however participants include the four founding major banks, Macquarie and Bendigo Bank, and COBA. In May 2023, the ABA reported that 14 of its 20 members were, or were in the process of, entering membership with the Fraud Reporting Exchange.

Table 22 outlines the estimated number of ADIs which are currently a part of voluntary industry codes, information sharing arrangements and EDR schemes. Almost all domestic ADIs are a member of an external dispute resolution scheme. According to APRA's register of ADIs and AFCA's member register, only 1 of the 80 Australian-owned authorised ADIs are not AFCA members.[93] This extends to 19 of the 49 Australian branches of foreign-owned banks on the APRA register.

Table 22 – Number of assumed regulated banking entities by current activity category

CATEGORY	NUMBER OF ENTITIES	VOLUNTARY CODE MEMBERSHIP	INFORMATION SHARING	EDR MEMBERSHIP
MAJOR BANKS	**4**	ABA Scam-Safe Accord	AFCX members	AFCA members
ABA/COBA MEMBERS	**72**		Soon to all be AFCX members	
NON-AFFILIATED[94] / AFCA MEMBERS	**40**	No applicable code	No information sharing arrangements	
NON-AFFILIATED/ NON-AFCA	**16**			No EDR scheme

[93] Identified through https://my.afca.org.au/ff-search/, September 2024
[94] Not a member of the ABA or COBA.

Telecommunications providers

For regulatory cost calculation purposes the SPF would be assumed to apply to carriers and carriage service providers as those terms are defined in s 7 of the *Telecommunications Act 1997* (Telco Act). Carriers require a license under the Act and are published under an ACMA register. Currently, there are 342 ACMA licensed carriers.[95] Carriage service providers represent a far wider market, with ACMA estimating there are around 1,500 'eligible CSPs' under the *Telecommunications (Consumer Protection and Service Standards) Act* (TCPSS Act).[96]

The TCPSS Act requires eligible CSPs to be members of, and comply with, the TIO Scheme. Under s 128 of the TCPSS Act, each *carrier* and each *eligible carriage service* provider must join the TIO Scheme.

- A "carrier" is a holder of a carrier licence granted under s 56 of the Telco Act.
- Under s 127, an "eligible carrier service provider" is a carriage service provider who supplies or arranges the supply of:
    - A standard telephone service to residential or small business customers
    - Public mobile telecommunication service
    - Access to the internet

Under option 2 a potentially broader group of entities would be required to join an EDR scheme than are currently required to join the TIO. Transit carriers and CSPs may be exempt from the requirement to join the TIO scheme as they do not have individual or small business customers,[97] but would be required to join the AFCA scheme under the SPF. As at the end of 2022-23 there were 1,686 TIO members,[98] and 32 transit carriers and CSPs with TIO membership exemptions.

ACMA published a regulation impact statement, *Reducing the impact of scam calls*, that estimated 413 carriers/CSPs provide public numbers to ACMA for mobile and local services in 2020.[99] The report noted that multiple carrier and/or CSP licences can be held by a single telecommunications provider entity. The IA provides the following estimates of the number of telco entities impacted by the scam calls code holding relevant licences as follows:

- large carriers: 4 (over 10 million numbers)
- medium CSPs: 18 (1 million to 10 million numbers)
- small CSPs: 150 (100,000 to 1 million numbers)
- very small CSPs: 241 (1 to 100,000 numbers)

[95] ACMA, *Register of licensed carriers* (5 September 2024)
[96] DITRDCA, *Registration or licensing scheme for carriage service providers Discussion Paper* (September 2023)
[97] Under s 129 of the TCPSS Act, ACMA may grant an exemption from the requirement to join the TIO Scheme. Before granting such an exemption, ACMA must have regard to the following matters (note, it can also have regard to other things): the extent to which the carrier or provider deals with residential customers or small businesses; the potential for complaints under the TIO about the services supplies by the carrier or provider; and, whether the carrier or provider is a statutory infrastructure provider (within the meaning of Part 19 of Telco Act).
[98] TIO Financial Report 2023
[99] ACMA, *Reducing the impact of scam calls Regulation Impact Statement* (December 2020); *Reducing the impact of scams delivered by short message service (SMS) Regulation Impact Statement* (June 2022)

These figures are used as the basis for the number of entities which would be regulated entities under option 2's SPF, with the addition of 32 transit carriers/CSPs. Table 23 outlines the number of entities in each category.

Table 23 – Number of assumed regulated telecommunications entities by current activity category

CATEGORY	NUMBER OF ENTITIES	MANDATORY CODE OBLIGATIONS	INFORMATION SHARING	EDR MEMBERSHIP
MAJOR TELCOS	4 (Telstra, Optus, TPG)	*Reducing Scam Calls and Scam SMs* code	*Reducing Scam Calls and Scam SMs* code & AFCX members	TIO members
MEDIUM CSPS	18		*Reducing Scam Calls and Scam SMs* code	
SMALL CSPS	150			
VERY SMALL CSPS	241			
TRANSIT CARRIERS/CSPS	32			TIO exempt

Digital platforms

The number of digital platform entities which would be regulated entities under option 2 has been estimated based on previous ACCC inquiries into the relevant services.

As the SPF would be intended to address where scams harms are most prevalent, the social media services that could be captured would include Facebook, YouTube, Instagram, Snap, TikTok, Pinterest, Reddit, LinkedIn, BeReal and X. This is based on the ACCC's 6th interim report of the Digital Platform Services Inquiry[100], which identified services of Meta (Facebook, Instagram), Google (YouTube), ByteDance (TikTok), Snap (Snapchat) and Pinterest having over 5 million monthly active users in 2022.

In the ACCC's 5th interim report of the Digital Platform Services Inquiry "online private messaging services" are defined as "services that enable users to communicate privately and in real-time with friends, family members, colleagues and other contacts, one-to-one and/or with a group using text, voice or video."[101] Based on Nielsen Digital Content Ratings the report identifies usage data for 17 direct messaging services, in addition to 3 services not captured by this ratings data.[102] The report identified Meta (Facebook Messenger, WhatsApp) and Apple (iMessage, FaceTime) as the 2 largest supplies of online messaging services, Snap (Snapchat) had over 4 million monthly

[100] ACCC (2023) Digital Platform Services Inquiry, *Report on social media services,* March 2023. Page 31
[101] ACCC (2022) Digital Platform Services Inquiry, Interim report No. 5 – Regulatory reform, September 2022. Page 23
[102] Ibid. Page 202

active users, and Zoom, Microsoft (Skype) and Discord had services with around or over 2 million monthly active users.

In terms of search advertising service providers, Google (through its Google search service) and Microsoft (though its Bing search service) would initially be captured. This is based on the ACCC's 2021 Digital Advertising Services Inquiry[103] and more recently, the ACCC's 9th interim report of the Digital Platform Services Inquiry issues paper on revisiting general search services[104] which reported that these entities provide almost all search engine services used in Australia. The recent issues paper reported that Google Search had an 86 per cent market share in desktop search and 98 per cent market share in mobile search, and Microsoft Bing had a 12 per cent market share in desktop search.[105]

Table 24 outlines the number of entities in each category assumed for this IA. Digital platform entities are grouped by the scale of their entity (major or medium) and whether they are a signatory to the AOSC in order to estimate the relative level of regulatory cost required to be incurred under the obligations in option 2. Major platforms operate either a social media platform or direct messaging service with over 4 million active monthly users (in 2022), or a search advertising service with a greater than 10 per cent market share on either desktop or mobile (in 2024).

Table 24 – Number of assumed regulated digital platform entities by current activity category

CATEGORY	NUMBER OF ENTITIES	VOLUNTARY CODE MEMBERSHIP	INFORMATION SHARING	EDR MEMBERSHIP
MAJOR PLATFORMS – AOSC	**5** (Meta, Google, Byte Dance, Snap, Apple)	Australian Online Scams Code (AOSC)	Engagement in NASC information sharing	No memberships of EDR schemes
MEDIUM PLATFORMS – AOSC	**2** (X, Discord)			
MAJOR PLATFORMS – NON-AOSC	**2** (Microsoft, Pinterest)	None	No current arrangements	
MEDIUM PLATFORMS - NON-AOSC	**12** (Reddit, BeReal, Zoom)			

[103] ACCC (2021) Digital advertising services inquiry - final report, 28 September 2024
[104] ACCC (2024) Digital Platform Services Inquiry – September 2024 report revisiting general search services, Issues Paper, 18 March 2024
[105] Ibid. pages 6-7

Option 2: Regulatory cost assumption tables

Table 25 – Option 2 - Banking sector annual regulatory cost assumptions by entity type (medium sized entity)

		Description of impacts		Technology ($m)		Administration ($m)	
Obligation	Entity type	Current actions	Uplift required	Initial	Ongoing	Initial	Ongoing
Anti-scam activity	Major banks	Scam-Safe Accord standards	Minor anti-scam activity improvements, Governance operations	1.12	0.00	0.21	0.05
	Other ABA/COBA	Scam-Safe Accord standards	Minor anti-scam activity improvements, Governance operations	0.22	0.00	0.04	0.01
	Non-affiliated/ AFCA	No identifiable consistent standards	Material anti-scam activity improvements, Governance operations	0.67	0.22	0.44	0.22
	Non-affiliated/non-AFCA	No identifiable consistent standards	Material anti-scam activity improvements, Governance operations	0.67	0.22	0.44	0.22
Info sharing & reporting	Major banks	AFCX intel loop participation	Minor investment in info sharing	0.04	0.02		
	Other ABA/COBA	AFCX intel loop participation	Minor investment in info sharing	0.04	0.02		
	Non-affiliated/AFCA	None	Likely significant investment	0.17	0.06		
	Non-affiliated/non-AFCA	None	Likely significant investment	0.17	0.06		
EDR	Major banks	AFCA members	10% increase in complaints			0.18	0.18
	Other ABA/COBA	AFCA members	10% increase in complaints			0.01	0.01
	Non-affiliated/AFCA	AFCA members	10% increase in complaints			0.00	0.00

	Non-affiliated/non-AFCA	None	EDR for complaints with AFCA			0.01	0.01

Table 26 – Option 2 - Telecommunications sector annual regulatory cost assumptions by entity type (medium sized entity)

		Description of impacts		Technology ($m)		Administration ($m)	
OBLIGATION	Entity type	Current actions	Uplift required	Initial	Ongoing	Initial	Ongoing
ANTI-SCAM ACTIVITY	Major telcos	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.10	0.05
	Medium CSPs	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.02	0.01
	Small CSPs	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.01	0.01
	Very small CSPs	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.01	0.01
	Transit carriers/CSPs	Reducing Scam Calls and Scam SMS code	Governance operations	0.00	0.00	0.01	0.011
INFO SHARING & REPORTING	Major telcos	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0 25	0.07		
	Medium CSPs	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.02	0.01		
	Small CSPs	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.02	0.01		
	Very small CSPs	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.02	0.01		
	Transit carriers/CSPs	Reducing Scam Calls and Scam SMS code	Minor investment in capabilities	0.02	0.01		
EDR	Major telcos	TIO members	AFCA fee level, 10% increase in complaints			1.00	1.00
	Medium CSPs	TIO members	AFCA fee level, 10% increase in complaints			0.06	0.06
	Small CSPs	TIO members	AFCA fee level, 10% increase in complaints			0.00	0.00
	Very small CSPs	TIO members	AFCA fee level, 10% increase in complaints			0.00	0.00
	Transit carriers/CSPs	No current EDR scheme	EDR for complaints with AFCA			0.01	0.01

Table 27 – Option 2 - Digital platforms sector regulatory cost assumptions by entity type (medium sized entity)

		Description of impacts		Technology ($m)		Administration ($m)	
OBLIGATION	**Entity type**	**Current actions**	**Uplift required**	**Initial**	**Ongoing**	**Initial**	**Ongoing**
ANTI-SCAM ACTIVITY	Major platforms - AOSC	Aus Online Scams Code	Moderate anti-scam activity improvements, Governance operations, IDR processes	2.25	0.22	5 31	2.65
	Major platforms - non-AOSC	None	Material anti-scam activity improvements, Governance operations, IDR processes	3.37	1.12	6 35	3.17
	Medium platforms - AOSC	Aus Online Scams Code	Moderate anti-scam activity improvements, Governance operations, IDR processes	0.45	0.04	1.06	0.53
	Medium platforms - non-AOSC	None	Material anti-scam activity improvements, Governance operations, IDR processes	0.67	0.22	1 27	0.63
INFO SHARING & REPORTING	Major platforms - AOSC	No current arrangements	Likely significant investment	1.00	0.30		
	Major platforms - non-AOSC	No current arrangements	Likely significant investment	1.00	0.30		
	Medium platforms - AOSC	No current arrangements	Likely significant investment	1.00	0.30		
	Medium platforms - non-AOSC	No current arrangements	Likely significant investment	1.00	0.30		
EDR	Major platforms - AOSC	None	AFCA membership			0 18	0.18
	Major platforms - non-AOSC	None	AFCA membership			0 18	0.18
	Medium platforms - AOSC	None	AFCA membership			0.01	0.01
	Medium platforms - non-AOSC	None	AFCA membership			0.01	0.01

Appendix 3 – Outcomes and evaluation matrix

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
Reduced demographic rates of exposure and victimisation of consumers to scams	Quantitative	ABS, *Personal Fraud* AIC, *Cybercrime in Australia* Treasury, *Australian Consumer Survey*	Consumer surveys in Australia have found that scam exposure is widespread. Estimates of exposure to scam attempts sit around 65% of the population, with victimisation between 2% to 3%.	Greater business anti-scam measures, particularly prevention and disruption measures, will contribute to lower rates of exposure and victimisation to scams. Increasing avenues for consumer redress may lead to a decline in average losses as the impacts of scams become less ruinous for the consumer.	Due to the nature and increasing prevalence of scam activity, it is impossible to eradicate overall exposure to scams. Figures relating to victimisation are more accurate assessments of the degree to which scam attempts 'break through' and impact Australians. Improvements should be analysed in context to short-term trends whilst accounting for the fact

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
					that scam activity can fluctuate, which the ACCC is well equipped to identify and account for.
Reduced consumer losses to scams reported to regulators		ACCC, *Targeting Scams, Scamwatch Dashboard* Treasury, *Australian Consumer Survey*	Consumers and businesses reported $3.1 billion in losses to scams in 2022, an increase of 80% from 2021. On average, a victim to a scam loses $20,000. There is evidence of recent Government and industry efforts leading to this figure to peak, but losses remain much higher than pre-		Changes in average losses should be considered with caution as they may reflect changing patterns to overarching scam methods, such as low-yield shopping scams or high-yield investment scams, rather than a reduced overall prevalence of scams. The ACCC records other

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
			pandemic levels.		figures, including recording median losses, and disaggregates reports and losses by scam type, which can corroborate evidence of improvements.
Improved reporting and information sharing on scam cases affecting consumers	Quantitative and qualitative	ACCC, *Targeting Scams, Scamwatch Dashboard* ATO, *Scam Data*	Consumer reports to regulators remain high. In 2023, Australians made over 300,000 reports to Scamwatch, an increase of 26% from 2022. Reporting and information sharing arrangements to regulators under the NASC are currently voluntary or limited due	Increased access to complaints handling and reporting measures may increase the level of consumer reports being made to regulators from consumers. More reports can be leveraged by information-sharing infrastructur	Increases or decreases in reporting do not necessarily reflect a desirable outcome. Although fewer consumer reports may reflect less scam activity, increased reporting may reflect improved accessibility to and quality of

