EXPLANATORY STATEMENT

Issued by authority of the Assistant Treasurer and Minister for Financial Services

Competition and Consumer Act 2010

Competition and Consumer (Scams Prevention Framework—SPF Codes) Instrument 2026

The *Scams Prevention Framework Act 2025* introduced Part IVF into the *Competition and Consumer Act* (the Act). Part IVF establishes the Scams Prevention Framework (SPF) for preventing and responding to scams that impact the Australian economy.

The SPF has the following features:

- overarching principles, called SPF principles, that apply to regulated entities in all regulated sectors;
- a power to make sector-specific codes, called SPF codes, that apply to regulated entities in the particular regulated sector;
- a power to make rules, called SPF rules, to support the operation of the SPF;
- a multi-regulator framework; regulatory and enforcement mechanisms; and dispute resolution and actions for damages mechanisms.

Section 58CB of the Act provides that the Minister may, by legislative instrument, make an SPF code for a regulated sector, which may follow the designation of that regulated sector. The banking, telecommunications and digital platforms sectors are designated as regulated sectors by the *Competition and Consumer (Scams Prevention Framework-Regulated Sectors) Designation 2026* (the Designation).

Under section 58CC of the Act, an SPF code must be consistent with the SPF principles and deal with only the SPF principles of governance, prevent, detect, disrupt and respond, related or incidental matters, and provisions prescribed by the SPF rules. An SPF code cannot deal with, or make obligations under, the SPF principle of report.

Pursuant to subsection 58CC(3) of the Act, an SPF code may provide that specified provisions are civil penalty provisions (within the meaning of the *Regulatory Powers (Standard Provisions) Act 2014*). A breach of a civil penalty provision in an SPF code may also constitute a breach of a civil penalty provision in an SPF principle – most notably for provisions in the SPF principles requiring a regulated entity to take 'reasonable steps' (noting section 58FM prevents civil penalty double jeopardy).

The purpose of the *Competition and Consumer (Scams Prevention Framework—SPF Codes) Instrument 2026* (the Codes) is to make SPF codes under the SPF for the banking, telecommunications, and digital platforms sectors, each being a regulated sector for the purposes of the SPF. SPF codes establish sector-specific, mandatory and enforceable obligations for regulated entities in these sectors so that incentives are in place in sectors where scammers act to cause harm in the community.

SPF codes aim to promote consistent standards of scams governance, prevention, detection, disruption and response to stop scammers harming consumers but, where appropriate, provide for targeted measures specific to the scam risks, consumer interactions and prevention capabilities in particular sectors.

The SPF codes will work in conjunction with the SPF principles in the Act and the SPF rules to reduce the prevalence and impact of scams. This will help keep Australians safer from scams while safeguarding the benefits of the digital economy.

The Codes establish 4 distinct categories of provisions:

- common provisions that apply across the banking, telecommunications, and digital platforms sectors;
- provisions that apply only to the banking sector;
- provisions that apply only to the telecommunications sector; and
- provisions that apply only to the digital platforms sector.

All the obligations specified in the Codes for SPF principles of prevent, detect and disrupt are relevant SPF code obligations for the purposes of section 58BB of the Act. This means that compliance with these code obligations is the primary factor when considering whether a regulated entity has taken reasonable steps for the purposes of the corresponding SPF principles of prevent, detect and disrupt in Division 2 of Part IVF of the Act.

An entity designated by the Minister under subsection 58ED(1) to be the SPF sector regulator for a regulated sector will be responsible for regulating and enforcing compliance with the SPF code for that sector (subsection 58ED(3)). If no entity is designated, the Australian Competition and Consumer Commission (ACCC) becomes the SPF sector regulator by default. Under section 58EF, the SPF general regulator (being the ACCC) and each SPF sector regulator must have an arrangement for the shared regulation and enforcement of the SPF. Breaches of an SPF code may also enliven pathways for consumer redress through internal dispute resolution, external dispute resolution (EDR), or through the courts.

The Codes form part of a wider package of SPF subordinate instruments, which include the Designation, SPF rules (including exceptions to the sector designations) and authorisation of the Australian Financial Complaints Authority scheme as the SPF EDR scheme for the designated sectors.

Public consultation was undertaken by Treasury on the "Scams Prevention Framework – Draft law package and position paper" from 28 November 2025 to 5 January 2026 which focused on obtaining stakeholder views on the scope of proposed designated sectors and to shape the policy outcomes of SPF codes and rules for those designated sectors. Feedback provided during that process informed the policy positions that the Codes reflect.

The Codes are a legislative instrument for the purposes of the *Legislation Act 2003*.

The Codes commence on the later of 31 March 2027; and the day after registration.

Details of the Codes are set out in Attachment A.

ATTACHMENT A

Details of the *Competition and Consumer (Scams Prevention Framework —SPF Codes) Instrument 2026*

Part 1 – Preliminary

Section 1-1 – Name

This section provides that the name of the instrument is the *Competition and Consumer (Scams Prevention Framework —SPF Codes) Instrument 2026* (the Instrument).

Section 1-2 – Commencement

The Instrument commences on the later of 31 March 2027 and the day after the instrument is registered on the Federal Register of Legislation.

Section 1-3 – Authority

The Instrument is made under the *Competition and Consumer Act 2010* (the Act).

Section 1-4 – Banking sector SPF code

This section provides that, for the purposes of section 58CB of the Act, Parts 2, 3 and 6 of the Instrument set out the SPF code provisions for the banking sector, designated under section 11 of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026* (the Designation).

Section 11 of the Designation designates 'covered banking services' as a regulated sector (the banking sector) for the purposes of the SPF. The banking sector comprises:

- a service provided by an Authorised Deposit-taking Institution (ADI) in the course of carrying on its banking business (within the meanings of the *Banking Act 1959*), and
- to the extent not already covered, the provision of a purchased payment facility (PPF) by an ADI in the course of carrying on its business in Australia.

The SPF rules that are also being consulted on as part of this consultation package include specified exceptions for certain providers of PPFs and will exclude certain indirect SPF consumers.

Section 1-5 – Telecommunications sector SPF code

This section provides that, for the purposes of section 58CB of the Act, Parts 2 (other than sections 2-15 and 2-16), 4 and 6 of the Instrument set out the SPF code provisions for the telecommunications sector, designated under section 13 of the Designation.

Section 13 of the Designation designates 'covered telecommunications services' as a regulated sector (the telecommunications sector) for the purposes of the SPF. The telecommunications sector comprises:

- a voice call service, or

- a message service,

if those services are provided by a carrier and a public carriage service provider and also provided using a listed carriage service.

For the purposes of exposure draft consultation, the substance of Part 4 is contained in a separate Instrument – the *Competition and Consumer Amendment (Scams Prevention Framework–Telecommunications Code) Instrument 2026*.

Section 1-6 – Digital platforms sector SPF code

This section provides that, for the purposes of section 58CB of the Act, Parts 2, 5 and 6 of the Instrument set out the SPF code provisions for the Digital Platforms sector, designated under section 15 of the Designation.

Section 15 of the Designation designates 'covered digital platform services' as a regulated sector (the digital platforms sector) for the purposes of the SPF. The digital platforms sector comprises:

- a designated instant messaging service,
- a designated internet search service (that is, the provision of advertising on an internet search engine), or
- a designated social media service.

The SPF rules that are also being consulted on as part of this consultation package include specified exceptions for digital platforms that do not meet a specified revenue test and services that do not meet a specified test for active Australian users.

Section 1-7 – Definitions

This section defines terms used in the Instrument. In the Instrument:

- ***ABN*** has the same meaning as in the *A New Tax System (Australian Business Number) Act 1999*.
- ***advertiser*** means a person who advertises or seeks to advertise a product or service on a regulated service of a regulated entity.
- ***designated instant messaging service*** has the same meaning as in the Designation.
- ***digital platform account*** means an account held with a regulated digital platform.
- ***direct SPF consumer*** of a regulated service means an SPF consumer of the regulated service to whom the regulated service is provided, or purportedly provided, directly.
- ***disruptive action*** means, for a regulated entity for a regulated sector, action taken where the entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity, and takes steps to disrupt the activity.

- ***internal dispute resolution mechanism*** of a regulated entity for a regulated sector means the accessible and transparent internal dispute resolution (IDR) mechanism the entity is required to have, under subsection 58BZD(1) of the Act, to deal with a person's complaint about an activity that is or may be a scam, or the entity's conduct relating to such activity.

- ***major scam event***: a regulated entity for a regulated sector is affected by a ***major scam event*** if a scam, or a group of related scams, relating to, connected with, or using a regulated service of the entity results in, or would if successful have resulted in, significant or widespread loss to SPF consumers of the entity's regulated service.

- ***reasonable steps*** has its ordinary meaning. It is not the intention of the Instrument to describe, for the purpose of a particular enabling provision in Part IVF of the CCA, what reasonable steps means.

- ***regulated bank*** means a regulated entity for the regulated sector designated under section 11 of the Designation.

- ***regulated digital platform*** means a regulated entity for the regulated sector designated under section 15 of the Designation.

- ***regulated telecommunications provider*** means a regulated entity for the regulated sector designated under section 13 of the Designation.

- ***reporting mechanism*** of a regulated entity for a regulated sector means the accessible mechanism the entity is required to have, under subsection 58BZC(1) of the Act, for a person to report an activity that is or may be a scam.

- ***required policies and procedures***, for a regulated entity for a regulated sector, means the entity's governance policies and procedures required under paragraph 58BD(1)(a) of the Act for the sector.

- ***SPF complaint*** means a complaint by a person of a kind described in paragraph 58BZD(1)(a) or (b) of the Act.

- ***SPF staff member*** means a person who is an employee of the regulated entity, a contractor or subcontractor of the regulated entity, or an employee of a contractor or subcontractor of the regulated entity. However, a person is only an SPF staff member if they carry out work related to the provision of the regulated entity's regulated service.

- ***SPF report*** means a report by a person made to a regulated entity for a regulated sector about an activity of a kind described in subsection 58BZC(1) of the Act.

- ***the Act*** means the *Competition and Consumer Act 2010.*

The section also notes that expressions have the same meaning in this instrument as in the Act as in force from time to time, as per paragraph 13(1)(b) of the *Legislation Act 2003*. There are several definitions in the Act which are important to the application of the obligations in this Instrument. This includes the following terms:

- ***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. Several obligations detailed below are enlivened by an entity having actionable scam intelligence.

- ***Scam***: A scam means a direct or indirect attempt 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 obtaining SPF personal information of the SPF consumer or their associates.

- ***SPF consumer***: An SPF consumer of a regulated service means either:

  – 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.

Part 2—Common SPF code provisions

Part 2 contains common provisions applying to SPF codes for the regulated sectors designated. The common provisions are intended to ensure a consistent baseline of expected conduct by regulated entities across regulated sectors. This is important because scams frequently involve multiple regulated entities across multiple regulated sectors. Consumer harm often arises from a combination of failures by those entities across sectors to prevent scams. Common provisions ensure consistency irrespective of the regulated service through which the scam occurs. While the common provisions set baseline obligations for all regulated entities and recognise the cross-sector nature of many scam typologies, sector-specific provisions are tailored to individual sectors and recognise differences in how scams occur in each sector.

Part 2 contains 5 divisions:

- Division 1, which concerns preliminary matters

- Division 2, which outlines common provisions (provisions applying to the banking, telecommunications and digital platforms sectors) for SPF principle 1: Governance

- Division 3, which outlines common provisions for SPF principle 2: Prevent

- Division 4, which outlines common provisions for SPF principle 3: Detect

- Division 5, which outlines common provisions for SPF principle 4: Disrupt

- Division 6, which outlines common provisions for SPF principle 5: Respond

While this Part contains provisions for each of these principles, the obligations set out below do not describe or detail what reasonable steps is where this is relevant to the

provisions under those principles. The provisions in this Part create new obligations on regulated entities in related sectors on the themes and matters covered by the Subdivisions containing those principles and related or incidental matters. This equally applies to relevant provisions in Part 3, 4, 5 [and 6].