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
			to the scope of privacy or tipping-off provisions.	e of the SPF and NASC.	reporting measures.
Increased rate of detection and disruption activities undertaken by the private sector	Quantitative and qualitative	ACCC, *Quarterly Report* ACMA, *Action on Scams, Spam and Telemarketing*	Outside of existing regulatory regimes including ACMA codes, there is little centralised evidence for sector-wide activities to address scams.	Potential monitoring of business action by regulators and subsequent reporting under the SPF will provide Government with clearer evidence on the extent of industry action on scams and in turn opportunities to identify regulatory gaps, effective actions, and ongoing trends.	Scam threats wax and wane over time. Quantitative information on industry action must be interpreted in the context of these trends; for instance, increases or decreases in blocked calls or numbers or account closures.
Increased assessment of quality in business anti-scam policies and procedures	Qualitative	ACCC, *Digital Platform Services Inquiry* ASIC, *Scam Prevention, Detection*	Regulators have identified significant levels of variation in the quality of business anti-scam	Uplift of quality of anti-scam policies and procedures in the business sector, which will	This measure depends on future regulatory review and reporting mechanisms which

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
		and Response	practices and procedures. Whilst some voluntary industry efforts such as the Scam-Safe Accord are in place, there will remain gaps in the voluntary framework for outsider participants.	in term limit regulatory gaps and contribute to other improved outcomes.	remain unconfirmed.
Increased levels of consumer satisfaction with business policies and procedures relating to scams	Qualitative	Treasury, *Scams Consumer Survey*	Consumer advocacy bodies have expressed dissatisfaction with current business policies and procedures relating to scams. The widespread impact of scams is anecdotally leading consumers to be more risk-averse and distrustful of everyday	Improved consumer protections will increase consumer satisfaction and trust in their communications and transactions with industry entities.	This metric is difficult to measure. Consumer satisfaction with business anti-scam policies and procedures are oriented towards positive resolution and redress of consumer disputes. An improvement in

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
			business functions, including communications, notifications and transactions relied on by businesses.		consumer satisfaction may not reflect the state of the overarching ecosystem and business impacts.
Consumer trust in the payments and communications system		Treasury, *Scams Consumer Survey*	The widespread impact of scams is anecdotally leading consumers to be more risk-averse and distrustful of everyday business functions, including communications, notifications and transactions relied on by businesses.	Improved consumer protections will increase consumer trust in their communications and transactions with the business sector.	This metric is difficult to measure. Some business sector participants believe increased consumer trust is a moral hazard in which risks are offset to be borne by the business sector.
Decreased levels of consumer complaints to external dispute	Quantitative and qualitative	AFCA, *Annual Review*	AFCA has noted increased pressure of consumer scam-related complaints	Prevention of scams and improved business complaints handling	Increased or decreased reporting may not indicate positive

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
resolution systems			on the financial dispute resolution system, affecting the efficiency of complaints resolution. In 2022-23, AFCA received over 6,000 scam-related complaints, an increase of 46% from 2021-22.	processes will contribute to a decreased level of consumer complaints and greater level of internal resolution, leading to a decrease in external dispute resolution complaints over time.	outcomes or broader trends in the scams ecosystem, as addressed in other sections in this column.
Increased consumer access to reporting outlets and support networks	Quantitative and qualitative	AIC, *Cybercrime in Australia* Treasury, *Scams Consumer Survey*	Despite there being several reporting avenues for support when a person is affected by a scam, there is low take-up of these services. The AIC estimates most Australians do not disclose their victimisation to scams or fraud with	Improved complaints handling and reporting processes may improve the connection of victims to support services and increase the overall take-up of these services.	The evidence base for consumer take-up is survey-based and limited. There are personal and situational elements that influence consumers' beliefs relating to supports that may not be improved, particularl

Outcomes	Measure type	Past evidence base	Status quo	Expected impacts	Caveats
			agencies, with low take-up of services such as ACSC and IDCARE and reporting outlets such as Scamwatch.		y a reluctance to escalate supports if it is known that funds lost to a scam are unrecovera ble from a financial institution. Also, not all victims of a scam report a loss, limiting their desire to escalate.

2022-2023-2024

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

Presented and read a first time

Scams Prevention Framework Bill 2024

No. , 2024

(Treasury)

A Bill for an Act to provide a framework for preventing and responding to scams, and for related purposes

Contents

A Bill for an Act to provide a framework for preventing and responding to scams, and for related purposes

The Parliament of Australia enacts:

1 Short title

This Act is the *Scams Prevention Framework Act 2024*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this Act	The day after this Act receives the Royal Assent.	

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Amendments

Part 1—Main amendments

Competition and Consumer Act 2010

1 After Part IVE

Insert:

Part IVF—Scams Prevention Framework

Division 1—Preliminary

Subdivision A—Object and simplified outline

58AA Object of this Part

The object of this Part is to prevent and respond to scams impacting:

(a) either:

(i) natural persons while they are in Australia; or

(ii) persons who carry on small businesses in Australia;

if the scams relate to, are connected with, or use certain services that are or may be provided or purportedly provided to those persons; or

(b) natural persons while they are outside of Australia if:

(i) they are ordinarily resident in Australia; and

(ii) the scams relate to, are connected with, or use certain services that are or may be provided or purportedly provided to those persons by Australian service providers or by foreign service providers through permanent establishments in Australia.

58AB Simplified outline of this Part

The Scams Prevention Framework is a multifaceted approach for protecting Australian consumers from scams. The Framework

requires service providers in selected sectors of the economy to take a variety of actions to combat scams relating to, connected with, or using their services.

These service providers must comply with the overarching principles of the Framework. These principles are about:

(a) governance arrangements relating to scams; and

(b) preventing, detecting, reporting, disrupting and responding to scams.

Under the Framework, the Minister may make a code (an ***SPF code***) setting out sector-specific requirements for the service providers in a selected sector of the economy relating to:

(a) governance arrangements relating to scams; and

(b) preventing, detecting, disrupting and responding to scams.

Under the Framework, the Minister may authorise external dispute resolution schemes for participation by these service providers. The operator of such a scheme will be able to determine complaints by consumers about how these service providers respond to scams.

The Commission is to regulate and enforce compliance with the overarching principles of the Framework. Other Commonwealth entities will be selected by the Minister to regulate and enforce compliance with SPF codes.

Subdivision B—Designating sectors subject to the Scams Prevention Framework

58AC *Regulated sectors* subject to the Scams Prevention Framework

(1) The Minister may, by legislative instrument, designate one or more businesses or services to be a ***regulated sector*** of the Australian economy.

Note 1: An individual business or service could be designated, or businesses or services could be designated by class (see subsection 13(3) of the *Legislation Act 2003*).

Note 2: For variation and repeal, see subsection 33(3) of the *Acts Interpretation Act 1901*.

(2) Without limiting subsection (1), the following classes of businesses or services could be designated:

(a) businesses of banking, other than State banking (within the meaning of paragraph 51(xiii) of the Constitution) not extending beyond the limits of the State concerned;

(b) businesses of insurance, other than State insurance (within the meaning of paragraph 51(xiv) of the Constitution) not extending beyond the limits of the State concerned;

(c) postal, telegraphic, telephonic or other like services (within the meaning of paragraph 51(v) of the Constitution), such as one or more of the following:

(i) carriage services (within the meaning of the *Telecommunications Act 1997*);

(ii) electronic services (within the meaning of the *Online Safety Act 2021*), such as social media services (within the meaning of that Act);

(iii) broadcasting services (within the meaning of the *Broadcasting Services Act 1992*).

Note: This is not an exhaustive list. Similarly, a subset of paragraph (a), (b) or (c) could be designated.

58AD *Regulated entities* for regulated sectors and their *regulated services*

Entities with businesses or services within the banking, insurance or communications constitutional powers

(1) To the extent that a regulated sector includes a business or service covered by paragraph 58AC(2)(a), (b) or (c):

(a) the person who carries on or provides that business or service is a ***regulated entity*** for the sector; and

(b) that business or service is a ***regulated service*** of the regulated entity for the sector.

Note 1: This subsection extends to a regulated sector consisting of businesses or services that are a subset of paragraph 58AC(2)(a), (b) or (c).

Note 2: Sections 58GA to 58GC extend the meaning of ***person*** for partnerships, unincorporated associations and trusts.

Other entities who may be regulated entities

(2) Otherwise:

(a) the ***regulated entities*** for a regulated sector; and

(b) the ***regulated services*** of each of those regulated entities;

are as set out in the following table:

Other regulated entities, and their regulated services, for the regulated sector

Item	This person is a *regulated entity*:	for this *regulated service*:
1	a corporation that carries on or provides a business or service that is part of the regulated sector	that business or service.
2	a person to the extent that the person is both: (a) carrying on or providing a business or service that is part of the regulated sector; and (b) acting using a postal, telegraphic, telephonic or other like service (within the meaning of paragraph 51(v) of the Constitution)	so much of that business or service as relates to the person acting in that way.
3	a person to the extent that the person is both: (a) carrying on or providing a business or service that is part of the regulated sector; and (b) acting in the course of, or in relation to, a kind of trade or commerce mentioned in subsection (3)	so much of that business or service as relates to the person acting in that way.

Note 1: For the meaning of ***corporation***, see section 4.

Note 2: Sections 58GA to 58GC extend the meaning of ***person*** for partnerships, unincorporated associations and trusts.

(3) For the purposes of item 3 of the table in subsection (2), the kinds of trade or commerce are as follows:

(a) trade or commerce between Australia and places outside Australia;

(b) trade or commerce among the States;

(c) trade or commerce within a Territory, between a State or Territory or between 2 Territories.

Exceptions—complete

(4) Despite subsections (1) and (2):

(a) a person is not a ***regulated entity*** for a regulated sector to the extent that an exception prescribed by the SPF rules applies to the person; and

(b) a business or service is not a ***regulated service*** of a person for a regulated sector to the extent that an exception prescribed by the SPF rules applies to the business or service.

Note: A person, business or service may be specified by class (see subsection 13(3) of the *Legislation Act 2003*).

Exceptions—partial

(5) Despite subsections (1) and (2), the instrument made under subsection 58AC(1) designating a business or service to be all or part of the regulated sector may declare that:

(a) the person who carries on or provides the business or service is not a ***regulated entity*** for the regulated sector for the purposes of specified SPF provisions; or

(b) the business or service is not a ***regulated service*** for the regulated sector for the purposes of specified SPF provisions.

Note: An individual person, business or service could be declared, or persons, businesses or services could be declared by class (see subsection 13(3) of the *Legislation Act 2003*).

58AE Minister must consider matters, and consult, before designating a sector

(1) Before making an instrument under subsection 58AC(1) about a sector of the economy, the Minister must:

(a) consider all of the following:

(i) scam activity in the sector;

(ii) the effectiveness of existing industry initiatives to address scams in the sector;

(iii) the interests of persons who would be SPF consumers of regulated services for the sector if the instrument were made;

(iv) the likely consequences (including benefits and risks) to the public if the instrument were made;

(v) the likely consequences (including benefits and risks) to the businesses or services making up the sector;

(vi) any other matters the Minister considers relevant; and

(b) consult the businesses or services making up the sector, or such associations or other bodies representing them as the Minister thinks appropriate; and

(c) consult such associations or other bodies representing the persons referred to in subparagraph (a)(iii) as the Minister thinks appropriate.

Note: For the meaning of ***SPF consumer***, see section 58AH.

(2) A failure to comply with subsection (1) does not invalidate an instrument made under subsection 58AC(1).

58AF Delegation

The Minister may, in writing, delegate the Minister's power to make an instrument under subsection 58AC(1) to another Minister.

Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations. For example, section 34A of that Act means that section 58AE of this Act can be satisfied by the delegate.

Subdivision C—Meanings of key terms

58AG Meaning of *scam*

(1) A ***scam*** is a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:

(a) involves deception (see subsection (2)); and

(b) would, if successful, cause loss or harm including obtaining SPF personal information of, or a financial or other benefit from, the SPF consumer or the SPF consumer's associates.

(2) The attempt involves deception if the attempt:

(a) deceptively represents something to be (or to be related to) the regulated service; or

(b) impersonates a regulated entity in connection with the regulated service; or

(c) is an attempt to deceive the SPF consumer into:

(i) performing an action using the regulated service; or

(ii) facilitating another person to perform an action using the regulated service; or

(d) is an attempt to deceive the SPF consumer that is made using the regulated service.

(3) The attempt may be a single act or a course of conduct.

(4) However, the attempt is not a ***scam*** if the attempt is of a kind prescribed by the SPF rules.

58AH Meaning of *SPF consumer*

(1) An ***SPF consumer***, of a regulated service, is any of the following:

(a) a natural person, or a small business operator, who is or may be provided or purportedly provided the service in Australia;

(b) a natural person who:

(i) is ordinarily resident in Australia; and

(ii) is or may be provided or purportedly provided the service outside of Australia by a regulated entity that satisfies the residency requirements in subsection (2).

(2) The regulated entity satisfies the residency requirements if it:

(a) is an Australian resident (within the meaning of the Income Tax Assessment Act 1997); or

(b) is so providing or purportedly providing the service through a permanent establishment (within the meaning of the *Income Tax Assessment Act 1997*) in Australia.

Note 1: For paragraph (1)(a), a person who is a small business operator at the time the person is impacted by a scam continues to be an SPF consumer *for that time* even if the business later has 100 or more employees.

Note 2: Sections 58GA to 58GC extend the meaning of ***person*** for partnerships, unincorporated associations and trusts.

(3) Subsection (1) includes the provision or purported provision of a regulated service:

(a) directly or indirectly to the person; or

(b) whether or not under a contract, arrangement or understanding with the person; or

(c) whether or not the regulated entity providing the service knows that the person is:

(i) a natural person; or

(ii) a small business operator; or

(d) that involves the supply of goods.

Note: This is not an exhaustive list.

(4) However, the person is not an ***SPF consumer*** of the regulated service if a condition prescribed by the SPF rules applies to the person in relation to regulated services of that kind.

(5) In this section:

annual turnover has the same meaning as in the *Corporations Act 2001*.

related body corporate has the same meaning as in the *Corporations Act 2001*.

small business operator means a person who carries on a business if:

(a) in the case of the person being a body corporate:

(i) the sum of the person's employees, and the employees of any body corporate related to the person, is less than 100 employees; and

(ii) the person's annual turnover during the last financial year is less than $10 million; and

(b) in the case of the person not being a body corporate:

(i) the person has less than 100 employees; and

(ii) the person's annual turnover (worked out as if the person were a body corporate) during the last financial year is less than $10 million; and

(c) in every case—the business has a principal place of business in Australia.

(6) Section 4B (about consumers) does not apply to this Part.

58AI Meaning of *actionable scam intelligence*

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 relating to, connected with, or using a regulated service of the entity is a scam.

Note 1: Whether there are reasonable grounds for such a suspicion is an objective test. Relevant information for this test may include:

(a) information about the mechanism or identifier being used to scam SPF consumers, such as URLs, email addresses, phone numbers, social media profiles, digital wallets and bank account information of the scam promotors; and

(b) information about the suspected scammer; and

(c) information (including complaints) provided by SPF consumers.

Note 2: Gathering and reporting this information will minimise the harm from scams (see SPF principles 4 and 5 in Subdivisions E and F of Division 2).