Division 1—Preliminary

Section 2-1 provides that Part 2 of the Instrument sets out that the provisions in that Part apply to a regulated bank and a regulated digital platform, as obligations in relation to the themes or matters covered in the Subdivisions concerning the SPF principles of Governance, Prevent, Detect, Disrupt and Respond, as well as incidental and related matters to those SPF principles.

It also sets out that that Part 2 of the Instrument, except for sections 2-15 (relating to risk assessments for disruptive actions) and 2-16 (reversing disruptive actions if not a scam), sets out obligations that apply to a regulated telecommunications provider.

Division 2—Common SPF code provisions for SPF principle 1: Governance

The SPF principle of Governance in Subdivision B of Division 2 of Part IVF of the Act requires regulated entities to, among other things, document and implement governance policies and procedures about their compliance with the SPF.

Section 2-2: Requirements for governance policies and procedures

Subsection 58BD of the Act requires regulated entities for regulated sectors to:

- document governance policies and procedures about preventing, detecting and disrupting scams, responding to scams, and reports relating to scams, relating to, connected with, or using the entity's regulated services for the sector;
- implement those governance policies and procedures; and
- develop and implement performance metrics and targets that are for measuring the effectiveness of those governance policies and procedures comply with any requirements for those metrics and targets that are prescribed by the SPF rules (the SPF rules consulted on with this Instrument do not prescribe anything for this purpose).

Section 2-2 outlines the factors that regulated entities must consider when developing their required policies and procedures. These include:

- the risk that a scam relating to, connected with, or using a regulated service of the entity will be committed considering:
  - the type and scale of regulated services provided by the entity; and
  - the ability of the regulated entity to implement measures that will stop or limit scams; and
  - scams relating to, connected with, or using the regulated service that have previously been committed; and

- the types of SPF consumers who use or are likely to use a regulated service of the entity and whether these types of consumers are likely to be at a higher risk of being targeted by scams than other members of the public; and
- how the entity's regulated services are provided; and
- the current and emerging threat of scams occurring in both the regulated sector and the wider Australian economy; and
- the effectiveness of the entity's existing policies and procedures (if any) in stopping or limiting scams; and
- any major scam event that the entity was affected by within the last 12 months.

The policies and procedures must also include information about how the entity assessed the risk that a scam relating to, connected with, or using a regulated service of the entity, could be committed, considering the factors outlined above.

These factors ensure the regulated entity assesses and considers the particular scam vulnerabilities applicable to the entity, by reference to the kind and scale of the regulated services provided by the entity, the kind of SPF consumers of those services, and how those services are provided. This reflects the fact that scam risks may be different for each business and their customers.

It is expected that as part of considering scam risks, a regulated entity will have regard to any significant scam events the entity has previously experienced in the time since the policies and procedures were last updated.

These factors should be considered by the regulated entity each time the entity revises its policies and procedures. This could occur on an annual basis, where a regulated entity reviews and revises accordingly to ensure its policies and procedures are kept up to date.

For the purposes of the last dot point above, a regulated entity for a regulated sector is affected by a major scam event if a scam, or a group of related scams, relating to, connected with, or using a regulated service of the entity results in, or would if successful have resulted in, significant or widespread loss to SPF consumers of the entity's regulated service. It will also include a significant rise in scams over a short period of time. For example, systemic scams that target a large number of people for a smaller amount of money (e.g. less than $500) will still be considered a major scam event.

Requiring consideration of major scam events over the previous 12 months reflects that scams are always evolving and those that commit scams seek to find gaps in existing scam protections. This requirement helps ensure that the policies, procedures, metrics and targets are reviewed and updated to reflect new and emerging scam threats, ahead of the annual certification by a senior officer.

This obligation is not intended to limit the matters or factors that a regulated entity may include or have regard to for its governance policies and procedures (either generally or for the purposes of the SPF) required by section 58BD of the Act. A regulated entity may also include other matters or consider other factors to comply with obligations under other legal frameworks. These may include, for example, obligations under the *Privacy Act 1988* or the financial services law under the *Corporations Act 2001*.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-3: Staff training

A regulated entity's required policies and procedures under section 58BD of the Act must include reasonable processes for developing and providing training and guidance to SPF staff members.

The policies and procedures must specify how the training will support the staff members to reasonably:

- identify scams;
- identify SPF consumers who are likely to be at a higher risk of being targeted by scams than other members of the public;
- identify and support SPF consumers who have been affected by a scam, including those that have made an SPF report or an SPF complaint;
- respond in a timely, fair and effective way to SPF reports or SPF complaints;
- identify and support SPF consumers who may require assistance to access the entity's IDR mechanism including people with disability, or from a culturally and linguistically diverse background;
- explain to SPF consumers their rights under the entity's IDR mechanism and the SPF external dispute resolution (EDR) scheme authorised for the entity's regulated sector; and
- understand the entity's obligations under the SPF provisions and how staff members can support compliance with those obligations.

The policies and procedures must also provide for the training to be provided to an SPF staff member within a reasonable time after the staff member begins to be engaged by the entity, and at least once every 12 months following the first time it is provided.

This obligation supports the obligation in paragraph 58BD(1)(a) of the Act to ensure that the relevant staff of regulated entities have training and expertise to support compliance with the SPF.

Relevant staff includes any staff that have duties related to the SPF obligations. It is expected that to comply with this obligation, a regulated entity will, for example, require relevant staff to undertake mandatory compliance training. This could be in the form of online self-paced learning modules, in person training or a combination of both. Ultimately the form of the training is a matter for the regulated entity to decide provided it meets the requirements discussed above.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Division 3—Common SPF code provisions for SPF principle 2: Prevent

The SPF principle of Prevent in Subdivision C of Division 2 of Part IVF of the Act requires regulated entities to take reasonable steps to prevent another person from committing a scam relating to, connected with, or using a regulated service of the entity (see in particular section 58BJ of the Act).

Obligations specified in Division 3 of Part 2 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Prevent.

Section 2-4: Reasonable systems, processes and resources

Regulated entities must have reasonable systems, processes and resources (including financial, technological and human resources) to ensure compliance with:

- the provisions of SPF Principle 2—Prevent, under Subdivision C of Division 2 of Part IVF of the Act
- a provision of an instrument made under Part IVF of the Act that applies to the entity and relates to the matters covered by that principle.

A regulated entity must implement, monitor and regularly review these systems and processes to ensure they remain fit for purpose (see section 6-2).

It is expected that, when determining whether systems, processes and resources are adequate a regulated entity should consider:

- the risk of scams faced by the entity for the sector based on the size and capability of the entity's regulated services;
- the kinds of SPF consumers of those regulated services;
- how these regulated services are provided and delivered;
- current and past scam incidents faced by the entity;
- magnitude of potential harm or loss to SPF consumers in the event of a scam incident;
- whether they are supported by investment commensurate with the size, sophistication and nature of the entity;
- whether they leverage contemporary technology that a reasonable person would expect for an entity of its size, sophistication and nature; and
- whether they are supported by processes in place to promote continuous improvement.

This obligation ensures that regulated entities dedicate adequate resources to support effective SPF compliance. This obligation is framed to ensure it can adapt to the size and operation of a particular entity. This ensures that smaller regulated entities are not subject to disproportionate burdens, while still requiring them to allocate resources adequate to their circumstances to support effective SPF compliance. This obligation prevents

regulated entities from underinvesting in resources to ensure SPF compliance and minimise their SPF consumers being at heightened risk of scam threats.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-5: Maintain secure systems

A regulated entity for a regulated sector must have reasonable and secure systems to protect SPF consumers' information and accounts from being accessed or misused by another person who is, or may be, facilitating or committing a scam relating to, connected with, or using a regulated service of the entity. A regulated entity must implement, monitor and regularly review these systems to ensure they remain fit for purpose (see section 6-2).

Specifically, the regulated entity must:

- undertake regular assessments of its systems to detect potential security vulnerabilities; and
- undertake ongoing testing, patching and updating of the software used in its systems.

When considering whether a regulated entity has reasonable and secure systems to protect SPF consumers' information and accounts, the following are relevant:

- compliance with applicable privacy laws;
- compliance with recognised industry standards
- whether security and governance measures are proportionate to the size, nature and sensitivity of the SPF consumers' information and accounts it holds or manages; and
- whether contemporary, appropriate and effective technologies are used to identify, mitigate and manage information security risks of a kind expected of a business of the entity's size and sophistication.

This obligation is not a general-purpose cybersecurity requirement. Instead, this obligation ensures regulated entities' digital systems are adequately robust to prevent the types of compromises that can result in scams. This is important because scammers often exploit vulnerabilities in digital systems to gain unauthorised access to consumer accounts, intercept communications, or steal personal or other information that can be misused to commit scams.

The types of breaches or breach attempts entities' systems should protect against include:

- unauthorised access to consumers' online accounts through exploitation of weak or outdated authentication methods;
- interception of sensitive communications between consumers and the entity due to inadequate encryption protocols; and
- exposure of consumers' personal information, which can be used by scammers to facilitate phishing and other types of scams.

The section does not prescribe exactly how SPF consumers' information and accounts should be secured. Instead, entities are required to protect SPF consumer information and accounts. This means the obligation will apply over time as scam risks and technological developments evolve.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-6: Supervise third party service providers

Regulated entities must have reasonable systems and processes to ensure that its agents and third party service providers act consistently with:

- the provisions of SPF Principle 2—Prevent, under Subdivision C of Division 2 of Part IVF of the Act; and

- a provision of an instrument made under Part IVF of the Act that applies to the entity and relates to the matters covered by the Prevent SPF Principle.

For the purposes of this obligation, a ***third party service provider*** is an entity that, under an arrangement with the regulated entity, is authorised to deliver, facilitate or support a regulated service of the regulated entity or any part of that service.

A regulated entity must implement, monitor and regularly review these systems and processes to ensure they are fit for purpose (see section 6-2).

Without limiting what may be reasonable systems and processes the systems and processes must include that the regulated entity must:

- take due skill and care when selecting a suitable agent or other third-party service provider;

- monitor the ongoing performance of its agents and other third-party service providers to ensure compliance with the regulated entity's SPF obligations; and

- appropriately deal with any action by an agent or other third-party service provider that results in a breach of the regulated entity's SPF obligations.

This means that this section requires regulated entities to have reasonable systems and processes to ensure agents and third party service providers both to ensure the regulated entity complies with its own SPF obligations, and also to require the regulated entity to have in place systems and processes to ensure the agents and third party service providers act consistent with the Prevent principle.

Many regulated entities outsource part or all of their regulated services, as well as use principal-agent arrangements as part of their regulated services. This obligation has the effect of ensuring that regulated entities cannot avoid liability under the SPF by outsourcing their regulated services.

This obligation ensures that regulated entities undertake appropriate supervision of any third-party service providers that are supporting the regulated entity to provide part or all of a regulated service of the regulated entity.

The obligation captures ordinary outsourced arrangements, but also arrangements where the regulated entity provides a service that is white-labelled through the owner/provider of the service.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Example

A regulated bank has a contractual agreement with a third-party service provider to provide cloud services for its digital systems, including its account management and customer portals, so the third-party service provider is supporting the delivery of the regulated service by that bank. The bank relies in part on these cloud services to meet its obligations under the SPF to maintain secure systems.

Under this arrangement, the bank is responsible for complying with its obligations under the SPF. Given the third-party service provider is authorised to support the delivery of a regulated service of the bank, the bank must adequately supervise the third-party service provider's delivery of the contracted services to ensure the provider's compliance with the SPF. The bank must also have arrangements in place to ensure any non-compliance with the SPF Prevent principle by the third party is identified and reported to the regulated entity in a timely way and appropriately dealt with.

Section 2-7: Brand impersonation

A regulated entity for a regulated sector must have reasonable systems and processes to prevent brand impersonation. A regulated entity must implement, monitor and regularly review these systems and processes to ensure they remain fit for purpose (see section 6-2).

These systems and processes must enable the regulated entity to:

- inform SPF consumers of the entity's regulated service about the regulated entity's official communication channels for customer engagement (for example, that the entity only contacts customers through its mobile application);
- protect the communication channels used for customer engagement from brand impersonation (including "spoofing");
- monitor the internet for brand impersonation; and
- for websites containing brand impersonation material—promptly send a request to the publisher of the website to remove the material.

When considering whether the entity has taken reasonable steps to comply with this obligation, regard must be had to the following matters:

- the risk that a scam relating to, connected with, or using a regulated service of the entity will be committed considering:
  - the type and scale of regulated services provided by the entity; and
  - scams relating to, connected with or using the regulated service that have previously been committed; and
- the types of SPF consumers who use or are likely to use a regulated service of the entity;
- how the entity's regulated services are provided;
- the current and emerging threat of scams occurring in the entity's regulated sector;
- whether the amount invested by the entity to comply with this obligation is commensurate with the type and scale of regulated services provided by the entity;
- the appropriateness of using contemporary technologies to counter scam threats;
- mechanisms for continuous improvement;
- consistency with relevant industry standards and practices, and
- the magnitude of potential harm or loss to SPF consumers if scam activity occurs.

This obligation is intended to prevent scams such as where a person impersonates a business to deceive victims into giving personal or financial information or sending money to the scammer.

Protect communication channels

This limb of the obligation is aimed at ensuring that customers understand what an entity's legitimate communication channels are, to help prevent customers from getting scammed by interacting with scammers impersonating regulated entities outside those channels.

Steps a regulated entity may take under this obligation include, for example:

- sending emails or producing advertising to inform customers how they will act with sensitive information; for example, clear messaging by a regulated entity that it will never ask for sensitive information like passwords;
- using any available protections provided by the entity's telecommunications provider to prevent impersonation scam calls; and
- registering the entity's alpha tags with the Australian Communications and Media Authority's SMS Sender ID Register (as defined in sections 7 and 483E of the *Telecommunications Act 1997*).

Other measures regulated entities in the banking sector may additionally implement in compliance with this obligation include:

- informing their customers that they do not use links in text messages to customers, so customers can better recognise whether a text from or purportedly from their bank is a scam; and

- authentication features, such as in-app systems, that verify the customer's identity or enable the customer to verify when they are speaking to banking staff.

Monitoring the internet

Scammers may use illegitimate websites that mimic the brand of a regulated entity or otherwise provide false contact information for a regulated entity. This limb of the obligation ensures regulated entities proactively monitor for this, take action to remove such material, and inform their customers of the scam risk.

This is intended to reflect current practice of some entities in the banking, telecommunications and digital platforms sectors (for example, monitoring mentions of their brand on social media channels and in news publications). The scope of this obligation is proportionate to the type and scale of the regulated entity's regulated service. For example, this means that entities with a larger market presence or higher exposure to risk are expected to do more than a smaller entity with lower-risk exposure. What is required to meet this standard will therefore differ depending on the regulated entity's role, scale and the level of risk its activities create. This section does not limit the ways regulated entities can undertake monitoring. For example, it may be sufficient to capture news alerts, regular checks of social media channels and specific brand monitoring tools.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-8: Consumer awareness

A regulated entity for a regulated sector must make information about the risk of scams related to the entity's regulated service publicly available.

This information must include:

- common types of scams related to the entity's regulated service;

- the mechanisms and services available to SPF consumers of the entity's regulated service which may assist its SPF consumers to protect themselves from scams; and

- website links and contact details for other publicly available resources about scams.

The information must also be easy to understand and locate, including for a person with disability, or from a culturally and linguistically diverse background. It must also be regularly updated to reflect current scam risks and incidents.

The intention of this obligation is to help prevent scams by raising consumer awareness. The requirement that the information relates to common types of scams related to the entity's regulated service requires the entity to tailor the information to its specific service, rather than only setting out general purpose information. It reflects the existing practice of many entities in the banking and digital platforms sectors who already have websites or

application pages that inform consumers of scams related to their services and provide consumers with security alerts and guides on how to spot, avoid and report scams.

Information would be publicly accessible for the purposes of this obligation if it were included prominently on the regulated entity's website. It may also be necessary in specific circumstances for the regulated entity to provide other forms of access to the information. For example, where consumers interact in person with the regulated entities, such as in bank branches, the information should also be provided in hard copy (for example, in pamphlets).

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Division 4—Common SPF code provisions for SPF principle 3: Detect

The SPF principle of Detect in Subdivision D of Division 2 of Part IVF of the Act requires regulated entities to take reasonable steps to detect a scam relating to, connected with, or using a regulated service of the entity. This includes both investigating activities that are the subject of actionable scam intelligence, and identifying consumers impacted by these activities, in a timely way.

Obligations specified in Division 4 of Part 2 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Detect.

Section 2-9: Reasonable systems, processes and resources

Regulated entities must have reasonable systems, processes and resources (including financial, technological and human resources) to ensure compliance with:

- the provisions of SPF Principle 3—Detect, under Subdivision D of Division 2 of Part IVF of the Act; and
- a provision of an instrument made under Part IVF of the Act that applies to the entity and relates to the matters covered by that principle.

A regulated entity must implement, monitor and regularly review these systems and processes to ensure they are fit for purpose (see section 6-2).

For the factors an entity should have regard to when complying with this principle, see those discussed above in relation to section 2-4.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-10: Identifying an activity as a scam

Under subsection 58BN(1) of the Act, a regulated entity who has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity must take reasonable steps to investigate whether or not the activity is a scam. This investigation must be undertaken during a 28-day period starting on the day the regulated

entity first has the actionable scam intelligence. Consistent with the definition of actionable scam intelligence in section 58AI of the Act, this will capture circumstances including:

- when the entity first forms reasonable grounds to suspect a communication, transaction or other activity relating to, connected with, or using its regulated service is a scam; or

- when the entity first receives information from a third party about a communication, transaction or activity so relating or connected to its service about which it has those reasonable grounds.

Section 2-10 requires a regulated entity who has actionable scam intelligence relating to, connected with, or using a regulated service of the entity to identify whether or not the activity is a scam. If the entity has reasonable grounds to believe that the activity is a scam, the entity must identify the activity as a scam. Whether there are reasonable grounds for such a belief is an objective test. This imposes a positive obligation on a regulated entity to identify an activity is a scam, if there are reasonable grounds to believe the activity is a scam.

Regard must be had to the following non-exhaustive factors when considering whether or not the activity is a scam:

- information that corroborates the actionable scam intelligence about the activity (if any);

- characteristics of the activity shared with other scams;

- the number of reports submitted to the entity in relation to the activity;

- the presence of common indicators of consumers at high risk of scam activity;

- any known systemic or widespread scam issues or risks.

This obligation is broad and will adapt to size and operation of the particular regulated entity.

This obligation operates alongside but independently of the 28-day timeframe set out in section 58BN of the Act.

If a regulated entity has reasonable grounds to believe the activity is or is not a scam before the end of the 28-day investigation period, then when it forms those grounds, the safe-harbour provisions under subsection 58BZA(2) of the Act will no longer apply (see paragraph 58BZA(2)(d).

While the activity related to actionable scam intelligence is subject to investigation, and not yet identified as a scam or not a scam, it will be considered a suspected scam.

Generally, before an entity has identified if an activity is a scam, the entity will be required to take a risk-based approach to disrupt the suspected scam (see 2-15: Risk assessment for disruptive actions). It may also be required to take action consistent with a code applying to its specific regulated sector.

The obligation to identify whether an activity is a scam works in conjunction with several obligations in Principle 4—Disrupt.

If an entity has identified an activity as a scam, it may need to consider other sector-specific disrupt obligations. For example, if a bank has identified that a transaction giving effect to a payment to another account is a scam, it must reverse, or request the reversal of, the effect of that transaction as soon as practicable (see *3-11 Payment recall requests*).

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-11: Recording information about investigation

Subject to the exception below, a regulated entity who has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity must record information relevant to the entity's investigation into that activity.

The information must include (but is limited to) the following:

- whether or not the regulated entity identifies the activity as a scam;
- information supporting the entity's consideration of the factors mentioned in subsection 2-10(3); and
- the method used to initiate contact with the relevant SPF consumers of the entity's service, such as telephone calls, text messages, emails and social media; and
- if the entity identifies the activity as a scam:
  - the type of scam;
  - the mechanisms and identifiers used to scam, or attempt to scam, the SPF consumers, such as URLs, email addresses, phone numbers and social media profiles.

However, a regulated entity is not required to record information if the information can only be obtained from an SPF consumer and the entity has been unable to obtain that information from the SPF consumer. This may be because the SPF consumer has chosen not to engage with the regulated entity so the entity cannot collect relevant information. This means practical barriers that might exist to obtaining information from a person who does not wish to provide consent to the collection and use of that information do not cause the regulated entity to be non-compliant with this obligation.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-12: Identifying affected SPF consumers

Subject to the exception below, a regulated entity must have reasonable systems and processes to identify SPF consumers of the entity's regulated service who have, or may have, been affected by an activity about which the entity has actionable scam intelligence.

This obligation complements section 58BO of the Act, which requires regulated entities 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 an activity about which the entity has actionable scam intelligence.

The systems and processes must enable the entity to identify the direct SPF consumers of the regulated service and take reasonable steps to identify SPF consumers who are not direct SPF consumers of the regulated service, as soon as practicable after the intelligence becomes actionable scam intelligence for the entity. As noted above, this will capture both where the entity had intelligence before it identified the intelligence was actionable scam intelligence, as well as where the entity receives actionable scam intelligence about its services from someone else.

A regulated entity must implement, monitor and regularly review these systems and processes to ensure they remain fit for purpose (see section 6-2).

This obligation ensures that regulated entities have the structure and capability to identify SPF consumers that have been or may be impacted. However, a breach of this obligation does not necessarily occur simply because a regulated entity fails to identify an SPF consumer.

This obligation is works with section 2-14: Notify affected SPF consumers, which requires regulated entities to notify an SPF consumer that has, or may have, been affected by the activity.

Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Division 5—Common SPF code provisions for SPF principle 4: Disrupt

The SPF principle of Disrupt in Subdivision F of Division 2 of Part IVF of the Act requires regulated entities to take reasonable steps to disrupt an activity that is the subject of actionable scam intelligence and prevent losses from such an activity. It also imposes reporting requirements to the SPF general regulator about the outcomes of an entity's investigation.

Obligations specified in Division 5 of Part 2 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Disrupt.

Section 2-13: Reasonable systems, processes and resources

Regulated entities must have reasonable systems, processes and resources (including financial, technological and human resources) to ensure compliance with:

- the provisions of SPF Principle 4—Disrupt, under Subdivision F of Division 2 of Part IVF of the Act

- a provision of an instrument made under Part IVF of the Act that applies to the entity and relates to the matters covered by that principle.

A regulated entity must implement, monitor and regularly review these systems and processes to ensure they remain fit for purpose (see section 6-2).

For the factors an entity should have regard to when complying with this principle, see those discussed above in relation to section 2-4.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-14: Notify affected SPF consumers

A regulated entity who has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity must take reasonable steps to notify an SPF consumer of the regulated service that the consumer has, or may have, been affected by the activity. This is intended to follow the identification of affected SPF consumers required by section 2-12.

The notification must:

- be given as soon as practicable after the intelligence becomes actionable scam intelligence for the entity;
- be relevant and proportionate to the risk of loss or harm arising from the activity; and
- if the entity has contact details for the SPF consumer:
  - be given to the SPF consumer using the most appropriate contact details; and
  - explain the reason that the entity suspects the SPF consumer is, or may be, affected by the activity.

Whether the notification meets the above will depend on the circumstances. For example, where actionable scam intelligence is received by a regulated entity that is a bank that a bank account held by a person is being used to facilitate scams, the bank should identify customers that have made payments to that account (see section 2-12: Identifying affected SPF consumers). The bank should also notify these customers that they may have been impacted by a scam. The notification should include information about why the bank suspects the customer may have been impacted by a scam and provide information about the risk of loss or harm of the scam, including the risk of further loss or harm. The requirement that the notification be relevant and proportion means it would not be sufficient for the bank to provide general information to all customers, including affected customers, about the suspected scam.

Where actionable scam intelligence involves a less direct link between the SPF consumer and the entity, it may not be proportionate to notify all individual clients personally (for example by phone). For example, where consumers might have seen brand impersonation of a bank on social media, an email or public alert (such as an update on the entity's

website) warning SPF consumers about the risk may be sufficient. This would depend on the circumstances of the brand impersonation.