Subdivision D—Extension to external Territories and outside of Australia

58AJ Extension to external Territories and outside of Australia

(1) Each of the following provisions (the ***SPF provisions***) extends to every external Territory:

(a) a provision of this Part;

(b) a provision of a legislative instrument made under this Part;

(c) another provision of this Act to the extent that it relates to a provision covered by paragraph (a) or (b);

(d) a provision of the Regulatory Powers Act to the extent that it applies in relation to a provision covered by paragraph (a) or (b).

(2) The SPF provisions extend to acts, omissions, matters and things outside Australia.

Subdivision E—Application to acts done by or in relation to agents etc. of regulated entities

58AK Acts done by or in relation to agents etc. of regulated entities

Conduct of agents etc. of a regulated entity is attributable to the regulated entity

(1) For the purposes of the SPF provisions, section 97 of the Regulatory Powers Act (to the extent that it applies in relation to the SPF provisions) applies to a regulated entity who is not a body corporate in a corresponding way to the way that provision applies to a regulated entity who is a body corporate.

Acts done in relation to an agent of a regulated entity taken to be done in relation to the regulated entity

(2) For the purposes of SPF provisions, if an act is done by a person in relation to another person (the ***agent***) who:

(a) is acting on behalf of a regulated entity; and

(b) is so acting within the scope of the agent's actual or apparent authority;

the act is taken to have also been done in relation to the regulated entity.

Division 2—Overarching principles of the Scams Prevention Framework

Subdivision A—Preliminary

58BA Simplified outline of this Division

Each regulated entity must comply with the overarching principles of the Scams Prevention Framework.

These principles require each regulated entity to:

(a) document and implement governance arrangements to combat scams; and

(b) take reasonable steps to prevent, detect, report, disrupt and respond to scams.

These requirements are civil penalty provisions. The Commission (in its capacity as the SPF general regulator) will monitor, investigate and enforce compliance with these provisions. Division 6 sets out remedies for non-compliance with these provisions.

58BB Meaning of *reasonable steps*

Matters relevant to whether a regulated entity has taken ***reasonable steps*** for the purposes of a provision of this Division include:

(a) the size of the regulated entity; and
(b) the kind of regulated services concerned; and
(c) the consumer base of those services; and
(d) the kinds of scam risks those services face; and
(e) whether the regulated entity has complied with any relevant SPF code obligations relating to that provision.

Subdivision B—SPF principle 1: Governance

58BC Simplified outline of this Subdivision

Each regulated entity must document and implement governance policies, procedures, metrics and targets for combatting scams.

These must be reviewed, and certified by a senior officer of the entity, at least annually.

The entity must keep records and give reports about its compliance with this principle.

The SPF code for the sector may include sector-specific provisions for this principle.

58BD Documenting and implementing governance policies and procedures—civil penalty provision

(1) A regulated entity for a regulated sector contravenes this subsection if the entity fails to do one or more of the following:

(a) document governance policies and procedures about:

(i) preventing, detecting and disrupting scams; and

(ii) responding to scams; and

(iii) reports relating to scams;

relating to, connected with, or using the entity's regulated services for the sector;

(b) implement those governance policies and procedures;

(c) develop and implement performance metrics and targets that:

(i) are for measuring the effectiveness of those governance policies and procedures; and

(ii) comply with any requirements for those metrics and targets that are prescribed by the SPF rules.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BE Annual certification about SPF governance policies, procedures, metrics and targets—civil penalty provision

(1) A regulated entity for a regulated sector contravenes this subsection if:

(a) no senior officer of the entity certifies in writing, within 12 months of the day the entity becomes a regulated entity for the sector, whether the entity's SPF governance policies, procedures, metrics and targets for the sector comply with this Subdivision; or

(b) no senior officer of the entity certifies in writing, within 7 days after each 12-month anniversary of the day the entity becomes a regulated entity for the sector, whether the entity's SPF governance policies, procedures, metrics and targets for the sector comply with this Subdivision.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BF Record keeping of compliance with SPF provisions—civil penalty provision

(1) A regulated entity for a regulated sector contravenes this subsection if the entity fails to keep records of information of a material nature relating to each of the following activities for at least 6 years after that activity happens:

(a) the initial documenting, and each revision of the documenting, of the entity's SPF governance policies, procedures, metrics and targets for the sector;

(b) the initial implementation, and each reimplementation, of those SPF governance policies, procedures, metrics and targets;

(c) each consideration (including certification) by one of the entity's senior officers of those SPF governance policies, procedures, metrics and targets, including in relation to their documenting, implementation and review;

(d) any other activities that are prescribed by the SPF rules.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BG Reporting about compliance with this Subdivision—civil penalty provision

(1) A regulated entity for a regulated sector contravenes this subsection if:

(a) the SPF general regulator, or the SPF sector regulator for the sector, gives the entity a written request for a copy of:

(i) the entity's SPF governance policies, procedures, metrics and targets for the sector; or

(ii) specified kinds of other records required by this Subdivision to be kept for the sector by the entity; and

(b) the entity fails to comply with the request within:

(i) 10 business days after the day the entity is given the request; or

(ii) such longer period as is allowed by the SPF regulator.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BH Sector-specific details can be set out in SPF codes

For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions describing:

(a) the matters that a regulated entity for the sector must include in the entity's governance policies and procedures for the purposes of this Subdivision; or

(b) the factors that a regulated entity for the sector must have regard to when developing the entity's governance policies and procedures for the purposes of this Subdivision.

Subdivision C—SPF principle 2: Prevent

58BI Simplified outline of this Subdivision

Each regulated entity for a regulated sector must take reasonable steps to prevent scams.

The SPF code for the sector may include sector-specific provisions for this principle.

58BJ Taking reasonable steps to prevent scams from being committed—civil penalty provision

(1) A regulated entity contravenes this subsection if the entity fails to take reasonable steps to prevent another person from committing a scam relating to, connected with, or using a regulated service of the entity.

Note: Sections 58GA to 58GC extend the meaning of ***person*** for partnerships, unincorporated associations and trusts.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BK Further detail about certain concepts

(1) Taking reasonable steps for the purposes of subsection 58BJ(1) requires more than merely acting on actionable scam intelligence in the form of information provided to the regulated entity by another person.

Further sector-specific details can be set out in SPF codes

(2) For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions:

(a) describing what are reasonable steps for the purposes of this Subdivision (see also section 58BB); or

(b) requiring each regulated entity for the sector to:

(i) identify its SPF consumers who are at risk of being targeted by a scam; or

(ii) identify its SPF consumers who have a higher risk of being targeted by a scam; or

(c) requiring each regulated entity for the sector to provide information about such scams to an SPF consumer described in subparagraph (b)(i) or (ii).

Subdivision D—SPF principle 3: Detect

58BL Simplified outline of this Subdivision

Each regulated entity for a regulated sector must take reasonable steps to detect scams. This includes:

(a) investigating, in a timely way, activities that are the subjects of its actionable scam intelligence; and

(b) identifying, in a timely way, its consumers that have or may have been impacted by such activities.

The SPF code for the sector may include sector-specific provisions for this principle.

58BM Taking reasonable steps to detect scams—civil penalty provision

(1) A regulated entity contravenes this subsection if the entity fails to take reasonable steps to detect a scam relating to, connected with, or using a regulated service of the entity.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

(3) Without limiting subsection (1), the regulated entity fails to take reasonable steps to detect a scam relating to, connected with, or using a regulated service of the entity if the entity fails to take reasonable steps to:

(a) detect such a scam as it happens; or

(b) detect such a scam after it happens.

Note: For further details about the meaning of reasonable steps, see sections 58BB and 58BP.

58BN Investigating actionable scam intelligence—civil penalty provision

(1) A regulated entity contravenes this subsection if the entity:

(a) has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity; and

(b) fails to take reasonable steps to investigate whether or not the activity is a scam during the 28-day period starting on the day that the intelligence becomes actionable scam intelligence for the entity.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BO Identifying impacted SPF consumers—civil penalty provision

(1) A regulated entity contravenes this subsection if the entity:

(a) has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity; and

(b) fails to take reasonable steps within a reasonable time to identify the persons who were SPF consumers of that service at the time when the persons were or may have been impacted by the activity.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BP Sector-specific details can be set out in SPF codes

For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions describing:

(a) what are reasonable steps (see also section 58BB); or

(b) what is a reasonable time;

for the purposes of this Subdivision.

Subdivision E—SPF principle 4: Report

58BQ Simplified outline of this Subdivision

Each regulated entity must give the SPF general regulator reports of any actionable intelligence the entity has about activities relating to, connected with, or using the entity's regulated services.

A regulated entity must give an SPF regulator a report about a scam if the SPF regulator requests.

The SPF general regulator may disclose information about scams to certain other entities.

58BR Reporting actionable scam intelligence to SPF regulators—civil penalty provision

(1) This section applies if a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity.

Civil penalty provision

(2) The entity contravenes this subsection if the entity fails to give a report about the actionable scam intelligence:

(a) to the SPF general regulator within the period, and in the manner and form, prescribed by the SPF rules; and

(b) that contains the kinds of information prescribed by the SPF rules.

Note: This subsection only applies to the entity when the SPF rules prescribe matters for paragraphs (a) and (b) that apply to the entity.

(3) Subsection (2) is a civil penalty provision.

Note: This means subsection (2) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

Defence

(4) Subsection (2) does not apply to the entity if circumstances of a kind prescribed by the SPF rules apply to the entity.

Note: A defendant bears an evidential burden in relation to the matter in this subsection (see section 96 of the Regulatory Powers Act).

Matters relevant to reports

(5) For the purposes of (but without limiting) subsection (2), the SPF rules may prescribe:

(a) that the report may be given via access to a specified data gateway, portal or website; and

(b) that the report include the sources or evidence that the entity has for that intelligence (see section 58AI); and

(c) different matters for different kinds of regulated entities.

Note: For more about the data gateways, portals or websites referred to in paragraph (a), see section 58BT.

(6) The report may be required to include SPF personal information.

58BS Reporting scams to SPF regulators—civil penalty provisions

(1) This section applies if an SPF regulator gives a written request to a regulated entity for the entity to give the SPF regulator a report

about a scam relating to, connected with, or using a regulated service of the entity.

Civil penalty provision

(2) The entity contravenes this subsection if the entity fails to give a report about the scam:

(a) to the SPF regulator within the period, and in the manner and form, set out in the request; and

(b) that contains the kinds of information set out in the request.

(3) Subsection (2) is a civil penalty provision.

Note: This means subsection (2) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

(4) For the purposes of (but without limiting) subsection (2), the SPF regulator's request may:

(a) provide that the report may be given via access to a specified data gateway, portal or website; and

(b) ask that the report set out:

(i) what loss or harm may have resulted from the scam, what disruptive actions the entity has taken and whether any of those actions have been reversed; and

(ii) what steps the entity is taking to disrupt similar scams, and to prevent loss or harm resulting from similar scams.

Note: For more about the data gateways, portals or websites referred to in paragraph (a), see section 58BT.

(5) The request may ask for the report to include SPF personal information. If so, the request must require the entity to de-identify the information unless the SPF regulator reasonably believes that doing so would not achieve the object of this Part.

(6) If:

(a) a regulated entity gives a scam report to an SPF regulator under this section; and

(b) another SPF regulator later requests a scam report under this section from the regulated entity about the same matters;

then, despite subsection (2), the later scam report need only state that an earlier scam report about those matters was given to the first-mentioned SPF regulator on a specified date and time.

Note: The SPF regulators can share the earlier scam report under Subdivision C of Division 5.

58BT Authorised third party data gateways, portals or websites for accessing reports

(1) The SPF rules may prescribe a scheme for authorising third parties to operate data gateways, portals or websites that give access to reports under this Division.

(2) For the purposes of (but without limiting) subsection (1), the SPF rules may include the following:

(a) provisions conferring functions or powers on the SPF general regulator under the scheme;

(b) the criteria for a person to be authorised under the scheme;

(c) provisions providing that authorisations may be granted subject to conditions, and that conditions may be imposed on an authorisation after it has been granted;

(d) provisions providing that authorisations may be granted at different levels corresponding to different risks;

(e) provisions specifying what a person authorised at a particular level is authorised to do (or not authorised to do);

(f) provisions dealing with the period, renewal, transfer, variation, suspension, revocation or surrender of authorisations;

(g) notification requirements on persons whose authorisations have been varied, suspended, revoked or surrendered;

(h) transitional rules for when an authorisation is varied, is suspended or ends, including in relation to SPF personal information;

(i) provisions for the making of applications for internal review, or of applications to the Administrative Review Tribunal for review, of decisions of a person under the scheme.

(3) A person authorised under the scheme may use or disclose SPF personal information to the extent that this is reasonably necessary to achieve the object of this Part.

58BU Relationship with other duties and obligations

A duty of confidence owed under an agreement or arrangement is of no effect to the extent that it is contrary to section 58BR or 58BS.

Note: Each of sections 58BR and 58BS is also a requirement by law to disclose the information contained in the report referred to in that section. So, complying with that section can be a defence to a secrecy provision such as section 276 of the *Telecommunications Act 1997* (see paragraph 280(1)(b) of that Act).

58BV SPF general regulator may share information relating to scamming actions with relevant entities

(1) The SPF general regulator may disclose information relating to either of the following actions (a ***scamming action***):

(a) a scam (as defined in section 58AG);

(b) a scam (within the ordinary meaning of that expression);

to an entity mentioned in subsection (2).

Note 1: This includes disclosing SPF personal information, but such information may first need to be de-identified (see subsection (4)).

Note 2: The SPF general regulator can also disclose the information to an SPF sector regulator (see section 58EG).

(2) The entities are as follows:

(a) a regulated entity;

(b) a Commonwealth agency or authority involved in developing Government policy relating to this Part;

(c) a law enforcement agency of the Commonwealth, or of a State or Territory;

(d) an agency of a foreign country, or of part of a foreign country, that:

(i) is a law enforcement agency; or

(ii) is a regulatory agency responsible for scam prevention;

if subsection (3) applies to a disclosure of information to the agency.

(3) This subsection applies to a disclosure of information to a foreign agency if the SPF general regulator is satisfied that:

(a) the agency has given an undertaking for the following:

(i) controlling the storage and handling of the information;
(ii) controlling the use that will be made of the information;
(iii) ensuring that the information will be used only for the purpose for which it is disclosed to the agency; and

(b) it is appropriate, in all the circumstances, to disclose the information to the agency.

(4) SPF personal information may be disclosed under subsection (1). However, for a disclosure to an entity mentioned in paragraph (2)(b) such information must be de-identified unless the SPF general regulator reasonably believes that doing so would not achieve the object of this Part.

Subdivision F—SPF principle 5: Disrupt

58BW Simplified outline of this Subdivision

Each regulated entity for a regulated sector must take reasonable steps to:

(a) disrupt an activity that is the subject of actionable scam intelligence; and

(b) prevent losses from such an activity.

The entity will also need to report to the SPF general regulator the outcomes of the entity's investigation about whether such an activity is a scam. The report may also need to describe any disruptive actions the entity has taken in relation to the activity.

The entity is not liable for damages etc. in taking certain actions to disrupt such an activity.

The SPF code for the sector may include sector-specific provisions for this principle.

58BX Taking reasonable steps to disrupt activities that are the subjects of actionable scam intelligence—civil penalty provision

(1) A regulated entity contravenes this subsection if the entity:

(a) has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity; and

(b) fails to take reasonable steps within a reasonable time to:

(i) disrupt the activity; or

(ii) prevent loss or harm (including further loss or harm) arising from the activity.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

(3) For the purposes of subsection (1), the steps taken should be proportionate to the actionable scam intelligence that the entity has.

Note 1: For example, if a bank has received a substantial number of similar reports of suspicious activities, it may be appropriate to pause or delay authorised push payments while the bank investigates these suspicious activities.

Note 2: For further details about the meaning of reasonable steps, see sections 58BB and 58BZ.

58BY Reporting about the outcomes of investigations of activities that are the subjects of actionable scam intelligence—civil penalty provision

(1) This section applies if a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity.

Civil penalty provision

(2) The entity contravenes this subsection if the entity fails to give a report about the actionable scam intelligence:

(a) to the SPF general regulator:

(i) before the end of the period prescribed by the SPF rules that starts at the end of the period referred to in paragraph 58BZA(2)(d) for that intelligence; and

(ii) in the manner and form prescribed by the SPF rules; and

(b) that contains the kinds of information prescribed by the SPF rules.

Note: This subsection only applies to the entity when the SPF rules prescribe matters for paragraphs (a) and (b) that apply to the entity.

(3) Subsection (2) is a civil penalty provision.

Note: This means subsection (2) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

(4) For the purposes of (but without limiting) subsection (2), the SPF rules may prescribe:

(a) that the report may be given via access to a specified data gateway, portal or website; and

(b) that the report set out whether the entity reasonably believes that the activity that is the subject of the intelligence is a scam; and

(c) different matters for different kinds of regulated entities.

Note: For more about the data gateways, portals or websites referred to in paragraph (a), see section 58BT.

(5) The report may be required to include SPF personal information.

(6) A duty of confidence owed under an agreement or arrangement is of no effect to the extent that it is contrary to this section.

58BZ Sector-specific details can be set out in SPF codes

For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions:

(a) describing what are reasonable steps (see also section 58BB), or what is a reasonable time, for the purposes of this Subdivision; or

(b) requiring each regulated entity for the sector to provide its SPF consumers with information about activities that are the subjects of the entity's actionable scam intelligence.

58BZA Safe harbour for taking actions to disrupt an activity while investigating whether the activity is a scam

(1) This section applies if a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity.

(2) The regulated entity is not liable in a civil action or civil proceeding for taking action to disrupt the activity if the action:

(a) is taken in good faith; and

(b) is taken in compliance with the SPF provisions; and

(c) is reasonably proportionate to the activity, and to information that would reasonably be expected to be available to the entity about the activity; and

(d) is taken during the period:

(i) starting on the day that the intelligence becomes actionable scam intelligence for the entity; and

(ii) ending when the entity reasonably believes that the activity is or is not a scam, or after 28 days, whichever is the earlier; and

(e) is promptly reversed if:

(i) the entity identifies that the activity is not a scam; and

(ii) it is reasonably practicable to reverse the action.

Note: Assume the regulated entity temporarily blocks an SPF consumer's website while investigating whether an activity relating to the website is a scam. This subsection protects the regulated entity from civil actions brought by the consumer when the regulated entity is acting appropriately.

(3) For the purposes of paragraph (2)(c), matters relevant to whether the action is reasonably proportionate to the activity include:

(a) the potential loss or damage to SPF consumers, or to persons carrying on the activity, if the action is not taken; and

(b) the potential loss or damage to SPF consumers, or to persons carrying on the activity, if the action is taken and the activity is not a scam.

Subdivision G—SPF principle 6: Respond

58BZB Simplified outline of this Subdivision

Each regulated entity must have an accessible mechanism for its consumers to report activities that are or may be scams.

The entity must have an accessible and transparent internal dispute resolution mechanism for its consumers to complain about:

(a) activities that are or may be scams; or
(b) the entity's conduct relating to such activities.

The entity must publish information about these mechanisms.

When undertaking such internal dispute resolution, the entity must have regard to:

(a) any processes prescribed by the SPF rules; and
(b) any guidelines prescribed by the SPF rules for apportioning any liability.

The entity must become a member of an authorised external dispute resolution scheme for dealing with complaints about scams if the entity provides services regulated by the Scams Prevention Framework.

The SPF code for the sector may include sector-specific provisions for this principle.

58BZC Enabling SPF consumers to easily report activities that are or may be scams—civil penalty provision

(1) A regulated entity contravenes this subsection if the entity does not have an accessible mechanism for a person to report to the entity an activity that:

(a) is or may be a scam; and
(b) relates to, is connected with, or uses a regulated service of the entity; and
(c) impacts the person at a time when the person is an SPF consumer of the service.

Note: The reporting mechanism will need to extend to scams impacting the person at a time when the regulated service is only purportedly being provided to the person (see subsection 58AH(1) (about the meaning of SPF consumer)).

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BZD Having an accessible and transparent internal dispute resolution mechanism—civil penalty provision

(1) A regulated entity contravenes this subsection if the entity does not have an accessible and transparent internal dispute resolution mechanism to deal with a person's complaint about:

(a) an activity that:

(i) is or may be a scam; and

(ii) relates to, is connected with, or uses a regulated service of the entity; and

(iii) impacts the person at a time when the person is an SPF consumer of the service; or

(b) the entity's conduct relating to an activity of a kind described in paragraph (a).

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BZE Having regard to processes and guidelines when undertaking internal dispute resolution—civil penalty provision

(1) A regulated entity contravenes this subsection if the entity:

(a) is undertaking internal dispute resolution in dealing with a person's complaint of a kind described in paragraph 58BZD(1)(a) or (b); and

(b) in doing so, the entity fails to have regard to:

(i) any process prescribed by the SPF rules for undertaking internal dispute resolution; or

(ii) any guidelines prescribed by the SPF rules for apportioning any liability arising from the complaint.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BZF Publishing information about reporting and dispute resolution mechanisms—civil penalty provision

(1) A regulated entity for a regulated sector contravenes this subsection if the entity fails to make publicly accessible information about the rights of SPF consumers of the entity's regulated services for the sector under:

(a) the reporting mechanism required by subsection 58BZC(1); or

(b) the internal dispute resolution mechanism required by subsection 58BZD(1); or

(c) if the entity is a member of an SPF EDR scheme for the sector—the SPF EDR scheme.

(2) Subsection (1) is a civil penalty provision.

Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BZG SPF external dispute resolution schemes—civil penalty provisions

Regulated entity must not provide a regulated service if the entity is not a member of an SPF EDR scheme

(1) A regulated entity for a regulated sector contravenes this subsection if the entity:

(a) provides a regulated service for the sector that has one or more SPF consumers; and

(b) is not a member of an SPF EDR scheme for the sector.

Regulated entity that is a member of an SPF EDR scheme must give reasonable assistance to, and cooperate with, the scheme operator

(2) A regulated entity for a regulated sector contravenes this subsection if the entity:

(a) is a member of an SPF EDR scheme for the sector; and

(b) fails to give reasonable assistance to, or cooperate with, the operator of the scheme.

Regulated entity that is a member of an SPF EDR scheme must comply with related obligations in an SPF code

(3) A regulated entity for a regulated sector contravenes this subsection if the entity:

(a) is a member of an SPF EDR scheme for the sector; and

(b) fails to comply with an obligation in the SPF code for the sector that relates to the scheme.

Civil penalty provisions

(4) Subsections (1), (2) and (3) are civil penalty provisions.

Note: This means these subsections are ***civil penalty provisions of an SPF principle*** for the purposes of section 58FJ (about civil penalties).

58BZH Sector-specific details can be set out in SPF codes

For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions setting out:

(a) conditions that must be met for a reporting mechanism required by subsection 58BZC(1); or

(b) conditions (such as standards and requirements) that must be met for an internal dispute resolution mechanism required by subsection 58BZD(1); or

(c) obligations that must be met in relation to an SPF EDR scheme for the sector by a regulated entity for the sector that is a member of the scheme.

Division 3—Sector-specific codes for the Scams Prevention Framework

58CA Simplified outline of this Division

The Minister may make a code for each regulated sector.

Each code is to include sector-specific provisions for the following overarching principles of the Scams Prevention Framework (see Subdivisions B, C, D, F and G of Division 2):

(a) SPF principle 1—governance;
(b) SPF principle 2—prevent;
(c) SPF principle 3—detect;
(d) SPF principle 5—disrupt;
(e) SPF principle 6—respond.

Requirements in a code can be civil penalty provisions. The relevant SPF sector regulator will monitor, investigate and enforce compliance with these provisions. Division 6 sets out remedies for non-compliance with these provisions.

58CB Sector-specific codes (SPF codes)

The Minister may, by legislative instrument, make a code (an ***SPF code***) for a regulated sector.

58CC Content of SPF codes

Main rule about the content of SPF codes

(1) An SPF code must:
(a) be consistent with the SPF principles; and
(b) deal with only:
(i) the themes or matters covered by Subdivisions B, C, D, F and G of Division 2; and
(ii) related or incidental matters; and
(c) subject to paragraphs (a) and (b), include provisions about matters of a kind (if any) prescribed by the SPF rules.

Related or incidental matters in SPF codes

(2) Without limiting subparagraph (1)(b)(ii), an SPF code for a regulated sector may include the following:
(a) provisions relating to only certain kinds of regulated services for the sector;
(b) provisions relating to only certain kinds of SPF consumers of regulated services for the sector;

(c) provisions dealing with the circumstances in which entities are, or may be, relieved from complying with requirements in the SPF code that would otherwise apply to them;

(d) a provision that:

(i) confers powers on the SPF sector regulator for the sector or on another person; or

(ii) depends on the SPF sector regulator for the sector, or another person, being satisfied of one or more specified matters;

(e) provisions for the making of applications for internal review, or of applications to the Administrative Review Tribunal for review, of decisions of a person under the SPF code;

(f) provisions about the manner or form in which persons or bodies:

(i) may exercise powers under the SPF code; or

(ii) must comply with requirements imposed by the SPF code;

which could include requiring the use of a form approved by the SPF sector regulator for the sector or by the SPF general regulator;

(g) provisions about the following matters:

(i) whether a regulated entity for the sector may charge (or cause to be charged) a fee for a matter covered by the SPF code;

(ii) the manner in which such a fee may be charged;

(iii) the time for paying such a fee;

(iv) giving notice of, or publicising, such a fee or matters about such a fee;

(h) provisions requiring agents of a regulated entity for the sector to do or not to do specified things when acting on behalf of the regulated entity and within the scope of the agent's actual or apparent authority;

(i) provisions authorising a regulated entity for the sector to use or disclose SPF personal information to the extent necessary to comply with the entity's obligations under the code;

(j) provisions about any other matters that the provisions of this Part provide may be included, or otherwise dealt with, in the SPF code.

Civil penalty provisions of the SPF code

(3) An SPF code may provide that specified provisions of the SPF code are civil penalty provisions (within the meaning of the Regulatory Powers Act).

Note: Division 6 of this Part deals with enforcing the civil penalty provisions.

Adopting matters in instruments as in force from time to time etc.

(4) An SPF code may make provision in relation to a matter by applying, adopting or incorporating (with or without modification) any matter contained in any other instrument or writing:

(a) as in force or existing at a particular time; or

(b) as in force or existing from time to time.

(5) Subsection (4) has effect despite subsection 14(2) of the *Legislation Act 2003*.

58CD Delegation

The Minister may, in writing, delegate the Minister's power under section 58CB to make a code for a regulated sector to:

(a) another Minister; or

(b) the Commission; or

(c) the entity that is, or is to be, the SPF sector regulator for the sector.

Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

Division 4—External dispute resolution for the Scams Prevention Framework

58DA Simplified outline of this Division

One or more external dispute resolution schemes may be authorised for dealing with consumer complaints about scams relating to, connected with, or using regulated services.

An existing scheme like the AFCA scheme could be authorised for this purpose, or new schemes could be developed and authorised.

58DB Minister may authorise external dispute resolution schemes for a regulated sector

(1) The Minister may, by legislative instrument, authorise an external dispute resolution scheme (an ***SPF EDR scheme***) for the purposes of this Part and one or more regulated sectors if:

(a) the scheme is already authorised under a Commonwealth law for another purpose; or

(b) the Minister is satisfied that the requirements prescribed by the SPF rules for the purposes of subsection 58DC(1) are met for the scheme.

Note 1: For paragraph (a), the Minister could, for example, authorise the AFCA scheme (within the meaning of the *Corporations Act 2001*) to apply for the purposes of this Part and a regulated sector. If that happens, ASIC's functions and powers relating to the AFCA scheme (for example, under section 1052A of that Act) will also apply for the purposes of this Part and the regulated sector.

Note 2: For variation and repeal, see subsection 33(3) of the *Acts Interpretation Act 1901*.

(2) Before authorising a scheme, the Minister must consider:

(a) the accessibility of the scheme; and

(b) the independence of the scheme; and

(c) the fairness of the scheme; and

(d) the accountability of the scheme; and

(e) the efficiency of the scheme; and

(f) the effectiveness of the scheme; and

(g) any other matters the Minister considers relevant.

A failure to comply with this subsection does not invalidate an instrument made under subsection (1) authorising the scheme.

(3) An instrument made under subsection (1) may make the authorisation of the scheme subject to specified conditions.

(4) An instrument made under subsection (1) authorising a scheme for which paragraph (1)(b) applies must set out the scheme.

(5) More than one scheme may be authorised under subsection (1).

58DC Content, including requirements, of a scheme that is not already authorised under a Commonwealth law

(1) The SPF rules may prescribe the following requirements for a scheme for which paragraph 58DB(1)(b) is to apply:

(a) organisational requirements for membership of the scheme;

(b) requirements for the operator (the ***operator***) of the scheme;

(c) requirements for how the scheme is to operate;

(d) requirements to be complied with by members of the scheme;

(e) requirements for making changes to the scheme.

(2) A scheme for which paragraph 58DB(1)(b) is to apply may also include provisions dealing with the following:

(a) powers of one or more of the following under the scheme:

(i) the Minister;

(ii) an SPF regulator;

(iii) a Commonwealth entity (within the meaning of the *Public Governance, Performance and Accountability Act 2013*);

(b) powers of the operator under the scheme, including powers to:

(i) seek information; and

(ii) make determinations of complaints; and

(iii) make determinations imposing financial and non-financial remedies; and

(c) appeals to the Federal Court from such determinations by the operator;

(d) information sharing and reporting;

(e) a provision that depends on the operator or another person being satisfied of one or more specified matters;

(f) provisions about the following matters:

(i) the manner in which the operator may charge (or cause to be charged) a fee under the scheme;

(ii) the time for paying such a fee;

(iii) giving notice of, or publicising, such a fee or matters about such a fee;

(g) provisions about any other matters that the provisions of this Part provide may be specified, or otherwise dealt with, in the scheme.

58DD Scheme operator to report to SPF regulators

Referring contraventions, failures and systemic issues

(1) If the operator of an SPF EDR scheme for a regulated sector becomes aware that:

(a) a serious contravention of any law may have occurred in connection with a complaint under the scheme; or

(b) a party to a complaint under the scheme may have failed to give effect to a determination by the operator relating to the complaint; or

(c) there is a systemic issue arising from the consideration of complaints under the scheme;

the operator must give particulars of the contravention, failure or issue to the SPF general regulator and to the SPF sector regulator for the sector.

Referring settled complaints

(2) If:

(a) the parties to a complaint made under an SPF EDR scheme for a regulated sector agree to a settlement of the complaint; and

(b) the operator of the scheme thinks the settlement may require investigation;

the operator may give particulars of the settlement to the SPF general regulator and to the SPF sector regulator for the sector.