The obligation to notify may connected to particular activities in respect of which there may be multiple pieces of actionable scam intelligence. This means that one notification could draw on or reflect multiple pieces of actionable scam intelligence.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Tipping off – banking sector

For regulated entities of the banking sector under the Anti-Money Laundering and Counter-Terrorism Financing regime, the SPF does not require those entities to act contrary to the "tipping off" offence under section 123 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. It is expected that regulated entities take a risk-based approach to determining how to notify impacted consumers in a way that is consistent with their obligations.

Section 2-15: Risk assessment for disruptive actions

A regulated entity that has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity must undertake a risk assessment of the activity to inform the proportionate disruptive action to be taken by the entity.

This obligation relates to subsection 58BX(1) of the Act, which requires regulated entities to take reasonable steps within a reasonable time to disrupt the activity or prevent loss or harm (including further loss or harm) arising from the activity. Subsection 58BX(3) of the Act requires that disruptive action should be proportionate to the actionable scam intelligence that the entity has about the activity.

When undertaking the risk assessment to determine what disruptive action should be taken, the regulated entity must consider:

- whether the entity suspects or reasonably believes that the activity is a scam;
- the likelihood and severity of potential loss or harm caused by the activity;
- the nature of the activity and the presence of any high-risk indicators of a scam;
- known systemic or widespread scam issues or risks (including information shared by SPF regulators); and
- if the activity is suspected, but not yet identified, to be a scam:
  - the strength of the actionable scam intelligence;
  - the potential loss or harm to SPF consumers and persons carrying on the activity if disruptive action is taken and the activity is not a scam; and
  - the extent to which it would be reasonably practicable to reverse the disruptive action if the entity identifies that the activity is not a scam.

Several specific other obligations require regulated entities to take specific disruptive actions when an entity has actionable scam intelligence or a scam is identified. For example, digital platforms are required to suppress, reduce or limit an activity from being displayed to SPF consumers when actionable scam intelligence about the activity is attained (*5-9: Disruptive action during investigation*). However, the action required such in this instance will need to be taken regardless of a risk assessment.

Contrastingly, this obligation requires entities to undertake a risk assessment to inform the proportionate disruption of a scam once an entity has actionable scam intelligence separate to any standalone obligations in this Instrument to take specific disruption activities. This provides flexibility for entities to respond to unique scam threats in a way that mitigates consumer harms while considering the risk of unintended consequences, particularly where a scam is still being investigated.

A risk assessment should be an ongoing process for considering how information gathered about the activity should inform what disruptive action should be taken both during and after the investigation period. The nature or scale of the risk assessment will depend on the circumstances.

Further, this does not prevent the entity from taking disruptive action immediately after attaining actionable scam intelligence, if the entity has reasonable grounds to believe that action is necessary to prevent loss or harm (including further loss or harm) arising from the activity. Similarly, a risk assessment should inform whether ongoing disruptive actions are reasonable for the activity and how disruptive actions may need to change as further information about the activity is considered.

Section 58BZA of the Act provides a safe harbour for a regulated entity taking actions while investigating whether an activity subject of actionable scam intelligence is a scam.

This section does not apply in relation to a regulated telecommunications provider (see sections 1-5 and 2-1).

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-16: Reverse disruptive actions if not a scam

Where a regulated entity has taken disruptive action to disrupt an activity that, at that time, was suspected to be a scam, but after the disruptive action is taken the entity identifies that the activity is not in fact a scam, the entity must, to the extent reasonably practicable, reverse the disruptive action. They must do this as soon as practicable after the entity identifies that the activity is not a scam.

Under paragraph 58BZA(2)(e) of the Act, the regulated entity is not liable in a civil action or civil proceeding for taking action to disrupt the activity if the action is promptly reversed if:

- the entity identifies that the activity is not a scam; and
- it is reasonably practicable to reverse the action

- the other requirements in subsection 58BZA(2) are made out.

To be protected by the safe harbour under section 58BZA of the Act, a regulated entity must promptly reverse any disruptive action taken if it identifies the activity is not a scam. This obligation ensures such compliance by imposing a positive obligation to reverse the action. For example, it is expected that a regulated bank would restore to the account holder's control any bank account that it blocked, banned or froze while they investigated whether suspicious activity on that account was a scam, if the bank subsequently identifies the activity was not a scam.

This section does not apply in relation to a regulated telecommunications provider (see sections 1-5 and 2-1).

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Division 6—Common SPF code provisions for SPF principle 6: Respond

The SPF principle of Respond in Subdivision G of Division 2 of Part IVF of the Act requires, among other things, that regulated entities have an accessible mechanism for its consumers to report activities that are or may be scams, and an accessible and transparent IDR mechanism for scam complaints.

Section 2-17: Reasonable systems, processes and resources

Regulated entities must have reasonable systems, processes and resources (including financial, technological and human resources) to ensure compliance with:

- the provisions of SPF Principle 6—Respond, under Subdivision G of Division 2 of Part IVF of the Act

- a provision of an instrument made under Part IVF of the Act that applies to the entity and relates to the matters covered by that principle.

A regulated entity must implement, monitor and regularly review these systems and processes to ensure they remain fit for purpose (see section 6-2).

For the factors an entity should have regard to when complying with this principle, see those discussed above in relation to section 2-4.

SPF sector regulators will be able to take action to correct insufficient arrangements, systems or resources to ensure the entity's proper compliance with the SPF.

This obligation is intentionally broad so it adapts to the size and operation of regulated entities.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-18: Requirements for reporting mechanisms

A regulated entity's reporting mechanism must meet the following conditions:

- be free of charge for a person to make, and monitor the progress of, a report about an activity that is or may be a scam;
- be easy to understand, locate and use, including by a person with disability, or from a culturally and linguistically diverse background;
- include multiple options for a person to report an activity that is or may be a scam;
- include an option, that is easy to understand, locate and use, for a person to access assistance from an SPF staff member within a reasonable time after the person requests the assistance; and
- be able to receive reports at any time (that is, have "24/7 availability").

A regulated entity must not charge, or cause to be charged, a fee for a person to access information about the entity's reporting mechanism.

<u>24/7 Availability</u>

Ensuring that SPF consumers can make scams reports at any time facilitates timely reporting, more efficient scam disruption by the regulated entity, and better outcomes for consumers.

It is intended that this obligation could be satisfied by a 24/7 telephone number, email, or other form of online submission, such as a website or an app portal.

It is not necessary that access to a human representative is similarly available 24/7. This is because there may be a considerable volume of suspected scam/scam reports and no benefit to have human access in some circumstances.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-19: Acknowledgement of scams report

If a regulated entity receives a report through its reporting mechanism about an activity that is or may be a scam, the regulated entity must acknowledge receipt of the report within 24 hours after the report is received. The purpose of the report acknowledgement is to ensure consumers know that their report has been received, to provide them information that there is a separate complaint process so they do not conflate reports and complaints, and to advise them of actions they can take to minimise the loss.

The acknowledgement must, in relation to the person who made the report (the reporting person):

- include suggested actions, which may be general in nature, to mitigate the risk of harm or loss (or further harm or loss) from the activity. For example, the acknowledgement might reasonably suggest that the reporting person contact their

bank (if the report is made to a non-bank) as soon as possible to try to freeze or recall transactions;

- advise the reporting person that they may nominate a preferred contact method or contact person and any accessibility requirements;
- if the reporting person has nominated any accessibility requirements, advise that, as far as possible, those requirements will be accommodated;
- include a summary of the information required to be published under subsection 58BZF(1) of the Act and how that information may be accessed; and
- be in the form the regulated entity considers to be most suitable, taking into account the way the report was made. For example, if a consumer provides a verbal complaint to an entity, the entity may deem it most suitable to provide a verbal form of acknowledgement to the consumer (subject to the below requirement to follow up with written acknowledgement).

For the purposes of the second-last dot point, the information required is the information about the rights of SPF consumers of the entity's regulated services for the sector under reporting mechanism, the IDR mechanism, and if the entity is a member of an SPF EDR scheme for the sector, the SPF EDR scheme.

An acknowledgement is only required when the report is made through the regulated entity's reporting mechanisms. Therefore, if a person reports a scam through an alternate reporting avenue, this section does not apply. For example, a consumer posting on their own social media about a scam involving a bank would not require acknowledgement from that bank.

In some cases, a consumer will provide incorrect or false contact information in a report. Where this occurs, an entity is not expected to take steps to gather correct information from the consumer to provide the acknowledgment.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Content of acknowledgement

An acknowledgment is not required to include tailored information. This means, if suitable, an automated or standard response acknowledging a scam report will comply with this obligation, provided it complies with the other above requirements.

It is intended that the actions referred to in the acknowledgement about mitigating harm should be within the consumer's abilities and controls. For example, the entity may suggest that the consumer contact their bank to reverse transactions if the consumer has not already done so, change passwords, not transferring any or any further funds, and pausing debit or credit cards. The information could also be about where the SPF consumer can get further support, such as IDCARE.

Form of acknowledgment

As above, the regulated entity must consider the most appropriate form for the acknowledgement – for example, verbally or in writing, taking into account how the

person made the report. However, where an acknowledgement is made verbally, because, for example, the person reported the scam over the phone, and where the reporting person has nominated an appropriate contact method, the entity must follow up with an equivalent written acknowledgement as soon as practicable.

The time constraint of 24 hours ensures that the person who made the report has confidence that the report has been received and quickly has information to assist them with taking action to mitigate any loss or harm.

Section 2-20: Timely assistance to reporting person

A regulated entity for a regulated sector must give timely assistance and support to a person who makes a report about an activity that is or may be a scam, appropriate to the nature of the report.

This obligation ensures there are no unnecessary delays in progressing scams reports, and that persons who have made a report are supported in a timely manner and are provided ongoing support and responses to any further information/requests they make. This is important as there is no intention to prescribe timeframes for progressing these matters.

An SPF consumer may make a report under section 58BZC of the Act to a regulated entity about a suspected scam, or a scam attempt. In this case, the person may not have suffered loss or harm and is merely alerting the regulated entity to the scam or scam attempt. Beyond acknowledging the scam report, there may be nothing further the regulated entity may do to assist the reporting person, and the report could be considered resolved.

Another circumstance will be where a scam report made under section 58BZC of the Act may be an SPF consumer making a report of a scam that they allege they have suffered loss or harm from. In some instances, it might then be reasonable that an entity proactively tries to mitigate scam loss or harm on receipt of such a report, in line with other SPF principles such as the Disrupt principle. For example, if a person has transferred money out of their bank account and contacts their bank when they realise they have been scammed, on receiving the report the bank might reasonably seek to disrupt the scam by freezing or recalling funds, consistent with its other obligations under the SPF. The person may not be alleging or complaining about the regulated entity's conduct in relation to that scam, but this does not prohibit the entity from considering whether compensation is appropriate prior to the report escalating to a complaint.

A report will escalate to a complaint when the SPF consumer makes a complaint about the regulated entity's conduct relating to an activity set out in paragraph 58BZD(1)(a) or (b) of the Act and the report should at that point be considered resolved (noting it is being dealt with as a complaint).

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-21: Requirements for internal dispute resolution mechanisms

A regulated entity's IDR mechanism must:

- be free of charge for a person to make, and monitor the progress of, a complaint about an activity that is or may be a scam or the entity's conduct relating to such activity;

- be easy to understand, locate and use, including by a person with disability or from a culturally and linguistically diverse background;

- include multiple options for a person to make a complaint about an activity that is or may be a scam, or the entity's conduct relating to such activity and

- include an option, that is easy to understand, locate and use, for a person to access assistance from an SPF staff member within a reasonable time after the person requests the assistance.

A regulated entity also must not charge, or cause to be charged, a fee for a person to access information about the entity's internal dispute resolution mechanism.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Free of charge

For both sections 2-18 and 2-21, the obligation to not charge a fee ensures there are no costs-based barriers limiting the accessibility of a regulated entity's reporting (section 2-18) and IDR processes (section 2-21). It is designed to apply to a regulated entity's scam reporting mechanism as well as its IDR mechanism.

Easy to understand, locate and use

The following are examples of matters that may be relevant in determining whether the mechanisms are easy to understand, locate and use for both the reporting (section 2-18) and IDR mechanisms (section 2-21):

- consistency with any applicable industry standards that separately apply to the regulated entity (including for example Australian Securities and Investments Commission (ASIC) Regulatory Guide 271: Internal Dispute Resolution)

- provision of multiple avenues to access the mechanism (such as via telephone, email, website and applications)

- use of plain language and clear instructions

- availability of a range of languages and formats

- consideration of the privacy, safety and confidentiality of users, and

- making trained staff available to provide support or assistance.

Multiple reporting and complaint lodgement methods

This obligation is aimed at ensuring that reporting (section 2-18) and IDR mechanisms (section 2-21) are accessible, and allow SPF consumers to make reports or complaints in a

way that is connected to the way the scam is encountered. For example, where an SPF consumer receives a phishing email, the SPF consumer should be able to make a report or lodge a complaint with an email address. This is to reduce barriers and difficulty for SPF consumers in reporting and making complaints.

Examples of methods that may be appropriate include email, phone, social media, and in person.

24/7 availability not required for IDR mechanism

Unlike section 2-18 above, relating to reporting, there is no obligation for entities to be able to receive IDR complaints at any time in section 2-21. This is because there is less urgency with respect to complaints. For example, consumers would be encouraged to use the 24/7 reporting mechanism for matters that might require urgent action from the regulated entity to disrupt a scam.

Section 2-22: Detecting issues with internal dispute resolution mechanism

A regulated entity's required policies and procedures under the Governance principle must:

- set clear accountabilities for the identification of issues with the operation of the entity's IDR mechanism;
- require, enable and assist the entity's staff to promptly escalate possible issues with the operation of the entity's IDR mechanism; and
- deal with how issues with the operation of the entity's IDR mechanism will be identified and managed including, but not limited to, by requiring the entity to regularly analyse data held by the entity.

This requires regulated entities to examine their IDR mechanism for ways in which it may not be working effectively, and to ensure regulated entities have processes to identify issues and make improvements where needed. An effective IDR mechanism is much more likely to resolve consumer complaints in a timely way.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-23: Acknowledgement of internal dispute resolution complaint

If a regulated entity for a regulated sector receives a complaint through its IDR mechanism about an activity that is or may be a scam or the entity's conduct relating to such activity, the entity must acknowledge receipt of the complaint as soon as practicable. The acknowledgement may be in the form of an automated response. While not as time sensitive as a report acknowledgement where timely action could make a difference to mitigating scam loss or harm, the complaint acknowledgement should be sent as soon as practicable. This is important because a person who has been scammed will be keen to confirm that complaint has been received and will be actioned and to understand the complaints process and what to expect.

Specifically, the acknowledgement must:

- include suggested actions, which may be general in nature, to mitigate the risk of harm or loss (or further harm or loss) from the activity. This might, for example, include suggesting that the SPF consumer change passwords, not transfer any (or any further) funds, or pause debit/credit cards;

- provide a summary of the regulated entity's key steps for dealing with complaints, including timeframes for those steps;

- advise the complainant that they may nominate a preferred contact method or contact person and any accessibility requirements;

- if the complainant has nominated any accessibility requirements—advise that, as far as possible, those requirements will be accommodated;

- include a summary of the information required to be published under subsection 58BZF(1) of the Act and advise how that information may be accessed;

- if relevant, advise the complainant that there may be other regulated entities whose activities or conduct may relate to the suspected scam to which the complainant could consider making a report or complaint; and

- be in the form the regulated entity considers to be most suitable, taking into account the way the complaint was made.

This obligation complements subsection 58BZF(1) of the Act which requires a regulated entity for a regulated sector to make certain information about the rights of SPF consumers of its regulated services publicly accessible.

A complaint is considered resolved where the complainant and regulated entity have agreed to an outcome. A complaint would also be considered resolved, or the regulated entity would have met its obligation to resolve IDR mechanism complaints, when the regulated entity has determined the complaint to be frivolous or vexatious, noting that the complainant would retain the right to escalate to EDR.

If a complaint acknowledgement is made verbally (for example on the telephone), and the complainant has nominated an appropriate contact method for written acknowledgement, the entity must also give the complainant the acknowledgement in writing as soon as practicable.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-24: Timely resolution of complaints

A regulated entity must have reasonable systems and processes to ensure that complaints received through its IDR mechanism about an activity, or the entity's conduct relating to an activity, are dealt with as quickly as possible, in consideration of the complexity of the complaint and the scale of the activity.

A regulated entity must implement, monitor and regularly review these systems and processes (see section 6-2).

It is not expected that a regulated entity needs to deal with a complaint that is about the same activity, or the same conduct, that is the subject of an existing process, or an earlier complaint by the same complainant that has been resolved.

This obligation ensures that regulated entities have a positive obligation to resolve complaints as soon as practicable – what is practicable depends on aspects of the complaint, such as novelty, complexity, the number of entities involved, and the monetary amount.

Many complaints can be resolved within a short timeframe, including at first point of contact with the entity after the complaint is made.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-25: Notice if complaint not resolved within 30 days

A regulated entity for a regulated sector, who has received a complaint through its IDR about an activity that is or may be a scam, must provide certain information to the person who made the complaint if the complaint is not resolved within 30 calendar days. Regulated entities who do not resolve complaints within 30 days must provide the following:

- reasoning as to why the complaint has not been resolved within 30 days; and
- a summary of the complainant's rights under the SPF EDR scheme authorised for the entity's regulated sector and how to access the scheme.

This obligation supports objectives of complaints being settled a timely manner and ensures that SPF consumers are receiving timely communication. If a complaint is not resolved within 30 days, the regulated entity must provide information listed above, so that the complainant is aware of why there has been a delay and to provide them with information on the option to seek a resolution through EDR.

This is designed to align with the timeframes for the statement of compliance in the SPF rules, so that entities have 21 calendar days to provide the statement of compliance and then an additional 9 days to attempt to settle complaints, including multiparty complaints where regulated entities are working together to resolve a shared complaint (a complaint from the same SPF consumer about the same scam).

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-26: Cooperation between regulated entities

Regulated entities must have reasonable systems and processes in place to facilitate cooperation with other regulated entities when it comes to receiving complaints through their IDR mechanisms.

A regulated entity must implement, monitor and regularly review these systems and processes to ensure they remain fit for purpose (see section 6-2).

The systems and processes must enable the entity to respond to requests for information or queries from other regulated entities in relation to the complaint in a reasonable time and

cooperate with other regulated entities to apportion liability between the entities (as necessary), including sharing information (as appropriate) about assessments of liability for the loss or harm suffered by the complainant.

This obligation is intended to ensure that regulated entities adopt a coordinated and consistent approach to resolving complaints that involve multiple parties under the SPF. Scams frequently involve more than one regulated service and without effective cooperation consumers may face delays, gaps in information or inconsistent outcomes. By requiring regulated entities to cooperate at the IDR stage, this obligation is intended to support timely resolution of complaints, promotes transparent apportionment of liability and reduces the risk of disputes being shifted between entities to the detriment of consumers.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-27: Vexatious or frivolous complaints

Where a regulated entity reasonably considers a complaint received through its IDR mechanism to be frivolous or vexatious, the entity may decide not to deal with, or further deal with, that complaint. In this case, the regulated entity must give the complainant written notice of the decision that includes reasons for the decision and information about the complainant's rights under the SPF EDR scheme within 5 business days of making the decision.

It is expected that, before determining a complaint is frivolous or vexatious, a regulated entity must appropriately escalate the complaint internally.

Whether a complaint is vexatious or frivolous is a case-by-case analysis. Generally, a complaint will be considered frivolous if it clearly has no real basis, is groundless and done with a particular motive, such as a malicious motive. It will likely be considered vexatious if the complaint is being used for an unrelated purpose or is clearly without merit.

A regulated entity must not consider a complaint to be frivolous only because of the amount of loss to the complainant resulting, or potentially resulting, from the activity that is the subject of the complaint.

A regulated entity's processes for determining whether complaints are vexatious or frivolous should be reflected in its governance policies and procedures required under subparagraph 58BD(1)(a)(ii) of the Act. SPF consumers' rights in relation to those processes should be published in the information required under paragraph 58BZF(1)(b) of the Act.

Further, complying with this obligation does not mean a regulated entity is exempt from compliance with the requirement to give reasonable assistance to, and cooperate with, the EDR scheme operator (per subsection 58BZG(2)) if the complaint being dealt with at EDR is the same complaint the regulated entity determined was frivolous or vexatious.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 2-28: Recording information about complaints

For each complaint made through its IDR mechanism, regulated entities must record the following information:

- details of the complaint, including the date it was made;
- a brief description of the type of activity giving rise to the complaint;
- the date when the complaint was acknowledged;
- the date when the complaint was finalised;
- a brief description of the outcome of the complaint; for example, whether the complaint was resolved, unresolved, withdrawn or escalated to an SPF EDR scheme.

This information must be kept in a way that allows data to be analysed for a particular period. For example, a regulated entity should be able to track complaint metrics for a particular period including:

- total number of complaints made;
- types of scams giving rise to complaints;
- average time taken to acknowledge complaints and resolve them;
- number of complaints escalated to SPF EDR schemes.

Access to dispute resolution and consumer redress is an essential part of the SPF and is critical to its effectiveness. This obligation supports transparent and effective dispute resolution, by requiring all regulated entities to keep consistent information about IDR complaint numbers, resolutions and other relevant metrics received under the SPF.

This obligation ensures entities keep records about complaints for regulatory monitoring and enforcement reasons, but also in the case that a complaint gets escalated to EDR following an unsatisfactory outcome at IDR. Under paragraph 58BZG(2)(b) of the Act, a regulated entity must give reasonable assistance to, or cooperate with, the Australian Financial Complaints Authority, which may include providing these records.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Part 3—Provisions applying to the banking sector

Part 3 contains provisions applying to the SPF code for the banking sector. These provisions set out the obligations to apply specifically to regulated entities in the designated banking sector. Banking services are frequently targeted by scammers, who use a variety of methods to obtain access to consumers' accounts, intercept payment transfers or manipulate consumers into sending money to fraudulent bank accounts. The obligations in this Part are designed to address the inherent risks and features associated with consumers' use of the banking sector.

Part 3 contains 4 divisions:

- Division 1, which concerns preliminary matters;
- Division 2, which outlines provisions applying to the banking sector for Principle 2: Prevent;
- Division 3, which outlines provisions applying to the banking sector for Principle 3: Detect;
- Division 4, which outlines provisions applying to the banking sector for Principle 5: Disrupt.

Division 1—Preliminary

Section 3-1: Purpose of this Part

This section provides that Part 3 of the Instrument sets out the obligations that apply to a regulated bank in relation to the themes or matters covered in the Subdivisions concerning the SPF principles of Governance, Prevent, Detect, Disrupt and Respond, as well as incidental and related matters to those SPF principles.

Division 2—Banking SPF code provisions for SPF Principle 2: Prevent

Obligations specified in Division 2 of Part 3 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Prevent for the banking sector.

Section 3-2: Payee confirmation

If a direct SPF consumer of a regulated bank's regulated service provides information to the bank for a purpose connected with authorising an electronic funds transfer, the bank must, before the transfer is made, enable the SPF consumer to do either of the following:

- if the SPF consumer provides a name, BSB and account to the bank – verify whether the name, BSB and account number matches information held or provided to the bank in respect of the BSB and account number; or
- if the SPF consumer provides a mobile phone number, ABN, email address or other type of authorised identifier (other than a BSB and account number) – view the name associated with the payee identifier if it has been registered for use for electronic funds transfer.

The bank must enable whichever applies to the transaction. The former is relevant where the proposed transaction is via BSB and account number.

In the former case, where the BSB and account number do not match the information held by or provided to the bank, the bank must notify the SPF consumer of this fact, warn them that they may be the subject of a scam, and give the SPF consumer the option not to proceed with the transfer.

A regulated bank must also, on request by another regulated bank, provide that other regulated bank with the information required to comply with this obligation.

Payee confirmation is a preventative measure for scams, or attempted scams, involving a consumer being deceived into authorising an account-to-account payment. Bank transfers are the most common requested payment method by scammers. This obligation enables consumers to verify the recipient of a payment, helping guard against scams such as phishing or payment redirection scams where impersonation is used and the payer expects the payee to be a specific and genuine recipient.