De-identifying any SPF personal information

(3) If any SPF personal information is to be given under subsection (1) or (2) by the operator of the scheme, the operator must de-identify the information unless the operator reasonably believes that doing so would not achieve the object of this Part.

58DE Disclosing information to the operator of an SPF EDR scheme

(1) An SPF regulator may disclose information to the operator of an SPF EDR scheme for the purposes of enabling or assisting the operator to perform any of the operator's functions or powers.

(2) The SPF regulator may impose conditions to be complied with by the operator in relation to the information.

(3) If an SPF regulator is to disclose SPF personal information under subsection (1), the SPF regulator must de-identify the information unless the SPF regulator reasonably believes that doing so would not achieve the object of this Part.

Division 5—Regulating the Scams Prevention Framework

Subdivision A—Preliminary

58EA Simplified outline of this Division

The Commission is the regulator (the ***SPF general regulator***) of most aspects of the Scams Prevention Framework, in particular of the overarching principles of the Framework.

Other Commonwealth entities may be selected to be regulators (***SPF sector regulators***) of each of the SPF codes.

The SPF general regulator must enter into arrangements with the SPF sector regulators about the regulation and enforcement of the Framework. These regulators may disclose relevant information and documents to each other for this purpose.

Subdivision B—Regulators of the Scams Prevention Framework

58EB General regulator of the Scams Prevention Framework

(1) The Commission is the ***SPF general regulator*** for all SPF provisions apart from the provisions of SPF codes.

(2) The functions and powers of the SPF general regulator include:

(a) reviewing, and advising the Minister about, the operation of the SPF provisions; and

(b) the Commission's functions and powers under section 155 to the extent that section 155 relates to:

(i) the SPF provisions, other than the provisions of SPF codes; or

(ii) a designated scams prevention framework matter (within the meaning of that section), other than the performance of a function, or the exercise of a power, conferred by or under an SPF code; and

(c) developing and publishing non-binding guidance material relating to the SPF provisions, other than the provisions of SPF codes; and

(d) the functions and powers of the SPF general regulator conferred by any other SPF provisions.

Note: Paragraph (d) includes the SPF general regulator's powers under the Regulatory Powers Act that are referred to in Division 6.

58EC Delegation of the SPF general regulator's functions and powers

(1) The Commission may, by resolution, delegate any of:

(a) the Commission's functions and powers (as the SPF general regulator) under an SPF provision; or

(b) the Commission's functions and powers under section 155 as described in paragraph 58EB(2)(b);

to a person to whom subsection (3) applies.

(2) A member of the Commission may, by writing, delegate any of the member's functions and powers under section 155 to the extent that section 155 relates to:

(a) the SPF provisions, other than the provisions of SPF codes; or

(b) a designated scams prevention framework matter (within the meaning of that section), other than the performance of a function, or the exercise of a power, conferred by or under an SPF code;

to a person to whom any of paragraphs (3)(b) to (e) applies.

(3) This subsection applies to the following persons:
  (a) a member of the Commission;
  (b) person who is an employee of the Commission who:
    (i) is an SES employee or acting SES employee; or
    (ii) holds or performs the duties of an Executive Level 1 or 2 position;
  and who the Commission is satisfied has appropriate qualifications, training, skills or experience to perform the functions or exercise the powers;
  (c) an SPF sector regulator;
  (d) a member (if any) of an SPF sector regulator;
  (e) an employee of an SPF sector regulator who holds or performs the duties of a position that is equivalent to a position mentioned in subparagraph (b)(i) or (ii).

(4) A delegation of functions or powers must not be made under subsection (1) or (2) to a person to whom paragraph (3)(c), (d) or (e) applies unless the relevant SPF sector regulator:
  (a) has agreed to the delegation in writing; and
  (b) in the case of a person to whom paragraph (3)(e) applies—is satisfied that the person has appropriate qualifications, training, skills or experience to perform the functions or exercise the powers.

(5) In performing any functions or exercising any powers under a delegation under subsection (1) or (2), the delegate must comply with any directions of the delegator.

58ED Regulator of a regulated sector

(1) The Minister may, by legislative instrument, designate an entity that:
  (a) is a Commonwealth entity (within the meaning of the *Public Governance, Performance and Accountability Act 2013*); and
  (b) is already conferred functions by or under a law;
to be the ***SPF sector regulator*** for a regulated sector.

(2) The Commission is the ***SPF sector regulator*** for a regulated sector if (and while) no instrument under subsection (1) is in force for the sector.

Note: The Commission could also be designated under subsection (1) to be the SPF sector regulator for a regulated sector.

(3) The functions and powers of the SPF sector regulator for a regulated sector include those conferred:

(a) by the SPF code for the sector; or

(b) by any other SPF provisions; or

(c) if the SPF sector regulator is the Commission—the Commission's functions and powers under section 155 to the extent that section 155 relates to:

(i) the provisions of the SPF code for the sector; or

(ii) a designated scams prevention framework matter (within the meaning of that section) involving the performance of a function, or the exercise of a power, conferred by or under the SPF code for the sector.

Note: The functions and powers of SPF regulators other than the Commission include the monitoring and investigating functions and powers referred to in Division 6 (see paragraph (b) of this subsection).

(4) The Minister may, in writing, delegate the Minister's power under subsection (1) to another Minister.

Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

58EE Delegation of an SPF sector regulator's functions and powers

(1) An SPF sector regulator may, by writing, delegate any of the SPF sector regulator's functions and powers under:

(a) an SPF provision, other than a provision of the Regulatory Powers Act; or

(b) if the SPF sector regulator is the Commission—the Commission's functions and powers under section 155 as described in paragraph 58ED(3)(c);

to a person to whom subsection (3) applies.

Note: A function or power of the SPF sector regulator under a provision of the Regulatory Powers Act may be able to be delegated under the Subdivision of Division 6 of this Part that refers to that provision of that Act (for example, see subsection 58FE(5) of this Act).

(2) If an SPF sector regulator is the Commission, a member of the Commission may, by writing, delegate any of the member's

functions and powers under section 155 to the extent that section 155 relates to:

(a) the provisions of the SPF code for the sector; or

(b) a designated scams prevention framework matter (within the meaning of that section) involving the performance of a function, or the exercise of a power, conferred by or under the SPF code for the sector;

to a person to whom paragraph (3)(b) applies.

(3) This subsection applies to the following persons:

(a) a member (if any) of the SPF sector regulator;

(b) person who is an employee of the SPF sector regulator who:

(i) is an SES employee or acting SES employee; or

(ii) holds or performs the duties of an Executive Level 1 or 2 position; or

(iii) holds or performs the duties of a position that is equivalent to a position mentioned in subparagraph (i) or (ii);

and who the SPF sector regulator is satisfied has appropriate qualifications, training, skills or experience to perform the functions or exercise the powers.

(4) In performing any functions or exercising any powers under a delegation under subsection (1) or (2), the delegate must comply with any directions of the delegator.

58EF Arrangements for regulating the Scams Prevention Framework

(1) The SPF general regulator, and each SPF sector regulator, must enter into an arrangement relating to the regulation and enforcement of the SPF provisions.

(2) The SPF general regulator may choose to comply with subsection (1) by entering into:

(a) a single arrangement with all, or one or more, SPF sector regulators; or

(b) a separate arrangement with each SPF sector regulator.

However, subsection (1) does not apply to the extent that the Commission is an SPF sector regulator.

(3) The arrangement must include provisions relating to the matters (if any) prescribed by the SPF rules.

Note: For example, the SPF rules could require an SPF regulator that requests a scam report under subsection 58BS(1) to:

(a) notify each other SPF regulator of the request; and

(b) give a copy of the scam report to any of those other SPF regulators that asks for one.

(4) Each SPF regulator that is a party to such an arrangement must publish the arrangement on its website.

(5) A failure to comply with this section does not invalidate the performance or exercise of a function or power by an SPF regulator.

Subdivision C—Information sharing between SPF regulators

58EG SPF regulators may disclose information to each other

(1) An SPF regulator may disclose to another SPF regulator:

(a) particular information or documents; or

(b) information or documents of a particular kind;

held by the first-mentioned SPF regulator that are relevant to the operation (including enforcement) of the SPF provisions.

(2) An SPF regulator may make a disclosure under subsection (1) on request or on its own initiative.

Note: This section means such a disclosure is permitted by provisions like:

(a) paragraph 155AAA(1)(b); and

(b) section 59DB of the *Australian Communications and Media Authority Act 2005*; and

(c) subsection 127(2) of the *Australian Securities and Investments Commission Act 2001*.

Similarly, the exception in paragraph 6.2(b) of Australian Privacy Principle 6 will apply to such a disclosure.

(3) SPF personal information may be disclosed under subsection (1).

58EH Regard must be had to the object of this Part when considering whether to make such a disclosure

An SPF regulator must have regard to the object of this Part when deciding whether to make a disclosure under this Subdivision.

Note: Arrangements made under section 58EF between SPF regulators could deal with when disclosures should be made (see subsection 58EF(3) in particular).

58EI Notice need not be given of a collection, use or disclosure of information or documents under this Part

An SPF regulator need not notify any person that the SPF regulator:

(a) has collected SPF personal information under this Part; or

(b) plans to make a disclosure of information or documents under this Part; or

(c) has made such a disclosure under this Part; or

(d) plans to use information or documents disclosed under this Part; or

(e) has used such information or documents under this Part.

58EJ Information that need not be disclosed

Nothing in this Part requires an SPF regulator to disclose information or documents that:

(a) concern the internal administrative functioning of that regulator; or

(b) disclose a matter in respect of which that regulator or any other person has claimed legal professional privilege; or

(c) are of a kind prescribed by the SPF rules.

Division 6—Enforcing the Scams Prevention Framework

Subdivision A—Preliminary

58FA Simplified outline of this Division

The Commission, in its role as the SPF general regulator or an SPF sector regulator, may use its powers under this Act (including section 155) to monitor and investigate compliance with the aspects of the Scams Prevention Framework that are relevant for that role.

If the ACMA or ASIC is an SPF sector regulator, it must use powers in its own legislation to monitor and investigate compliance with an SPF code for the sector. Other SPF sector regulators may monitor and investigate compliance with an SPF code either using the powers in Subdivision B or, with the Minister's permission, powers in their own legislation.

The maximum penalties for contraventions of the civil penalty provisions of the Scams Prevention Framework are set out in Subdivision C.

Other remedies for contraventions of the Framework are set out in later Subdivisions of this Division, and include:

(a) infringement notices; and
(b) enforceable undertakings; and
(c) injunctions; and
(d) actions for damages; and
(e) public warning notices; and
(f) remedial directions; and
(g) adverse publicity orders; and
(h) other punitive and non-punitive orders.

Some of these remedies may also be available against a person involved in a contravention of the Framework by a regulated entity, such as a senior officer of the regulated entity (for example, see subsection 58FW(1)).

Note: Sections 58GA to 58GC extend the meaning of ***person*** for partnerships, unincorporated associations and trusts.

58FB Appointment of inspectors

(1) An SPF regulator may, in writing, appoint a person who is one of the following to be an ***inspector*** of that regulator for the purposes of one or more Subdivisions of this Division:

(a) a person who is an employee of that regulator who:

(i) is an SES employee or acting SES employee; or

(ii) holds or performs the duties of an Executive Level 1 or 2 position; or

(iii) holds or performs the duties of a position that is equivalent to a position mentioned in subparagraph (i) or (ii);

(b) a member or special member of the Australian Federal Police.

(2) However, the SPF regulator must not appoint a person as an inspector unless the SPF regulator is satisfied that the person has appropriate qualifications, training, skills or experience to exercise the powers of an inspector.

(3) A person must, in exercising powers as an inspector of an SPF regulator, comply with any directions of the SPF regulator that are of an administrative character.

(4) If (and while) no appointments under subsection (1) by an SPF regulator are in force for the purposes of a Subdivision of this Division, the SPF regulator is an ***inspector*** of the SPF regulator for the purposes of that Subdivision.

58FC Multiple remedies can be sought for a single contravention

Subject to section 58FM (about civil penalties), a provision of this Division does not limit a court's powers under any other provision of this Act or of any other Act.

58FD Preference must be given to compensation for victims

If a court considers that:

(a) it is appropriate to order a person (the ***defendant***) to pay a pecuniary penalty under an SPF civil penalty order in relation to a contravention or conduct; and

(b) it is appropriate to order under Subdivision G the defendant to pay compensation to a person who has suffered loss or damage as result of that contravention or conduct; and

(c) the defendant does not have sufficient financial resources to pay both the pecuniary penalty and the compensation;

the court must give preference to making an order for compensation.

Subdivision B—Monitoring or investigating compliance with an SPF code

58FE Monitoring compliance with an SPF code—default

No alternative monitoring powers apply

(1) This section applies for the SPF code for a regulated sector unless:

(a) the ACMA, ASIC or the Commission is the SPF sector regulator for the sector; or

(b) a declaration is in force under subsection 58FI(2) declaring that provisions that include monitoring powers of the kind mentioned in subparagraph 58FI(1)(a)(i) apply in relation to provisions of the SPF code.

Provisions subject to monitoring

(2) Each provision of the SPF code is subject to monitoring under Part 2 of the Regulatory Powers Act.

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether these provisions have been complied with. That Part includes powers of entry and inspection.

Information subject to monitoring

(3) Information given in compliance or purported compliance with the SPF code is subject to monitoring under Part 2 of the Regulatory Powers Act.

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the information is correct. It includes powers of entry and inspection.

Related provisions, authorised applicant, authorised person, issuing officer, relevant chief executive and relevant court

(4) For the purposes of Part 2 of the Regulatory Powers Act, as that Part applies in relation to the provisions mentioned in subsection (2) and the information mentioned in subsection (3):

(a) there are no related provisions; and

(b) an inspector of the SPF sector regulator is an authorised applicant; and

(c) an inspector of the SPF sector regulator is an authorised person; and

(d) a magistrate is an issuing officer; and

(e) the SPF sector regulator is the relevant chief executive; and

(f) each of the following courts is a relevant court:

(i) the Federal Court;

(ii) the Federal Circuit and Family Court of Australia (Division 2);

(iii) a court of a State or Territory that has jurisdiction in relation to the matter.

(5) The relevant chief executive may, in writing, delegate the powers and functions mentioned in subsection (6) to:

(a) an SES employee, or acting SES employee, of the SPF sector regulator; or

(b) an employee of the SPF sector regulator who holds or performs the duties of a position that is equivalent to an SES employee;

if the relevant chief executive is satisfied that the employee has appropriate qualifications, training, skills or experience to exercise the powers and perform the functions.

(6) The powers and functions that may be delegated are:

(a) powers and functions under Part 2 of the Regulatory Powers Act in relation to the provisions mentioned in subsection (2) and the information mentioned in subsection (3); and

(b) powers and functions under the Regulatory Powers Act that are incidental to a power or function mentioned in paragraph (a) of this subsection.

(7) A person exercising powers or performing functions under a delegation under subsection (5) must comply with any directions of the relevant chief executive.

Person assisting

(8) An authorised person may be assisted by other persons in exercising powers or performing functions or duties under Part 2 of the Regulatory Powers Act in relation to the provisions mentioned in subsection (2) and the information mentioned in subsection (3).