Existing payee confirmation arrangements, for example Confirmation of Payee facilitated by Australian Payments Plus, build on New Payments Platform infrastructure to match the name entered by the consumer and the name held by the receiving bank, when sending a domestic payment using a payee's BSB and account number. This obligation is intended to cover existing technologies used by ADIs. However, the obligation is technologically neutral. This ensures ADIs can choose the most appropriate method for their payee confirmation arrangements to meet the outcomes of this requirement.

Under section 6-1, this section is a civil penalty provision. Failure to comply with these obligations may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 3-3: Identity verification of SPF consumers

A regulated bank must verify the identity of each direct SPF consumer of the bank's regulated service.

The Government is seeking feedback on the final design of this obligation. In particular, the italicised text indicates that the Government is seeking feedback on what banks should be obliged to do in order to verify identity.

Initial intent is that identity verification will require regulated banks to cross-check the identity information obtained from SPF consumers against, for example, reliable identity documents. It is an important "first line of defence" to prevent scammers from opening fraudulent accounts using fake or stolen information.

Identity verification is an ongoing obligation. For example, if a regulated bank becomes aware of circumstances that raise or elevate the scam risk for a particular SPF consumer, then the bank should be required to re-verify the identity of that consumer or obtain additional verification.

It is intended that this obligation will require the regulated bank to have systems and processes to:

- trace transactions and communication to identify the parties involved (and their identifiers such as account names and details, contact information, email and postal addresses etc.),
- identify the SPF consumer's name and client number, and cross-reference that with accounts the person has with the regulated entity, and
- contact the SPF consumer to verify information about details such as their identity or their transaction/account history.

It is intended that this obligation will work alongside existing identity verification obligations imposed on regulated entities by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.*

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 3-4 Systems and processes for identifying high-risk activities

A regulated bank must have reasonable systems and processes to identify the kinds of transactions and activities that relate to, are connected with, or use the bank's regulated service that have a high risk of being, or facilitating, a scam.

What is considered a high-risk activity will depend on the types of scam risks faced by the relevant regulated bank and may change over time. It may include activities that put the SPF consumer at higher risk of being the victim of a scam, or if the activity is related to or connected with a scam, put the SPF consumer at risk of significant loss or harm. The activities contemplated by this provision may or may not be considered actionable scam intelligence.

For example, changing a daily transfer limit may be considered high-risk, as it is a common precursor to many scam types. Similarly, the types of transactions that may be considered high-risk are transactions commonly used by scammers as 'exit-ramps' to move money out of a consumers account so it cannot be recovered by regulated banks, but where, in isolation, these types of transactions or activities would likely not be considered actionable scam intelligence. Some examples of activities that may be captured by this provision include, but are not limited to:

- changing an existing payee's details (mobile details, comprising account)
- changing two factor authentication details;
- adding additional card holders; and
- changes to payment limits.

Some types of transactions that may be captured by the provision include, but are not limited to:

- transferring funds to a new or recently added payee;
- making large or unusual payments that are inconsistent with the customer's typical transaction patterns;
- making international transfers or remittances, especially to jurisdictions or recipients not previously used by the customer; and
- certain payments to accounts held by non-regulated entities, particularly where not owned by the account holder.

This obligation ensures that regulated banks have systems and processes in place to monitor and identify such high-risk activities.

A regulated entity must implement, monitor and regularly review these systems and processes to ensure they remain fit for purpose (see section 6-2).

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 3-5: Targeted warnings and alerts

If an SPF consumer of a regulated bank uses, or attempts to use, the bank's regulated service to undertake a transaction or activity of a kind identified using the systems and processes required under section 3-4, the bank must provide a warning to the SPF consumer about the risks of making the transaction or undertaking the activity. The warning must:

- be relevant to the risk faced by the SPF consumer; and
- be clear, concise and timely; and
- include information about actions the SPF consumer can take to limit their risk of being targeted by a scam relating to a transaction or activity of that kind.

This is intended to make sure that warnings and alerts are proportionate to the scam risk associated with the relevant activity or transaction so that consumers understand the relevant risk and know how to take actions to protect themselves. The requirement that warnings and alerts be relevant to the risk, clear, concise and timely guards against "warning fatigue", which occurs where consumers ignore warnings if they are overused.

This obligation ensures that a regulated bank provides warnings to customers and other SPF consumers about the risk of scams when entering into a transaction or activity identified using the systems and processes required under section 3-4. This is distinct from the general obligations to notify in response to specific actionable scam intelligence (as would be covered under Disrupt). This influences the behaviour of SPF consumers when they are exposed to a scam risk by enabling them to pause and consider the risk even when banks do not have actionable scam intelligence about a specific scam threat (noting additional restrictions or warnings to be put in place to deal with that situation).

The kinds of warnings contemplated by this obligation may include:

- specific warnings on the bank's website; and
- pamphlets in a specific branch on particular scams that may be occurring in a local community.

Regulated banks should choose the most appropriate communication channel to issue the warnings, considering the relevant scam risk and class of persons (or person) being warned. Depending on the risk, which may change over time, a customer could be warned or alerted via an in-app notification, SMS, phone call, on their website account or any other type of suitable and trusted communication.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Example

ABC Bank identifies increasing transaction limits as an activity that has a high-risk of being a scam, as it is a common precursor for many scam types. As such, ABC Bank provides an automated alert to all customers that are seeking to increase their transaction limit. The alert informs the customer where they can find additional information and instructs the customer to contact the bank through trusted channels if they have not requested to increase their transfer limit, or if they are increasing their transfer limit to make a payment to a person they met online.

Section 3-6: Identifying scam transactions

If an SPF consumer of a regulated bank uses, or attempts to use, the bank's regulated service to make a transaction of a kind identified using the bank's systems and processes required under section 3-4, the bank must, before the transaction is made, take proportionate action to enable the bank to identify whether the transaction is, or is facilitating, a scam.

Factors that the regulated entity may have regard to when determining what steps are proportionate may include:

- the size and nature of the transaction and/or scam risk,
- as appropriate, technology and or processes utilised to verify and assess the payments; and
- level of risk identified.

For example, where a payment is small, it may be an appropriate proportionate action to ask the payer to confirm their intention to complete the transfer. Where the amount is larger, it might entail holding the payment until proportionate checks can be completed by the bank, such as contacting the SPF consumer through a separate channel, or undertaking multi-factor authentication.

This obligation requires the regulated entity to undertake the verification steps prior to the payment being processed so that if the entity identifies that the payment is, or is related to, a scam, they are able to disrupt it.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 3-7: Limiting high-risk transactions and activity

If a regulated bank identifies a kind of transaction or activity using the systems and processes required under section 3-4, the regulated bank must take action to limit SPF consumers of the bank's regulated service from making transactions, or undertaking activity, of that kind using the regulated service after the transaction has been identified.

The action taken by the regulated bank must be proportionate to the risk that the transaction or activity is, or is facilitating, a scam.

Factors relevant to whether the activity is proportionate may include:

- the size and nature of the transaction or activity;
- the effect that the regulated bank's actions will have on the consumer;
- previous preventative or disruptive action taken (e.g. warnings previously given);
- systems and processes that are available to the regulated bank; and
- the level of risk identified for the transaction or activity.

Some examples of proportionate steps a regulated entity may take under this obligation include:

- adding payment delays;
- additional confirmation steps, such as a one-time code;
- asking the customer for information about why they are making the payment;
- blocking transfers;
- warning customers about the risks of the transfers;
- capping monthly transfers, and
- delaying or manually reviewing transactions through high-risk payment channels.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Division 3—Banking SPF code provisions for SPF Principle 3: Detect

Obligations specified in Division 3 of Part 3 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Detect for the banking sector.

Section 3-8: Transaction monitoring

A regulated bank must monitor transactions made using its regulated service to identify actionable scam intelligence.

Banks have a significant role in detecting scams, as scams often result in bank customers making payments to scammers from their accounts.

This obligation requires regulated banks to take active steps to identify actionable scam intelligence, rather than passively receiving such intelligence through other sources such as

consumer reports. It ensures that banks are adequately monitoring for transaction-related indicators of scam activity.

This obligation covers any transaction occurring in the course of the provision of the covered banking service. This means that a bank must monitor transactions that involve customers making a payment or receiving a payment. This includes payments made to and from other entities and intra-bank transactions.

Under subsection (2), regulated banks must monitor transactions for the following:

- unusual transactions made using a bank account held with the bank, including transactions that are inconsistent with previous transactions made using the account; and
- attempts to make a transaction of a kind identified using the systems and processes required under section 3-4.

Banks may also look for other indicators of actionable scam intelligence.

The kind of transactions that may indicate scam activity include:

- complex, or unusually large transactions,
- unusual patterns of transactions,
- transactions to or from suspicious accounts, and
- transactions which have no apparent economic or visible lawful purpose.

The regulated bank would have actionable scam intelligence when such information about transaction activities, potentially in conjunction with other information such as account activity (see section 3-9), gives the regulated bank reasonable grounds to suspect the activity is a scam. The regulated bank would then be required to commence an investigation of the activity and take reasonable steps to disrupt the activity or prevent loss or harm arising from the activity.

The monitoring process should adapt to different customers and associated scam factors. For example, a $1,000 payment may not indicate a scam for a customer that regular makes high value transactions, but may be suspicious from a customer that does not.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 3-9 Account monitoring

A regulated bank must monitor activity (other than transactions: see section 3-8) relating to bank accounts held with the bank to identify actionable scam intelligence.

Scammers often manipulate victims to change settings in their account to make payments, either as a one off or over time, leading to a series of actions (e.g., changing contact details, increasing transfer limits) before the actual fraudulent transaction occurs. Furthermore, not all scams involve the consumer making the payment themselves. Successful phishing

scams and remote access scams result in scammers gaining access and control to the victims account, which can then enable them to transfer money out to the scammer's account.

The kind of account-related activities that might indicate an account holder is being engaged in scam activity include:

- changes to daily transfer limits or enabling new payment features (e.g. international transfers);
- adding new payees not previously seen in the customer's history;
- a customer ignoring scam warnings and overriding prompts designed to slow down risky payments;
- unusual login times or locations;
- a customer contacting the bank to ask how to bypass security features (for example increasing daily limits);
- an increased interaction with the bank's banking app or website, especially in areas like settings, limits or payee management; and
- resetting passwords.

The type of activities covered by this obligation will overlap with the high-risk activities identified in section 3-4.

Further, the kinds of account-related activities that may indicate a scammer has taken control of an account, include:

- a login from an unfamiliar device or location, especially if the location differs from the usual location and the customer has not confirmed or approved the login;
- changes to contact details (emails, phone numbers) without other context;
- disabling security features;
- unusual navigation behaviour, like accessing settings or security pages without making changes;
- attempts to add or verify new devices or browsers, especially from a different location;
- failed login attempts followed by a successful login in a way that suggests brute force or credential stuffing; and
- requests for password resets or recovery options that don't match the customer's usual behaviour.

The regulated bank would have actionable scam intelligence when such information about account activities, potentially in conjunction with other information about the activity, give

the regulated bank reasonable grounds to suspect the activity is a scam. The regulated bank would then be required to investigate of the activity, take reasonable steps to disrupt the activity or prevent loss or harm arising from the activity, and comply with other obligations under the SPF.

However, indicators depending on the circumstances, such as nature of the account and the SPF consumer. For example, regular access to an account from different locations may be normal for a customer who is regularly overseas, but unusual for another. A regulated bank should develop systems and processes that enable them to assess these circumstances. Indicators of scam activity will also ultimately evolve as scammers adapt their tactics to commit scams.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 3-10: Identifying SPF consumers and services affected by scams

A regulated bank must have reasonable systems and processes to do the following in relation to an activity about which the bank has actionable scam intelligence, as soon as practicable after the intelligence becomes actionable scam intelligence for the bank:

- identify transactions and communications made using the bank's regulated service relating to the activity;
- identify each bank account held with the bank that is involved in the activity and client identifiers (for example, account names and details, contact information, email postal address, client number) associated with each account; and
- contact each direct SPF consumer affected by the activity to verify the direct SPF consumer's identity and also any transactions made by the direct SPF consumer using the bank's regulated service.

This obligation is intended to ensure that, once a regulated bank has actionable scam intelligence, it can identify SPF consumers that may have been impacted by the scam to help limit the impact of the scam.

Identifying relevant transactions, communications and accounts enables the bank to understand the scope of the scam and help identify the kinds of consumers impacted. Identifying relevant client identifiers enables the bank to determine which consumers may be affected so the bank can take steps to protect the consumers, including by notifying these consumers as appropriate.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Division 4—Banking SPF code provisions for SPF Principle 5: Disrupt

Obligations specified in Division 4 of Part 3 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Disrupt for the banking sector.

Section 3-11: Payment recall requests

Where a regulated bank reasonably believes that a transaction made using the sending bank's regulated service is, or is facilitating a scam, the bank must:

- if the transaction is made to an entity other than the sending bank, as soon as reasonably practicable after the transaction is made, request that the entity assist the sending bank to reverse the effect of the transaction; or

- if the transaction is made to a bank account held with the sending bank, take reasonable steps to reverse the effect of the transaction as soon as reasonably practicable.

If a regulated bank receives a request of the kind required by this obligation, that regulated bank must take reasonable steps to assist the sending bank to reverse the effect of the transaction.

Where a regulated bank reasonably believes that a payment made from one account held with the bank to another account held with the same bank, and made using the bank's regulated service, is a scam, the bank must take reasonable steps to return the funds to the first account as soon as practicable.

This obligation will only apply where the bank reasonably believes that the payment is part of, or the result of, scam. In general, this will follow an investigation of the actionable scam intelligence, noting the investigation may occur swiftly given the importance of requests being sent in a timely manner to avoid SPF consumer harm or loss. This is to prevent legitimate payments being recalled, which may cause harm or inconvenience to SPF consumers.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 3-12: Blocking accounts associated with scams

If a regulated bank reasonably believes that a bank account is being used to facilitate a scam, the bank must stop the scam by taking one of the following actions, proportionate to the risk of loss or harm arising from the scam by:

- closing the account;

- freezing the account; or

- imposing other account restrictions.

If the account holder is an SPF consumer who is not carrying on the scam activity and has lost access or control of the account as a result of scam activity, the bank must also take reasonable steps to restore the consumer's access or control, if possible. In doing so, it may be appropriate for the entity to undertake additional identity verification.

Whether a regulated entity closes, freezes or places other restrictions on accounts will depend on the circumstances and level of risk involved. In determining what action is proportionate, subsection (2) requires that regard must be had to:

- the potential loss or damage to SPF consumers if no action is taken; and
- the potential loss or damage to SPF consumers if the action is taken and the activity is not a scam.

For example, a regulated entity would assess whether any recurring bills or legitimate payments may be disrupted and take action to reduce the risk of such disruption.

This provision is similar to subsection 58BZA(3) of the Act.

This obligation only applies where the entity believes on reasonable grounds that an account is being used to facilitate a scam. This means the obligation applies to the accounts of those committing scams as well as third party accounts being used as "mule accounts". These are accounts held by a third party (other than the scammer or the victim) who either knowingly or unknowingly facilitates a scam by transferring money on instruction from a scammer, or by the scammer themselves through control of the account. A scammer may have gained control of a third-party account through buying or renting the account from the third party, or through fraudulently gaining access to the third party's account information (such as via a phishing link) and then locking out the third-party.

Where it is not possible for the regulated entity to reinstate the account, it would be open to entities to explore other avenues such as creating a new account for the legitimate holder. However, the obligation in section 3-12 is to return the SPF consumer's control of, and access to, the account being used to facilitate a scam, if possible, and as soon as is possible.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Example

ABC Bank has identified payments to new overseas accounts as representing high risk of being or facilitating scams (see section 3-4).

Sophie is a customer of ABC Bank, and seeks to initiate a large overseas payment to Henry. Henry is a new payee in her mobile banking app. Before processing the payment, ABC Bank provides a warning to Sophie in her app that scammers often ask scam victims to make payments to new accounts overseas (see section 3-5). This warning includes a short questionnaire to confirm she has met Henry and to clarify the reason for the transfer (section 3-6). Sophie informs ABC Bank that she has only met Henry online.

As Sophie has not met Henry in person, and given the size of the transaction, ABC Bank has reasonable grounds to suspect the payment might be a scam. ABC Bank therefore has actionable scam intelligence.

ABC Bank undertakes a risk assessment of the suspected scam and puts an interim block on the payment, which it considers to be proportionate to the risk (see section 2-15 of the SPF code and section 58BX of the Act). In the meantime, ABC Bank immediately contacts

Sophie directly to investigate and identify whether the payment is or is facilitating a scam (section 2-10).

Sophie provides additional information to the ABC Bank, which enables the Bank to identify the activity to be a scam (section 2-10).

ABC Bank subsequently blocks all future payments to the overseas bank account to disrupt the scam, which was informed by its risk assessment (see section 2-15 of the SPF code and section 58BX of the Act).

ABC Bank investigates the activity further to identify other impacted SPF consumers and discovers another customer, Will, has made a series of small payments to the same account (see section 2-12 and section 3-10 of the Code).

ABC Bank contacts Will to inform him that he may have been impacted by a scam and explains it appears he made payments to a scam account (see section 2-14 and section 3-10 of the SPF code). This helps protect Will from further harm.

Part 4—Provisions applying to telecommunications sector

[*Part 4 will contain provisions applying to the SPF code for the telecommunications sector. For the purposes of exposure draft consultation, a placeholder for Part 4 has been included in the Instrument. For the substance of specified expected conduct for all regulated telecommunications services, refer to the separate Competition and Consumer Amendment (Scams Prevention Framework–Telecommunications Code) Instrument 2026*.]

Part 5—Provisions applying to digital platforms sector

Part 5 contains provisions applying to the SPF code for the digital platforms sector. These provisions are intended to specify expected conduct for all regulated digital platforms. Digital platforms present particular scam risks for consumers, as seen in increased digital platform account hacking and impersonation, false advertisements and phishing attempts by scammers. The obligations in this Part are tailored to these specific risks and features of digital platforms.

Part 5 contains 4 divisions:

- Division 1, which concerns preliminary matters
- Division 2, which outlines provisions applying to the digital platforms sector for Principle 2: Prevent
- Division 3, which outlines provisions applying to the digital platforms sector for Principle 3: Detect
- Division 4, which outlines provisions applying to the digital platforms sector for Principle 5: Disrupt

Division 1—Preliminary

Section 5-1: Purpose of this Part

This section provides that Part 5 of the Instrument sets out the obligations that apply to regulated digital platforms in relation to the themes or matters covered in the Subdivisions concerning the SPF principles of Governance, Prevent, Detect, Disrupt and Respond, as well as incidental and related matters to those SPF principles.

Division 2—SPF Principle 2: Prevent

Obligations specified in Division 2 of Part 5 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Prevent for the digital platforms sector.

Section 5-2: Terms of Service

This section sets out what a digital platform's terms of service must include. Terms of service define the legal relationship between the platform and users, and govern the platform's content moderation and enforcement action in relation to use of a regulated service.

The information that a regulated digital platform must state in its terms of service (and any standards, guidelines or policies, that apply to users or classes of users) includes, but is not limited to:

- a term to the effect that using the service, including by posting, advertising or sending messages, to commit or attempt to commit a scam within the meaning of the SPF provisions is prohibited;
- a summary of the digital platform's responsibilities under the SPF;
- a term to the effect that the digital platform will take action to ban users and disable digital platform accounts and content it reasonably suspects is a scam, including during and following an investigation.

The information must be in writing, expressed in plain-language and be easy to locate.

If the essential information required to be included in the terms of service is altered, the digital platform must provide SPF consumers of its regulated service with an updated terms of service (and updated standards, guidelines or policies that apply to the user or classes of users, if applicable) by way of:

- the digital platform's regulated service (for example, through a notification on the platform's social media service); and
- contacting the user (if the digital platform has the consumer's contact details) (for example, by email).

The digital platform must notify the consumer by way of a reasonable method using the available contact details that an updated terms of service (and updated standards,

guidelines or policies that apply to the user or classes of users, if applicable) is available on the regulated service.

Currently, references to prohibiting scams and taking action against scam activities in digital platforms' terms of service are inconsistent, sparse or absent. This obligation ensures terms of service cover such matters. The terms of service must not defer responsibility for compliance with the SPF codes to consumers by imposing any additional liabilities or responsibilities on consumers.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 5-3: User verification

This section provides that for each new user of a digital platform's regulated service, the digital platform must take reasonable steps to verify all of the following:

- the identity of the new user;
- that the new user has not previously been banned from using the digital platform's regulated service. When doing so, the digital platform must compare the details of the new user against details of digital platform accounts that have been banned and identifiers of digital platform accounts that have been banned; and
- if the new user is establishing a digital platform account on behalf of a business, that the new user is an authorised representative of the business.

A regulated digital platform must not activate a digital platform account for a new user if the platform is not satisfied on reasonable grounds that the new user meets the verification requirements set out above. Whether there are reasonable grounds for such a belief is an objective test.

This obligation is not intended to require digital platforms to collect additional personal information (such as ID documents or biometric data) if it is not part of the digital platform's standard operating procedure or otherwise required by another law. It is expected that regulated entities would compare, rather than simply match, details of new users against the details of banned digital platform accounts. This is because, for example, matching a name associated with a banned digital platform account may result in false positives.

In verifying whether or not a new user is an authorised representative of the business, it is expected that the digital platform would verify and/or collect contact details, ABNs and other identification documents, and review sources such as ASIC's company and business name registers, if applicable. Australian business accounts refer to professional or business account types that exist for the purpose of conducting commercial activities. The Government is seeking feedback on the final design of this obligation, in particular around what specific action is appropriate for verification.

A regulated digital platform must treat user verification as an ongoing obligation and must re-verify if the platform becomes aware that the information used for verification purposes

is not or may no longer be accurate. This is intended to address potential instances of digital platform account takeover.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 5-4: Advertiser additional verification

A regulated digital platform must verify certain information about an advertiser on the digital platform's regulated service, before an advertisement from the advertiser is published or otherwise displayed to SPF consumers:

- That the advertiser has not previously been banned from using the digital platform's regulated service;
- If a person is engaging with the digital platform on behalf of the advertiser – that the person is an authorised representative of the advertiser. The regulated digital platform is also explicitly required to check the information provided by the person against:
  - ASIC's registers in relation to organisation and business information,
  - the Australian Business Register in relation to ABN data,
  - registered trademarks.
  - other information the digital platform considers appropriate, which may include, for example:
    - registered domain name (such as in whois.auda.org.au),
    - international equivalents that are substantially similar to the above for overseas-based entities, and
    - any other information that might assist verification (such as checking the email domain of the representative).
- If the advertisement involves a product or service that requires the advertiser to hold a licence in Australia to sell the product or provide the service – that such a licence is held (such as an Australian Financial Services Licence; Australian Credit Licence and Australian Deposit-taking Institution (ADI) Licence). This obligation is limited to checking that the advertiser holds a relevant licence and is not intended to require regulated digital platforms to undertake a general assessment of compliance with that licence. As part of verifying that a requisite licence is held, regulated digital platforms may consider whether the key attributes of the licence are broadly consistent with the product or service being advertised. This includes, for example, identifying apparent inconsistencies that would reasonably indicate a heightened risk of scam activity (such as reliance on a wholesale-only license for services directed to retail consumers). Responsibility for supervising compliance with licence conditions remains with the relevant regulator outside the SPF. For the avoidance of doubt, this requirement applies where an advertisement represents, or purports to represent, that

a product or service is being offered, including where the purported product or service does not in fact exist (e.g., scam advertisements). In such cases, the regulated digital platform must verify that the advertiser holds any licence that would be required if the represented product or service were genuine.

- If the advertiser is or purports to be a charity – that the advertiser is included on the Australian Charities and Not-for-profits Register as a registered charity. This recognises that registered charities have different reporting requirements, by placing less onerous requirements on this sector in the event regulated entities seek this information directly from the registered charities.