58FF Investigating compliance with an SPF code—default

No alternative investigation powers apply

(1) This section applies for the SPF code for a regulated sector unless:

(a) the ACMA, ASIC or the Commission is the SPF sector regulator for the sector; or

(b) a declaration is in force under subsection 58FI(2) declaring that provisions that include investigation powers of the kind mentioned in subparagraph 58FI(1)(a)(ii) apply in relation to provisions of the SPF code.

Provisions subject to investigation

(2) Each civil penalty provision of the SPF code is subject to investigation under Part 3 of the Regulatory Powers Act.

Note: Part 3 of the Regulatory Powers Act creates a framework for investigating whether a provision has been contravened. It includes powers of entry, search and seizure.

Related provisions, authorised applicant, authorised person, issuing officer, relevant chief executive and relevant court

(3) For the purposes of Part 3 of the Regulatory Powers Act, as that Part applies in relation to evidential material that relates to a provision mentioned in subsection (2):

(a) there are no related provisions; and

(b) an inspector of the SPF sector regulator is an authorised applicant; and

(c) an inspector of the SPF sector regulator is an authorised person; and

(d) a magistrate is an issuing officer; and

(e) the SPF sector regulator is the relevant chief executive; and

(f) each of the following courts is a relevant court:

(i) the Federal Court;

(ii) the Federal Circuit and Family Court of Australia (Division 2);

(iii) a court of a State or Territory that has jurisdiction in relation to the matter.

(4) The relevant chief executive may, in writing, delegate the powers and functions mentioned in subsection (5) to:

(a) an SES employee, or acting SES employee, of the SPF sector regulator; or

(b) an employee of the SPF sector regulator who holds or performs the duties of a position that is equivalent to an SES employee.

if the relevant chief executive is satisfied that the employee has appropriate qualifications, training, skills or experience to exercise the powers and perform the functions.

(5) The powers and functions that may be delegated are:

(a) powers and functions under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (2); and

(b) powers and functions under the Regulatory Powers Act that are incidental to a power or function mentioned in paragraph (a).

(6) A person exercising powers or performing functions under a delegation under subsection (4) must comply with any directions of the relevant chief executive.

Person assisting

(7) An authorised person may be assisted by other persons in exercising powers or performing functions or duties under Part 3 of

the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (2).

58FG Monitoring or investigating—the ACMA

(1) This section applies if the ACMA is the SPF sector regulator for a regulated sector.

(2) Part 26 of the *Telecommunications Act 1997* also applies:

(a) to the ACMA in the ACMA's capacity as the SPF sector regulator; and

(b) in relation to a contravention of the SPF code for the sector in a corresponding way to the way that Part applies in relation to a contravention of that Act that does not relate to the content of a content service.

(3) Part 27 of the *Telecommunications Act 1997* also applies:

(a) to the ACMA in the ACMA's capacity as the SPF sector regulator; and

(b) in relation to the performance of any of the ACMA's functions under the SPF code for the sector in a corresponding way to the way that Part applies in relation to the performance of any of the ACMA's telecommunications functions; and

(c) in relation to the exercise of any of the ACMA's powers under the SPF code for the sector in a corresponding way to the way that Part applies in relation to the exercise of any of the ACMA's telecommunications powers.

(3) For the purposes of this additional application of Parts 26 and 27 of the *Telecommunications Act 1997*, the Minister may, by legislative instrument, specify modifications of one or more provisions of those Parts to remove any doubt about how those provisions apply in such a corresponding way in relation to the SPF code.

Note: The modifications are for this additional application of those Parts, and are not modifications of those Parts as they ordinarily apply.

(4) The instrument has effect accordingly.

(5) In this section:

ACMA's telecommunications functions has the same meaning as in the *Telecommunications Act 1997*.

ACMA's telecommunications powers has the same meaning as in the *Telecommunications Act 1997*.

content service has the same meaning as in the *Telecommunications Act 1997*.

58FH Monitoring or investigating—ASIC

(1) This section applies if ASIC is the SPF sector regulator for a regulated sector.

(2) ASIC's alternative power provisions also apply:

(a) to ASIC in ASIC's capacity as the SPF sector regulator; and

(b) in relation to the provisions of the SPF code for the sector in a corresponding way to the way:

(i) ASIC's alternative power provisions (other than those mentioned in subparagraph (ii)) apply in relation to the corporations legislation (other than the excluded provisions); and

(ii) sections 28, 30, 31 to 39, 39B and 39C and subsection 67(2) of the ASIC Act apply in relation to the corporations legislation.

(3) For the purposes of this additional application of ASIC's alternative power provisions, the Minister may, by legislative instrument, specify modifications of one or more of those provisions to remove any doubt about how those provisions apply in such a corresponding way in relation to the provisions of the SPF code.

Note: The modifications are for this additional application of ASIC's alternative power provisions, and are not modifications of those provisions as they ordinarily apply.

(4) The instrument has effect accordingly.

(5) In this section:

ASIC Act means the *Australian Securities and Investments Commission Act 2001*.

ASIC's alternative power provisions means Divisions 1, 2, 3 (other than sections 30A, 30B and 39A), 7, 9 and 10 of Part 3 of the ASIC Act.

corporations legislation has the same meaning as in the ASIC Act.

excluded provisions has the same meaning as in the ASIC Act.

58FI Monitoring or investigating—Minister may declare that alternative powers apply for other SPF sector regulators

(1) This section applies if provisions of another law (the ***alternative power provisions***):

(a) provide an entity with powers to:

(i) monitor compliance or purported compliance with provisions of a law (the ***alternative regulatory provisions***); or

(ii) investigate provisions of a law (also the ***alternative regulatory provisions***); or

(b) enable the effective operation and enforcement of such powers.

Note: Paragraph (b) covers, for example, a provision making it an offence to fail to appear to answer questions in relation to an investigation.

(2) The Minister may, by legislative instrument, declare that specified alternative power provisions (that relate to a specified entity and specified alternative regulatory provisions) also apply:

(a) to the entity in the entity's capacity as the SPF sector regulator for a regulated sector; and

(b) in relation to specified provisions of the SPF code for the sector in a corresponding way to the way the alternative power provisions apply in relation to the alternative regulatory provisions.

(3) For the purposes of this additional application of the alternative power provisions, the instrument may specify modifications of one or more of those provisions to remove any doubt about how those provisions apply in such a corresponding way in relation to the specified provisions of the SPF code.

Note: The modifications are for this additional application of the alternative power provisions, and are not modifications of those provisions as they ordinarily apply.

(4) The instrument has effect accordingly.

Subdivision C—Civil penalty provisions

58FJ Civil penalty provisions

Enforcing civil penalty provisions

(1) Each of the following is enforceable under Part 4 of the Regulatory Powers Act:

(a) a civil penalty provision of an SPF principle;

(b) a civil penalty provision of an SPF code.

Note: Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

Authorised applicant

(2) For the purposes of Part 4 of the Regulatory Powers Act:

(a) the SPF general regulator is an authorised applicant in relation to each civil penalty provision of an SPF principle; and

(b) the SPF sector regulator for a regulated sector is an authorised applicant in relation to each civil penalty provision of the SPF code for the sector.

Relevant court

(3) For the purposes of Part 4 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to each provision referred to in subsection (1):

(a) the Federal Court;

(b) the Federal Circuit and Family Court of Australia (Division 2);

(c) a court of a State or Territory that has jurisdiction in relation to the matter.

58FK Maximum penalty for tier 1 contraventions

(1) Despite subsection 82(5) of the Regulatory Powers Act, the pecuniary penalty payable by a person:

(a) under an SPF civil penalty order; and

(b) for a contravention of a civil penalty provision of an SPF principle in any of Subdivisions C, D, F or G of Division 2 of this Part;

must not be more than the maximum penalty amount worked out under this section for such a contravention by the person.

Maximum amount of civil penalty for bodies corporate

(2) For the purposes of subsection (1), the maximum penalty amount for such a contravention by a body corporate is the greater of the following:

(a) 159,745 penalty units;

(b) if the relevant court (see subsection 58FJ(3)) can determine the total value of the benefit that:

(i) the body corporate; and

(ii) any body corporate related to the body corporate;

have obtained directly or indirectly and that is reasonably attributable to the contravention—3 times that total value;

(c) if that court cannot determine that total value—30% of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

Maximum amount of civil penalty for other persons

(3) For the purposes of subsection (1), the maximum penalty amount for such a contravention by a person other than a body corporate is 7,990 penalty units.

58FL Maximum penalty for tier 2 contraventions

(1) Despite subsection 82(5) of the Regulatory Powers Act, the pecuniary penalty payable by a person:

(a) under an SPF civil penalty order; and

(b) for a contravention of:

(i) a civil penalty provision of an SPF principle in Subdivision B or E of Division 2 of this Part; or

(ii) a civil penalty provision of an SPF code;

must not be more than the maximum penalty amount worked out under this section for such a contravention by the person.

Maximum amount of civil penalty for bodies corporate

(2) For the purposes of subsection (1), the maximum penalty amount for such a contravention by a body corporate is the greater of the following:

(a) 31,950 penalty units;

(b) if the relevant court (see subsection 58FJ(3)) can determine the total value of the benefit that:

(i) the body corporate; and

(ii) any body corporate related to the body corporate;

have obtained directly or indirectly and that is reasonably attributable to the contravention—3 times that total value;

(c) if that court cannot determine that total value—10% of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

Maximum amount of civil penalty for other persons

(3) For the purposes of subsection (1), the maximum penalty amount for such a contravention by a person other than a body corporate is 1,600 penalty units.

58FM Civil penalty double jeopardy

If a person is ordered under an SPF civil penalty order to pay a pecuniary penalty in respect of particular conduct, the person is not liable to:

(a) a pecuniary penalty for contravening another civil penalty provision of an SPF principle or of an SPF code; or

(b) a pecuniary penalty under some other provision of a law of the Commonwealth;

in respect of that conduct.

Note: A court may make other kinds of orders under this Division, for example under section 58FZC (actions for damages), in relation to

particular conduct even if the court has made an SPF civil penalty order in relation to that conduct.

Subdivision D—Infringement notices

58FN Purpose and effect of this Subdivision

(1) The purpose of this Subdivision is to provide for the issue of an infringement notice to a person for an alleged contravention of:

(a) a civil penalty provision of an SPF principle in Subdivision B or E of Division 2 of this Part; or

(b) a civil penalty provision of an SPF code;

as an alternative to proceedings for an SPF civil penalty order.

(2) This Subdivision does not:

(a) require an SPF infringement notice to be issued for an alleged contravention of such a civil penalty provision; or

(b) affect a person's liability to proceedings for an SPF civil penalty order in relation to an alleged contravention of a civil penalty provision if:

(i) an SPF infringement notice is not issued to the person for the contravention; or

(ii) an SPF infringement notice issued to the person for the contravention is withdrawn under section 58FU; or

(c) prevent a court from imposing a higher penalty than the penalty specified in the SPF infringement notice if the person does not comply with the notice.

58FO Issuing an SPF infringement notice

Notices for contraventions of certain SPF principles

(1) If an inspector of the SPF general regulator reasonably believes that a person has contravened a civil penalty provision of an SPF principle in Subdivision B or E of Division 2 of this Part, the inspector may issue a notice (an ***SPF infringement notice***) to the person.

Notices for contraventions of SPF codes

(2) If an inspector of the SPF sector regulator for a regulated sector reasonably believes that a person has contravened a civil penalty provision of the SPF code for the sector, the inspector may issue a notice (an ***SPF infringement notice***) to the person.

Only one notice for each contravention

(3) Inspectors for an SPF regulator must not issue more than one SPF infringement notice to the person for the same alleged contravention of a civil penalty provision.

When notices do not have any effect

(4) An SPF infringement notice does not have any effect if the notice:
- (a) is issued more than 12 months after the day that the relevant contravention is alleged to have occurred; or
- (b) relates to more than one alleged contravention of a civil penalty provision by the person.

58FP Matters to be included in an SPF infringement notice

An SPF infringement notice must:
- (a) be identified by a unique number; and
- (b) state the day on which it is issued; and
- (c) state the name of the person to whom it is issued; and
- (d) state the name of the inspector who issued the notice, that the inspector is an inspector of the applicable SPF regulator, and how that SPF regulator may be contacted; and
- (e) give details of the alleged contravention, including:
  - (i) the day of the alleged contravention; and
  - (ii) the civil penalty provision that was allegedly contravened; and
- (f) state the maximum pecuniary penalty that a court could order the person to pay if the court were to make an SPF civil penalty order for the alleged contravention; and
- (g) specify the penalty that is payable in relation to the alleged contravention; and

(h) state that the penalty is payable within the infringement notice compliance period for the notice; and

(i) state that the penalty is payable to the SPF regulator on behalf of the Commonwealth; and

(j) explain how payment of the penalty is to be made; and

(k) explain the effect of sections 58FR to 58FU.

58FQ Amount of penalty

The penalty to be specified in an SPF infringement notice that is to be issued to a person must be equal to the following amount:

(a) if the person is a body corporate—60 penalty units;

(b) otherwise—12 penalty units.

58FR Effect of compliance with an SPF infringement notice

(1) This section applies if:

(a) an SPF infringement notice for an alleged contravention of a civil penalty provision is issued to a person; and

(b) the person pays the penalty specified in the notice within the infringement notice compliance period and in accordance with the notice; and

(c) the notice is not withdrawn under section 58FU.

(2) The person is not, merely because of the payment, regarded as having contravened the civil penalty provision.

(3) No proceedings (whether criminal or civil) may be started or continued against the person, by or on behalf of the Commonwealth, in relation to the alleged contravention of the civil penalty provision.

58FS Effect of failure to comply with an SPF infringement notice

If:

(a) an SPF infringement notice for an alleged contravention of a civil penalty provision is issued to a person; and

(b) the person fails to pay the penalty specified in the notice within the infringement notice compliance period and in accordance with the notice; and

(c) the notice is not withdrawn under section 58FU;

the person is liable to proceedings for an SPF civil penalty order in relation to the alleged contravention of the civil penalty provision.

58FT Infringement notice compliance period for infringement notice

(1) Subject to this section, the ***infringement notice compliance period***, for an SPF infringement notice issued to a person, is the period of 28 days beginning on the day after the day that the notice is so issued by an inspector of an SPF regulator.

(2) The SPF regulator may, by giving written notice to the person, extend that infringement notice compliance period if the SPF regulator is satisfied that it is appropriate to do so.

(3) Only one extension may be given and the extension must not be for longer than 28 days.

(4) A failure to give the person written notice of the extension does not affect the validity of the extension.

(5) If an infringement notice compliance period for an SPF infringement notice is extended under this section, a reference in this Subdivision to the infringement notice compliance period is taken to be a reference to that period as so extended.

58FU Withdrawal of an infringement notice

Representations to the SPF regulator

(1) A person to whom an SPF infringement notice has been issued:

(a) by an inspector of an SPF regulator; and

(b) for an alleged contravention of a civil penalty provision;

may make written representations to the SPF regulator seeking the withdrawal of the notice.

(2) Evidence or information that:

(a) the person; or

(b) a representative of the person;

gives to the SPF regulator in the course of making representations under subsection (1) is not admissible in evidence against the

person or representative in any proceedings (other than proceedings for an offence based on the evidence or information given being false or misleading).

Withdrawal by the SPF regulator

(3) If an inspector of an SPF regulator issues an SPF infringement notice to a person, the SPF regulator may, by giving written notice (a ***withdrawal notice***) to the person, withdraw the SPF infringement notice if the SPF regulator is satisfied that it is appropriate to do so.

(4) Subsection (3) applies whether or not the person has made representations seeking the withdrawal.

Content of withdrawal notices

(5) The withdrawal notice must state:
  (a) the name and address of the person; and
  (b) the day on which the SPF infringement notice was issued to the person; and
  (c) that the SPF infringement notice is withdrawn; and
  (d) that proceedings for an SPF civil penalty order may be started or continued against the person in relation to the alleged contravention of the civil penalty provision.

Time limit for giving withdrawal notices

(6) To be effective, the withdrawal notice must be given to the person within the infringement notice compliance period for the SPF infringement notice.

Refunds

(7) If an SPF regulator withdraws an SPF infringement notice given to a person after the person has paid the penalty specified in the SPF infringement notice, the SPF regulator must refund to the person an amount equal to the amount paid.

Subdivision E—Enforceable undertakings

58FV Enforceable undertakings

Accepting an undertaking

(1) The SPF general regulator may accept a written undertaking given by a person for the purposes of this section in connection with compliance with a provision of the SPF principles.

(2) The SPF sector regulator for a regulated sector may accept a written undertaking given by a person for the purposes of this section in connection with compliance with a provision of the SPF code for the sector.

Withdrawing or varying the undertaking

(3) The person who gave the undertaking may withdraw or vary it at any time, but only with the consent of the SPF regulator who accepted it.

Orders for enforcing the undertaking

(4) If an SPF regulator considers that the person who gave the SPF regulator an undertaking has breached any of its terms, the SPF regulator may apply to the Court for an order under subsection (5).

(5) If the Court is satisfied that the person has breached a term of the undertaking, the Court may make all or any of the following orders:

(a) an order directing the person to comply with that term of the undertaking;

(b) an order directing the person to pay to the Commonwealth an amount up to the amount of any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach;

(c) any order that the Court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach;

(d) any other order that the Court considers appropriate.

Definitions

(6) In this section:

Court, in relation to a matter, means any court having jurisdiction in the matter.

Subdivision F—Injunctions

58FW Granting injunctions

(1) The Court may, on application, grant an injunction in such terms as the Court considers appropriate if the Court is satisfied that a person has engaged, or is proposing to engage, in conduct that constitutes or would constitute:

(a) a contravention of:

(i) a civil penalty provision of an SPF principle; or

(ii) a civil penalty provision of an SPF code; or

(b) attempting to contravene such a provision; or

(c) aiding, abetting, counselling or procuring a person to contravene such a provision; or

(d) inducing, or attempting to induce, whether by threats, promises or otherwise, a person to contravene such a provision; or

(e) being in any way, directly or indirectly, knowingly concerned in, or party to, the contravention by a person of such a provision; or

(f) conspiring with others to contravene such a provision.

(2) In this Subdivision:

Court, in relation to a matter, means any court having jurisdiction in the matter.

58FX Particular kinds of injunctions

(1) The Court may grant an injunction under section 58FW restraining a person from engaging in conduct:

(a) whether or not it appears to the Court that the person intends to engage again, or to continue to engage, in conduct of that kind; and

(b) whether or not the person has previously engaged in conduct of that kind; and

(c) whether or not there is an imminent danger of substantial damage to any person if the first-mentioned person engages in conduct of that kind.

(2) The Court may grant an injunction under section 58FW requiring a person to do an act or thing:

(a) whether or not it appears to the Court that the person intends to refuse or fail again, or to continue to refuse or fail, to do that act or thing; and

(b) whether or not the person has previously refused or failed to do that act or thing; and

(c) whether or not there is an imminent danger of substantial damage to any person if the first-mentioned person refuses or fails to do that act or thing.

(3) The Court may grant an injunction under section 58FW by consent of all the parties to the proceedings whether or not the Court is satisfied that a person has engaged, or is proposing to engage, in conduct of a kind mentioned in that section.

58FY Interim injunctions

The Court may, if in the opinion of the Court it is desirable to do so, grant an interim injunction pending determination of an application for an injunction under section 58FW.

58FZ Rescinding or varying injunctions

The Court may rescind or vary an injunction granted under this Subdivision.

58FZA Applying for injunctions

(1) An application for an injunction under this Subdivision may be made by an SPF regulator or any other person.

(2) If an SPF regulator applies for such an injunction, the Court must not require the applicant or any other person, as a condition of

granting an interim injunction, to give any undertakings as to damages.

(3) If:

(a) a person other than an SPF regulator:

(i) applies for such an injunction; and

(ii) apart from this subsection, would be required by the Court to give an undertaking as to damages or costs; and

(b) an SPF regulator gives the undertaking;

the Court must accept the undertaking by the SPF regulator and must not require a further undertaking from any other person.

58FZB Other powers of the Court unaffected

The powers conferred on the Court by this Subdivision are in addition to, and not instead of, any other powers of the Court, whether conferred by this Act or otherwise.

Subdivision G—Actions for damages

58FZC Actions for damages—general rule

(1) A person (the ***victim***) who suffers loss or damage by conduct of another person that was done in contravention of:

(a) a civil penalty provision of an SPF principle; or

(b) a civil penalty provision of an SPF code;

may recover the amount of the loss or damage by action against that other person.

(2) An SPF regulator may make a claim under subsection (1) on behalf of the victim if the SPF regulator has the victim's written consent to do so.

(3) A claim under subsection (1) may be made at any time within 6 years after the day the cause of action that relates to the conduct accrued.

(4) However, this section applies subject to sections 58FZD to 58FZK (about proportionate liability for concurrent wrongdoers).

Note: See subsection 58FZF(1) in particular.

58FZD Meaning of *concurrent wrongdoers*

(1) In this Subdivision, a ***concurrent wrongdoer***, in relation to a claim under subsection 58FZC(1), is a person who is one of 2 or more persons:

(a) who each contravened a civil penalty provision of an SPF principle or a civil penalty provision of an SPF code (whether or not the same civil penalty provision); and

(b) whose contraventions caused, independently of each other or jointly, the loss or damage that is the subject of the claim.

(2) For the purposes of this Subdivision, a person can be a concurrent wrongdoer if the person is insolvent, is being wound up or has ceased to exist or died.

58FZE Certain concurrent wrongdoers not to have benefit of apportionment

(1) Nothing in this Subdivision operates to exclude the liability of a concurrent wrongdoer (an ***excluded concurrent wrongdoer***) in proceedings involving a claim under subsection 58FZC(1) to recover an amount of loss or damage if:

(a) the concurrent wrongdoer intended to cause the loss or damage; or

(b) the concurrent wrongdoer fraudulently caused the loss or damage.

(2) The liability of an excluded concurrent wrongdoer is to be determined in accordance with the legal rules (if any) that (apart from sections 58FZD to 58FZK) are relevant.

(3) The liability of any other concurrent wrongdoer who is not an excluded concurrent wrongdoer is to be determined in accordance with the other provisions of this Subdivision.

58FZF Proportionate liability for claims involving concurrent wrongdoers

(1) In any proceedings involving a claim under subsection 58FZC(1) to recover an amount of loss or damage:

(a) the liability of a defendant who is a concurrent wrongdoer in relation to the claim is limited to an amount reflecting that proportion of the loss or damage that the court considers just having regard to the extent of the defendant's responsibility for the loss or damage; and

(b) the court may give judgment against the defendant for not more than that amount.

(2) If the proceedings also involve another claim that is not a claim under subsection 58FZC(1), liability for the other claim is to be determined in accordance with the legal rules, if any, that (apart from this Subdivision) are relevant.

(3) In apportioning responsibility between defendants in the proceedings:

(a) the court is to exclude that proportion of the loss or damage in relation to which the victim is contributorily negligent under any relevant law; and

(b) the court may have regard to the comparative responsibility of any concurrent wrongdoer who is not a party to the proceedings.

(4) This section applies in proceedings whether or not all concurrent wrongdoers are parties to the proceedings.

(5) A reference in this Subdivision to a defendant in proceedings includes any person joined as a defendant or other party in the proceedings (except as a plaintiff) whether joined under this Subdivision, under rules of court or otherwise.

58FZG Defendant to notify plaintiff of concurrent wrongdoer of whom defendant aware

(1) If:

(a) a defendant in proceedings involving a claim under subsection 58FZC(1) has reasonable grounds to believe that a particular person (the ***other person***) may be a concurrent wrongdoer in relation to the claim; and

(b) the defendant fails to give the plaintiff, as soon as practicable, written notice of the information that the defendant has about:

(i) the identity of the other person; and

(ii) the circumstances that may make the other person a concurrent wrongdoer in relation to the claim; and

(c) the plaintiff unnecessarily incurs costs in the proceedings because the plaintiff was not aware that the other person may be a concurrent wrongdoer in relation to the claim;

the court hearing the proceedings may order that the defendant pay all or any of those costs of the plaintiff.

Note: The plaintiff is the victim or an SPF regulator (see subsections 58FZC(1) and (2)).

(2) The court may order that the costs to be paid by the defendant be assessed on an indemnity basis or otherwise.

58FZH Contribution not recoverable from defendant

A defendant against whom judgment is given under this Subdivision as a concurrent wrongdoer in relation to a claim under subsection 58FZC(1):

(a) cannot be required to contribute to any damages or contribution recovered from another concurrent wrongdoer in respect of the claim (whether or not the damages or contribution are recovered in the same proceedings in which judgment is given against the defendant); and

(b) cannot be required to indemnify any such wrongdoer.

58FZI Subsequent actions

(1) For a claim under subsection 58FZC(1), nothing in this Subdivision or any other law prevents a plaintiff (or a victim) who has previously recovered judgment against a concurrent wrongdoer for an apportionable part of any loss or damage from bringing another action against any other concurrent wrongdoer for that loss or damage.

(2) However, in any proceedings in respect of any such action, an amount of damages cannot be recovered by or for the victim that, having regard to any damages previously recovered by or for the victim in respect of the loss or damage, would result in the victim receiving compensation for loss or damage that is greater than the loss or damage actually sustained by the victim.

58FZJ Joining non-party concurrent wrongdoer in the action

(1) The court may give leave for any one or more persons to be joined as defendants in proceedings involving a claim under subsection 58FZC(1).

(2) The court is not to give leave for the joinder of any person who was a party to any previously concluded proceedings in respect of the claim.

58FZK Application of this Subdivision

Nothing in this Subdivision:

(a) prevents a person being held vicariously liable for a proportion of a claim under subsection 58FZC(1) for which another person is liable; or

(b) prevents a person from being held severally liable with another person for that proportion of a claim under subsection 58FZC(1) for which the other person is liable; or

(c) affects the operation of any other provision of this Act or of any other Act to the extent that the provision imposes several liability on any person in respect of what would otherwise be a claim under subsection 58FZC(1).

Subdivision H—Public warning notices

58FZL Public warning notices

Suspected contraventions of a provision of the SPF principles

(1) The SPF general regulator may issue to the public a written notice containing a warning about the conduct of a person if the SPF general regulator:

(a) reasonably suspects that the person's conduct may constitute a contravention of a specified provision of the SPF principles; and

(b) is satisfied that one or more persons has suffered, or is likely to suffer, detriment as a result of the conduct; and

(c) is satisfied that it is in the public interest to issue the notice.

Suspected contraventions of a provision of an SPF code

(2) The SPF sector regulator for a regulated sector may issue to the public a written notice containing a warning about the conduct of a person if the SPF sector regulator:

(a) reasonably suspects that the person's conduct may constitute a contravention of a specified provision of the SPF code for the sector; and

(b) is satisfied that one or more persons has suffered, or is likely to suffer, detriment as a result of the conduct; and

(c) is satisfied that it is in the public interest to issue the notice.

Related matters

(3) An SPF regulator that issues a notice under subsection (1) or (2) must publish the notice on the SPF regulator's website.

(4) A notice under subsection (1) or (2) is not a legislative instrument.

Subdivision I—Remedial directions

58FZM Remedial directions

Giving directions—to comply with an SPF principle

(1) If the SPF general regulator reasonably suspects that a regulated entity:

(a) is failing to comply with an SPF principle; or

(b) will fail to comply with an SPF principle;

the SPF general regulator may, by written notice given to the entity, direct the entity to take specified action to comply with that SPF principle.

Giving directions—to comply with an SPF code

(2) If the SPF sector regulator for a regulated sector reasonably suspects that a regulated entity for the sector:

(a) is failing to comply with a provision of the SPF code for the sector; or

(b) will fail to comply with such a provision;

the SPF sector regulator may, by written notice given to the entity, direct the entity to take specified action to comply with that provision of the SPF code.

Complying with a direction

(3) A regulated entity given a direction under subsection (1) or (2) must comply with the direction.

(a) within the time specified in the direction, which must be a reasonable time; or

(b) if the direction does not specify a reasonable time—within a reasonable time.

(4) Subsection (3) is a civil penalty provision.

Note: To work out how sections 58FJ to 58FL (about civil penalties) apply to subsection (3), see the definitions of ***civil penalty provision of an SPF principle***, and ***civil penalty provision of an SPF code*** in subsection 4(1).

Extending the time for complying with a direction

(5) The SPF regulator who gives a direction under subsection (1) or (2) to an entity may extend the time for complying with the direction by written notice given to the entity.

Before giving a direction

(6) Before an SPF regulator gives an entity a direction under subsection (1) or (2), the SPF regulator must give the entity an opportunity to make submissions to the SPF regulator on the matter.

Varying and revoking directions

(7) An SPF regulator may vary or revoke a direction given by the SPF regulator under subsection (1) or (2) in like manner and subject to like conditions.

Publishing directions

(8) As soon as practicable after an SPF regulator gives, varies or revokes a direction under subsection (1) or (2), the SPF regulator must publish a notice of its action on its website.

Subdivision J—Adverse publicity orders

58FZN Adverse publicity orders

Making adverse publicity orders

(1) The Court may, on application, make an adverse publicity order against a person who has been ordered to pay a pecuniary penalty under an SPF civil penalty order.

(2) Such an order may require the person to:

(a) disclose, in the way and to the persons specified in the order, specified information that the person has possession of or access to; and

(b) publish, at the person's expense and in in a specified way, an advertisement in the terms specified in, or determined in accordance with, the order.

Applying for adverse publicity orders

(3) An application for such an order may be made by:

(a) if the SPF civil penalty order was for a contravention of a civil penalty provision of an SPF principle—the SPF general regulator; or

(b) if the SPF civil penalty order was for a contravention of a civil penalty provision of an SPF code for a regulated sector—the SPF sector regulator for the sector.

Definitions

(4) In this section:

Court, in relation to a matter, means any court having jurisdiction in the matter.

Subdivision K—Non-punitive orders

58FZO Non-punitive orders

Making non-punitive orders

(1) The Court may, on application, make one or more of the following orders in relation to a person who has engaged in conduct contravening an SPF principle or a provision of an SPF code:

(a) a community service order;

(b) a probation order for a period of no longer than 3 years;

(c) an order requiring the person to disclose, in the way and to the persons specified in the order, specified information that the person has possession of or access to;

(d) an order requiring the person to publish, at the person's expense and in a specified way, an advertisement in the terms specified in, or determined in accordance with, the order.

Applying for non-punitive orders

(2) An application for such an order may be made by:

(a) for conduct contravening an SPF principle—the SPF general regulator; or

(b) for conduct contravening a provision of the SPF code for a regulated sector—the SPF sector regulator for the sector.

Definitions

(3) For the purposes of this section, a ***probation order*** is an order made to ensure that a person does not engage in:

(a) the conduct that resulted in the order; or

(b) similar conduct or related conduct;

during the period of the order.