A regulated digital platform must treat user verification as an ongoing obligation and must re-verify if the platform becomes aware that the information used for verification purposes is not or may no longer be accurate.

The Government is seeking feedback on the final design of this obligation, in particular around what specific action for verification is appropriate.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 5-5: Check advertisements

This section provides that a regulated digital platform must have reasonable systems and processes to review an advertisement for potential scam activity before the advertisement is published or otherwise displayed to SPF consumers of the digital platform's regulated service. A regulated digital platform must implement, monitor and regularly review these systems and processes (see section 6-2).

These systems and processes must:

- verify the identity of the advertiser and authorised representative of the advertiser (as required by section 5-4); and

- check the advertisement for any potential scams (including by checking whether the advertiser has or has previously had any other advertisements that may be or may have been identified as a scam or related to a scam).

This requirement is intended to operate alongside section 5-8. Regulated entities will be required to check advertisements before they are displayed and engage in ongoing monitoring of the advertisements. For example, this may require entities to conduct checks related to content, description, keywords, headings, and any images or videos, if applicable. Where a regulated entity identifies concerns with an advertisement (such as the advertisement contains potential scams), it is expected that the advertisement would not be published until the required conditions are met.

The Government is seeking feedback on the final design of this obligation, in particular around what specific action for verification is appropriate.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 5-6: Targeted warnings

A regulated digital platform must take reasonable steps to warn SPF consumers who are likely to be at a higher risk of being targeted by a particular type of scam activity relative to other members of the public, about the risk of engaging with that type of activity. This supplements section 2-14, which requires a regulated entity to notify SPF consumers that are, or may be, affected by the activity.

The warning must meet all of the following:

- be clear, concise and timely
- be provided through the digital platform's regulated service (for example, as a warning shown on a regulated social media platform's service)
- include information about educational resources relevant to that type of scam;
- include information about how to report scams through the digital platform's reporting mechanism.

When determining whether an SPF consumer is likely to be at a higher risk of being targeted by scams for the purpose of warning that consumer, a regulated digital platform must have regard to user behaviour and content attributes. Depending on the nature of the regulated platform and the scam risks facing its users, examples of circumstances that could put a user at higher risk of a suspected scam activity include:

- interacting or engaging with advertising, content, messages or digital platform accounts that have been identified as perpetrating scams,
- suspicion that receiving contact from digital platform accounts of individuals that the platform has identified as presenting risk of scam activity, such as accounts that have made large numbers of direct contact requests,
- receiving requests to exchange financial information, particularly from new or unknown digital platform accounts,
- receiving 'phishing attempts' e.g. through messages or content detected to contain inauthentic or 'cloaked' URLs or links to unsecure payment services,
- receiving request to share their screen with other users, and
- receiving direct contact from a recently created and/or unknown digital platform accounts (i.e. an account that is not in the user's friend or contact list).

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Division 3—SPF Principle 3: Detect

Obligations specified in Division 3 of Part 5 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Detect for the digital platforms sector.

Section 5-7: Suspicious behaviour, content and messages

This section provides that a regulated digital platform must have reasonable systems and processes to monitor the regulated service for activity that is or may be a scam. This includes:

- monitoring and analysing reports of suspicious user behaviour, content and messages; and
- monitoring suspicious user behaviour, content and messages.

In considering what is reasonable systems and processes for monitoring, regard must be had to the following factors:

- the risk that a scam relating to, connected with, or using a regulated service of the digital platform may be committed considering:
  - the type and scale of regulated services provided by the digital platform; and
  - scams relating to, connected with, or using the regulated service that have previously been committed;
- the types of SPF consumers who use or are likely to use a regulated service of the digital platform;
- how the digital platform's regulated services are provided;
- the current and emerging threat of scams occurring in the regulated sector;
- whether the amount invested by the digital platform to comply with its obligation under subsection (1) is commensurate with the type and scale of regulated services provided by the digital platform;
- the appropriateness of using contemporary technologies to counter scam threats;
- the magnitude of potential loss or harm to SPF consumers if scam activity occurs.

However, if the service is a designated instant messaging service, the systems and processes for monitoring are not required to decrypt encrypted messages. Encrypted messaging services should still be monitored for scams through available information, such as metadata, device information and any information that is voluntarily shared by users.

Digital platforms have a significant role in detecting scams, as scams often involve scammers communicating with victims using their services.

This obligation requires regulated digital platforms to take active steps to identify actionable scam intelligence, rather than passively receiving such intelligence through other sources such as consumer reports. It ensures that regulated digital platforms are adequately monitoring for indicators of scam activity.

The kinds of behaviour, content or messaging activities that might indicate scam activity include (but are not limited to):

- A user contacting large numbers of users that are unknown to them or otherwise unconnected
- A user that creates a vast number of posts, messages or friend requests soon after digital platform account creation
- A user that 'bulk sends' identical messages to other users
- Unusual login patterns (such as multiple logins from different geolocations in a short period of time), new or suspicious devices accessing the digital platform account, or use of VPNs or anonymising tools
- Digital platform accounts that duplicate profile pictures or usernames of other accounts and accounts with fake verification badges
- Inauthentic or 'cloaked URLs' (URLs that hide the real destination of a link by redirecting users to a different webpage)
- Requests to obtain or exchange financial information
- Attempts to gain remote access to other users' screens (i.e. to get a user to share their screen with someone else)
- Language associated with extortion attempts or threats.

The regulated digital platform would have actionable scam intelligence when such information about behaviour, content or messaging activities, potentially in conjunction with other information about the activity, give the regulated digital platform reasonable grounds to suspect the activity is a scam. The regulated digital platform would then be required to commence an investigation of the activity and take reasonable steps to disrupt the activity or prevent loss or harm arising from the activity.

When a regulated digital platform provides multiple regulated services that users can access under one digital platform account, it is intended that such a digital platform must have collective processes for detection and investigation that apply across their multiple services. For example, if suspicious activity is flagged in a user's social media post, the entity's processes may require an investigation of that user's instant messaging activity for the purposes of determining whether the activity is or may be a scam. It is also expected that information owned by a regulated service should be treated as being known across its multiple services. It is anticipated this could result in better scam prevention and disruption, as more scams may be detected across services. It may also lead to account-level action being taken (for example, an entity may then ban or suspend the digital platform account across the full suite of regulated services provided by the entity). This

can also have inadvertent beneficial outcomes for services provided by the entity that are not designated as regulated services.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 5-8: Monitor and assess advertisements

A regulated digital platform must have reasonable systems and processes to monitor and assess advertisements published or otherwise displayed to SPF consumers. A regulated digital platform must implement, monitor and regularly review these systems and processes (see section 6-2).

Without limiting what may be considered reasonable systems and processes for this obligation, these systems and processes must:

- monitor and assess reports made using the digital platform's reporting mechanism about advertising that is or may be a scam
- re-verify the identity and authority of the advertiser if any of the details have been changed; and
- monitor activity on its regulated service (including advertisements) for suspicious content.

Advertisements are intended to encompass any form of advertisement within the ordinary meaning of that term and limited to paid advertising (or where there has been consideration). It is intended to cover advertisements such as:

- paid advertisements on a search engine page
- advertising on social media services that is clearly demarcated as being advertising
- 'boosted' or paid posts on social media services, and
- all advertisements appearing in messaging applications.

Scanning for suspicious content is intended to include actionable scam intelligence, as defined in section 58AI of the Act. It could include:

- Checking keywords and content known to be associated with scams based on previous scam activity; including efforts to avoid keyword detection (such as using different hexadecimal characters that look similar to standard English characters)
- 'cloaked URLs' that redirect users to web pages other than the page the URL suggests; where technically feasible, this should include monitoring embedded URLs' end-location after publication of an advertisement
- identifying fake celebrity endorsements, including scanning for 'deepfake' or 'AI-generated' imagery, and cross-checking named public figures against user reports about advertising involving these figures (particularly where there is a history of certain public figures being used in impersonation scams).

This obligation is intended to operate in addition to the broader scams detection program requirements in section 5-7, and in combination with the advertiser verification requirements in section 5-4, in order to provide a higher level of monitoring in relation to advertising given the higher concentration of scams in this context.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Division 4—Digital platforms sector provisions applying to SPF codes for Principle 5: Disrupt

Obligations specified in Division 4 of Part 5 are relevant SPF code obligations for the purpose of section 58BB of the Act for the corresponding SPF Principle Disrupt for the digital platforms sector.

Section 5-9: Disruptive action during investigation

When a regulated digital platform has actionable scam intelligence about an activity it must:

- take reasonable steps to include a warning with all content and messages relating to the activity indicating that the digital platform is investigating whether or not the activity is a scam.

- suppress, reduce or otherwise limit the activity from being displayed to its SPF consumers on the digital platform while the digital platform investigates whether or not the activity is a scam.

Steps an entity may take to comply with the obligation could include:

- suppressing the reach or visibility of content that the entity has actionable scam intelligence about; and

- limiting users' ability to share or engage with the content that the entity has actionable scam intelligence about.

The kind of activity this obligation is intended to apply to includes content, messages and other material on regulated digital platform services. Section 5-11, explained below, imposes a similar obligation that relates to disruptive actions for advertisements on regulated digital platforms.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 5-10: Removal of content following investigation

A regulated digital platform must, as soon as practicable after the digital platform has identified that an activity is a scam:

- remove content relating to the scam; and

- block other content originating from the same or a related person that is committing the scam; and
- block content that is the same or substantially similar to the scam; and
- disable digital platform accounts associated with the person (or an associate of the person) who is committing the scam.

This obligation only applies where the entity has identified that the activity is a scam which, under subsection 2-10(2), is so identified if the digital platform has reasonable grounds to believe that the activity is a scam.

The kind of activity this could apply to includes content, messages and other material on regulated digital platform services. Section 5-11, explained below, imposes a similar obligation that relates to removal of content for advertisements on regulated digital platforms

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Section 5-11: Limiting scam advertising

A regulated digital platform must have reasonable systems and processes to prevent advertisements promoting a scam from being published or otherwise displayed on its regulated service. A regulated digital platform must implement, monitor and regularly review these systems and processes (see section 6-2).

Without limiting the general obligation, where an advertisement is suspected to be, but not yet identified as, a scam, these systems and processes must include that the regulated digital platform must:

- suspend the display of the advertisement to SPF consumers in Australia until the conclusion of the investigation into the advertisement; and
- suspend a digital platform account suspected of facilitating the advertisement where the account has previously been found to have facilitated scam activity.

Without limiting the general obligation, where an advertisement is identified as a scam, these systems and processes must include that the regulated digital platform must:

- remove the advertisement from being displayed to SPF consumers; and
- block other advertisements containing content that is the same or substantially similar to the scam; and
- ban persons and disable digital platform accounts associated with the person (or an associate of the person) who is committing the scam.

In relation to the action of disabling a digital platform account or banning a person for a single scam or multiple scams, this would be highly dependent on the nature and

seriousness of the scam event. Regulated digital platforms would assess this on a case-by-case basis depending on the exact facts and circumstances at hand.

Under section 6-1, this section is a civil penalty provision. Failure to comply with this obligation may attract a civil penalty. Civil penalty provisions in SPF codes are tier 2 civil penalties – see section 58FL of the Act.

Part 6- Miscellaneous

Section 6-1 – Civil penalty provisions

Section 6-1 provides that a provision of this Instrument referred to in an item in the table is a civil penalty provision (within the meaning of the Regulatory Powers Act). The civil penalty provisions are tier 2 contraventions, with the maximum penalty amount set out in section 58FL of the Act. For enforcement of civil penalty provisions and penalties for contravention of a civil penalty provision, see Subdivision C of Division 6 of Part IVF of the Act.

Section 6-2 – Implementing, monitoring and reviewing systems and processes

If a provision of the Instrument requires a regulated entity for a regulated sector to have a system or process, the entity must also:

- implement the system or process; and
- monitor whether the system or process is being followed; and
- regularly review whether the system or process remains fit for purpose.

Including this as a stand-alone obligation minimises drafting complexity and makes it clear that any time there is an obligation to have a system or process, a regulated entity must ensure those systems and processes are implemented, followed and regularly reviewed so that they remain fit for purpose to support the entity's compliance with the SPF and prevention of scams.