(4) Without limiting subsection (3), a ***probation order*** includes:

(a) an order directing a person to establish a compliance program, or an education and training program, that:

(i) is for employees or other persons involved in the person's business; and

(ii) is designed to ensure awareness of responsibilities and obligations relating to conduct covered by paragraph (3)(a) or (b); and

(b) an order directing a person to revise the internal operations of the person's business that lead to conduct covered by paragraph (3)(a) or (b).

(5) In this section:

community service order means an order directing a person to perform a service that:

(a) is specified in the order; and

(b) is or relates to the conduct that resulted in the order;

for the benefit of the community or a section of the community.

contravening: conduct ***contravening*** an SPF principle or a provision of an SPF code includes conduct that constitutes being involved in such a contravention.

Note: For the meaning of ***involved***, see subsection 4(1).

Court, in relation to a matter, means any court having jurisdiction in the matter.

Subdivision L—Orders (other than awards of damages) to redress loss or damage

58FZP Orders (other than awards of damages) to redress loss or damage—making such orders

Making orders

(1) The Court may, on application, make such orders (other than an award of damages) as the Court thinks appropriate against a person who:

(a) engaged in conduct (the ***contravening conduct***) contravening a civil penalty provision of an SPF principle or a civil penalty provision of an SPF code; or

(b) is involved in the contravening conduct;

if the contravening conduct caused, or is likely to cause, a class of persons (the ***victims***) to suffer loss or damage.

Note 1: The orders that the court may make include all or any of the orders set out in section 58FZQ.

Note 2: For the meaning of ***involved***, see subsection 4(1).

(2) Subsection (1) applies whether or not the victims include persons (***non-parties***) who are not, or have not been, parties to a proceeding (an ***enforcement proceeding***) instituted under another provision in or referred to in this Division in relation to the contravening conduct.

(3) The Court must not make such an order unless the Court considers that the order will:

(a) redress, in whole or in part, the loss or damage suffered by the victims in relation to the contravening conduct; or

(b) prevent or reduce the loss or damage suffered, or likely to be suffered, by the victims in relation to the contravening conduct.

Applying for orders

(4) An application for such an order may be made:

(a) by the following:

(i) if the contravening conduct contravened a civil penalty provision of an SPF principle—the SPF general regulator;

(ii) if the contravening conduct contravened a civil penalty provision of an SPF code for a regulated sector—the SPF sector regulator for the sector; and

(b) even if an enforcement proceeding in relation to the contravening conduct has not been instituted; and

(c) at any time within 6 years after the day on which the cause of action that relates to the contravening conduct accrues.

Working out whether to make an order

(5) In working out whether to make such an order against a person referred to in paragraph (1)(a) or (b), the Court may have regard to the conduct of:

(a) the person; and

(b) the victims;

in relation to the contravening conduct since the contravention occurred.

(6) However, the Court need not make a finding about either of the following matters:

(a) which persons are victims in relation to the contravening conduct;

(b) the nature of the loss or damage suffered, or likely to be suffered, by such persons.

When a non-party victim is bound by an order etc.

(7) If all of the following happen:

(a) such an order is made against a person;

(b) the loss or damage suffered, or likely to be suffered, by a non-party victim in relation to the contravening conduct has been redressed, prevented or reduced in accordance with the order;

(c) the non-party victim has accepted the redress, prevention or reduction;

then:

(d) the non-party victim is bound by the order; and

(e) any other order made under subsection (1) relating to that loss or damage has no effect in relation to the non-party victim; and

(f) despite any other provision of this Act or any other law of the Commonwealth, or a State or Territory, no claim, action or demand may be made or taken against the person by the non-party victim in relation to that loss or damage.

Definitions

(8) In this section:

Court, in relation to a matter, means any court having jurisdiction in the matter.

58FZQ Orders (other than awards of damages) to redress loss or damage—kinds of such orders

(1) Without limiting subsection 58FZP(1), the orders that the Court may make under that subsection against a person (the ***respondent***) include all or any of the following:

(a) an order declaring the whole or any part of a contract made between the respondent and a victim referred to in that subsection, or a collateral arrangement relating to such a contract:

(i) to be void; and

(ii) if the Court thinks fit—to have been void ab initio or void at all times on and after such date as is specified in the order (which may be a date that is before the date on which the order is made);

(b) an order:

(i) varying such a contract or arrangement in such manner as is specified in the order; and

(ii) if the Court thinks fit—declaring the contract or arrangement to have had effect as so varied on and after such date as is specified in the order (which may be a date that is before the date on which the order is made);

(c) an order refusing to enforce any or all of the provisions of such a contract or arrangement;

(d) an order directing the respondent to refund money or return property to a victim referred to in that subsection;

(e) an order directing the respondent, at the respondent's own expense, to repair, or provide parts for, goods that have been supplied under the contract or arrangement to a victim referred to in that subsection;

(f) an order directing the respondent, at the respondent's own expense, to supply specified services to a victim referred to in that subsection;

(g) an order, in relation to an instrument creating or transferring an interest in land, directing the respondent to execute an instrument that:

(i) varies, or has the effect of varying, the first-mentioned instrument; or

(ii) terminates or otherwise affects, or has the effect of terminating or otherwise affecting, the operation or effect of the first-mentioned instrument.

(2) In this section:

interest, in land, means:

(a) a legal or equitable estate or interest in the land; or

(b) a right of occupancy of the land, or of a building or part of a building erected on the land, arising by virtue of the holding of shares, or by virtue of a contract to purchase shares, in an incorporated company that owns the land or building; or

(c) a right, power or privilege over, or in connection with, the land.

Division 7—Other provisions

58GA Treatment of partnerships

(1) The SPF provisions apply to a partnership as if it were a person, but with the changes set out in this section.

(2) An obligation that would otherwise be imposed on the partnership by an SPF provision is imposed on each partner instead, but may be discharged by any of the partners.

(3) If an SPF provision would otherwise permit something to be done by the partnership, the thing may be done by one or more of the partners on behalf of the partnership.

(4) For the purposes of the SPF provisions, a change in the composition of a partnership does not affect the continuity of the partnership.

58GB Treatment of unincorporated associations

(1) The SPF provisions apply to an unincorporated association as if it were a person, but with the changes set out in this section.

(2) An obligation that would otherwise be imposed on the association by an SPF provision is imposed on each member of the

association's committee of management instead, but may be discharged by any of the members.

(3) If an SPF provision would otherwise permit something to be done by the unincorporated association, the thing may be done by one or more of the members of the association's committee of management on behalf of the association.

58GC Treatment of trusts

(1) The SPF provisions apply to a trust as if it were a person, but with the changes set out in this section.

Trusts with a single trustee

(2) If the trust has a single trustee:

(a) an obligation that would otherwise be imposed on the trust by an SPF provision is imposed on the trustee instead; and

(b) if an SPF provision would otherwise permit something to be done by the trust, the thing may be done by the trustee.

Trusts with multiple trustees

(3) If the trust has 2 or more trustees:

(a) an obligation that would otherwise be imposed on the trust by an SPF provision is imposed on each trustee instead, but may be discharged by any of the trustees; and

(b) if an SPF provision would otherwise permit something to be done by the trust, the thing may be done by any of the trustees.

58GD Compensation for acquisition of property

(1) This section applies if the operation of the SPF provisions would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from a person otherwise than on just terms (within the meaning of that paragraph).

(2) The person who acquires the property is liable to pay a reasonable amount of compensation to the first-mentioned person.

(3) If the 2 persons do not agree on the amount of the compensation, the person to whom compensation is payable may institute proceedings in:

(a) the Federal Court; or

(b) the Supreme Court of a State or Territory;

for the recovery from the other person of such reasonable amount of compensation as the Court determines.

58GE Rules for the purposes of this Part

(1) The Minister may, by legislative instrument, make rules (the ***SPF rules***) prescribing matters:

(a) required or permitted by this Part to be prescribed by the SPF rules; or

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Part.

Note: A matter may be prescribed by the SPF rules by class (see subsection 13(3) of the *Legislation Act 2003*). For example, a specific regulated entity or a class of regulated entities may be able to be prescribed in some cases.

(2) The Minister may, in writing, delegate the Minister's power to make SPF rules to another Minister or to an SPF regulator.

(3) To avoid doubt, the SPF rules may not do the following:

(a) create an offence or civil penalty;

(b) provide powers of:

(i) arrest or detention; or

(ii) entry, search or seizure;

(c) impose a tax;

(d) set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Act;

(e) directly amend the text of this Act.

58GF Report of the operation of the SPF provisions

(1) The Minister must cause a review to be conducted of the operation of the SPF provisions.

(2) The review must be conducted as soon as practicable after the end of the 3-year period starting on the day the first SPF code is made under section 58CB.

(3) The persons who conduct the review must give the Minister a written report of the review.

(4) The Minister must cause a copy of the report of the review to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

Part 2—Other amendments

Australian Communications and Media Authority Act 2005

2 At the end of paragraph 8(1)(j)

Add:

; or (vii) the SPF provisions (within the meaning of the *Competition and Consumer Act 2010*) if the ACMA is designated as a SPF sector regulator under subsection 58ED(1) of that Act;

3 After section 59DA

Insert:

59DB Disclosure of information that relates to the Scams Prevention Framework

An ACMA official authorised by the Chair, in writing, for the purposes of this section may disclose authorised disclosure information if the disclosure:

(a) is to:

(i) an SPF regulator (within the meaning of the *Competition and Consumer Act 2010*); or

(ii) the operator of an SPF EDR scheme (within the meaning of that Act); and

(b) is for the purposes of the operation (including enforcement) of the SPF provisions (within the meaning of that Act).

Australian Securities and Investments Commission Act 2001

4 At the end of subsection 12A(1)

Add:

; (o) the SPF provisions (within the meaning of the *Competition and Consumer Act 2010*).

Competition and Consumer Act 2010

5 Subsection 4(1)

Insert:

ACMA means the Australian Communications and Media Authority.

actionable scam intelligence has the meaning given by section 58AI.

associate, of an SPF consumer, means an associate (within the meaning of section 318 of the *Income Tax Assessment Act 1936*) of the SPF consumer who is:

(a) a natural person who is in Australia or is ordinarily resident in Australia; or

(b) a person who carries on a business having a principal place of business in Australia;

civil penalty provision of an SPF code means:

(a) a provision of an SPF code (see Division 3 of Part IVF) that is a civil penalty provision (within the meaning of the Regulatory Powers Act); or

(b) subsection 58FZM(3) in relation to compliance with a direction given under subsection 58FZM(2).

civil penalty provision of an SPF principle means:

(a) a provision of Division 2 of Part IVF (about the Scams Prevention Framework) that is a civil penalty provision (within the meaning of the Regulatory Powers Act); or

(b) subsection 58FZM(3) in relation to compliance with a direction given under subsection 58FZM(1).

de-identified: information is ***de-identified*** if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

infringement notice compliance period for an SPF infringement notice: see section 58FT.

inspector, of an SPF regulator, has the meaning given by section 58FB.

involved, in a contravention of a civil penalty provision of an SPF principle or of a civil penalty provision of an SPF code, means:

(a) aiding, abetting, counselling or procuring a contravention of the provision; or

(b) inducing, whether by threats or promises or otherwise, such a contravention; or

(c) being in any way, directly or indirectly, knowingly concerned in, or party to, such a contravention; or

(d) conspiring with others to effect such a contravention.

reasonable steps, for the purposes of Division 2 of Part IVF (about overarching principles of the Scams Prevention Framework), has a meaning affected by section 58BB.

regulated entity has the meaning given by section 58AD.

regulated sector has the meaning given by subsection 58AC(1).

regulated service has the meaning given by section 58AD.

scam has the meaning given by section 58AG.

senior officer, of a regulated entity, means:

(a) an officer (within the meaning of the *Corporations Act 2001*) of the entity; or

(b) a senior manager (within the meaning of that Act) of the entity.

SPF civil penalty order means a civil penalty order under Part 4 of Regulatory Powers Act (as that Part applies because of section 58FJ of this Act).

SPF code has the meaning given by section 58CB.

SPF consumer has the meaning given by section 58AH.

SPF EDR scheme, for a regulated sector, means an external dispute resolution scheme authorised under subsection 58DB(1) for the sector.

SPF general regulator has the meaning given by section 58EB.

SPF governance policies, procedures, metrics and targets, for a regulated entity for a regulated sector, means the entity's:

(a) policies and procedures required under paragraph 58BD(1)(a) for the sector; and

(b) performance metrics and targets required under paragraph 58BD(1)(c) for those policies and procedures.

SPF infringement notice means an infringement notice issued under subsection 58FO(1) or (2).

SPF personal information means:

(a) personal information; or

(b) information relating to a person that may be used (whether alone or in conjunction with other information) to access:

(i) a service or an account; or

(ii) funds, credit or other financial benefits.

SPF principles means the provisions in Subdivisions B to G of Division 2 of Part IVF (about the Scams Prevention Framework).

SPF provisions has the meaning given by section 58AJ.

SPF regulator means:

(a) the SPF general regulator; or

(b) the SPF sector regulator for a regulated sector.

SPF rules means rules made under section 58GE.

SPF sector regulator has the meaning given by section 58ED.

6 Section 52A (definition of *ACMA*)

Repeal the definition.

7 Section 151AB (definition of *ACMA*)

Repeal the definition.

8 Section 152AC (definition of *ACMA*)

Repeal the definition.

9 At the end of paragraph 155(2)(a)

Add:

(v) an SPF code; or

10 After subparagraph 155(2)(b)(ib)

Insert:

(ic) a designated scams prevention framework matter (as defined by subsection (9AC) of this section); or

11 After subsection 155(9AB)

Insert:

(9AC) A reference in this section to a ***designated scams prevention framework matter*** is a reference to the performance of a function, or the exercise of a power, conferred on the Commission (as an SPF regulator) by or under:

(a) Part IVF; or

(b) a legislative instrument (such as an SPF code) made under that Part; or

(c) the Regulatory Powers Act to the extent that it applies in relation to a provision of that Part.

12 Paragraph 155AAA(12)(b)

Omit "Australian Communications and Media Authority", substitute "ACMA".

Corporations Act 2001

13 At the end of subsection 1051(2)

Add:

Note: A law, instrument or condition referred to in paragraph (a) that requires entities to be members of the scheme need not be a law, instrument or condition regulating providers of financial products or services. The constitutional basis for that law, instrument or condition would need to support the scheme's application to such entities.

14 At the end of section 1052A

Add:

Note: This power to issue regulatory requirements extends to any application of the AFCA scheme in relation to members of the scheme that are not providers of financial products or services.

15 Subsection 1052B(1) (note)

Omit "Note", substitute "Note 1".

16 At the end of subsection 1052B(1)

Add:

Note 2: This power to give directions extends to any application of the AFCA scheme in relation to members of the scheme that are not providers of financial products or services.

17 At the end of subsections 1052BA(1) and 1052C(1)

Add:

Note: This power to give directions extends to any application of the AFCA scheme in relation to members of the scheme that are not providers of financial products or services.

18 Subsection 1052D(1) (note)

Omit "Note", substitute "Note 1".

19 At the end of subsection 1052D(1)

Add:

Note 2: This right to make requests extends to any application of the AFCA scheme in relation to members of the scheme that are not providers of financial products or services.

20 At the end of subsection 1052E(1)

Add:

Note: This subsection extends to any application of the AFCA scheme in relation to members of the scheme that are not providers of financial products or services.