EXPOSURE DRAFT

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

I, Daniel Mulino, Assistant Treasurer and Minister for Financial Services, make the following instrument.

Dated 2026

Dr Daniel Mulino **[DRAFT ONLY—NOT FOR SIGNATURE]**
Assistant Treasurer
Minister for Financial Services

Contents

Part 1—Preliminary

1-1 Name

This instrument is the *Competition and Consumer (Scams Prevention Framework—SPF Codes) Instrument 2026*.

1-2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	The later of: (a) 31 March 2027; and (b) the day after this instrument is registered.	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

1-3 Authority

This instrument is made under the *Competition and Consumer Act 2010*.

1-4 Banking sector SPF code

For the purposes of section 58CB of the Act, the SPF code for the regulated sector designated under section 11 of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026* is comprised of the provisions set out in Parts 2, 3 and 6 of this instrument.

1-5 Telecommunications sector SPF code

For the purposes of section 58CB of the Act, the SPF code for the regulated sector designated under section 13 of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026* is comprised of the provisions set out in Part 2 (other than sections 2-15 and 2-16) and Parts 4 and 6 of this instrument.

1-6 Digital platforms sector SPF code

For the purposes of section 58CB of the Act, the SPF code for the regulated sector designated under section 15 of the Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026 is comprised of the provisions set out in Parts 2, 5 and 6 of this instrument.

1-7 Definitions

Note: Expressions have the same meaning in this instrument as in the *Competition and Consumer Act 2010* as in force from time to time—see paragraph 13(1)(b) of the *Legislation Act 2003*.

In this 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 *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026*.

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: a regulated entity for a regulated sector takes ***disruptive action*** if the entity:

(a) has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity; and

(b) 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 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.

regulated bank means a regulated entity for the regulated sector designated under section 11 of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026*.

regulated digital platform means a regulated entity for the regulated sector designated under section 15 of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026*.

regulated telecommunications provider means a regulated entity for the regulated sector designated under section 13 of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026*.

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: a person is an ***SPF staff member*** of a regulated entity if the person:

(a) is one of the following:
  (i) an employee of the regulated entity;
  (ii) a contractor or subcontractor of the regulated entity;
  (iii) an employee of a contractor or subcontractor of the regulated entity; and

(b) carries 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*.

Part 2—Common SPF code provisions

Division 1—Preliminary

2-1 Purpose of this Part

(1) Subject to subsection (2), this Part sets out obligations that apply to a regulated bank, regulated telecommunications provider and a regulated digital platform in relation to:

(a) the themes or matters covered by Subdivisions B, C, D, F and G of Division 2 of Part IVF of the Act; and

(b) related or incidental matters.

(2) Despite subsection (1), the provisions in sections 2-15 and 2-16 do *not* apply to a regulated telecommunications provider.

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

2-2 Requirements for governance policies and procedures

(1) Without limiting the factors to which a regulated entity for a regulated sector must have regard when developing the entity's required policies and procedures, the entity must have regard to:

(a) the risk that a scam relating to, connected with, or using a regulated service of the entity will be committed, considering:

(i) the type and scale of regulated services provided by the entity; and

(ii) the ability of the regulated entity to implement measures that will stop or limit scams; and

(iii) scams relating to, connected with, or using the regulated service that have previously been committed; and

(b) 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

(c) how the entity's regulated services are provided; and

(d) the current and emerging threat of scams occurring in both the regulated sector and the wider Australian economy; and

(e) the effectiveness of the entity's existing policies and procedures (if any) in stopping or limiting scams; and

(f) any major scam event that the entity was affected by within the last 12 months.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Section 58BD of the Act requires regulated entities for a regulated sector to document and implement governance policies and procedures. Section 58BH provides that SPF codes for regulated sectors may give further information about how regulated entities must document governance policies and procedures.

(2) The regulated entity's required policies and procedures must include information about how the entity assessed the risk referred to in paragraph (1)(a).

Note: This subsection is a civil penalty provision (see section 6-1).

2-3 Staff training

A regulated entity's required policies and procedures must:

(a) include reasonable processes for developing and providing training and guidance to the entity's SPF staff members; and

(b) specify how the training will support the entity's SPF staff members to:

(i) identify scams; and

(ii) identify SPF consumers of the entity's regulated service who are likely to be at a higher risk of being targeted by scams than other members of the public; and

(iii) identify and support SPF consumers of the entity's regulated service who have been affected by a scam, including those that have made an SPF report or an SPF complaint; and

(iv) respond in a timely, fair and effective way to SPF reports or SPF complaints; and

(v) identify and support SPF consumers of the entity's regulated service who may require assistance to access the entity's internal dispute resolution mechanism including people with disability or from a culturally and linguistically diverse background; and

(vi) explain to SPF consumers of the entity's regulated service their rights under the entity's internal dispute resolution mechanism and the SPF EDR scheme authorised for the entity's regulated sector; and

(vii) understand the entity's obligations under the SPF provisions and how SPF staff members can support compliance with those obligations; and

(c) provide that the training is to be provided to an SPF staff member of the entity:

(i) within a reasonable time after the SPF staff member begins to be engaged by the entity; and

(ii) at least once every 12 months during the period the SPF staff member is engaged by the entity.

Note: This section is a civil penalty provision (see section 6-1).

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

2-4 Reasonable systems, processes and resources

A regulated entity for a regulated sector must have reasonable systems, processes and resources (including financial, technological and human resources) to ensure compliance with:

(a) the provisions in Subdivision C of Division 2 of Part IVF of the Act; and

(b) 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 Subdivision.

Note 1: This section is a civil penalty provision (see section 6-1).

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

2-5 Maintain secure systems

(1) A regulated entity for a regulated sector must have reasonable and secure systems to protect its 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.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

(2) Without limiting subsection (1), the regulated entity must:

(a) undertake regular assessments of its systems to detect potential security vulnerabilities; and

(b) undertake ongoing testing, patching and updating of the software used in its systems.

2-6 Supervise third party service providers

(1) A regulated entity for a regulated sector must have reasonable systems and processes to ensure that its agents, and any other entities (***third-party service providers***) that under an arrangement with the regulated entity are authorised to deliver, facilitate or support a regulated service of the regulated entity, or any part of that service, have reasonable systems, processes and resources (including financial, technological and human resources) to ensure that the agents and third-party service providers act consistently with:

(a) the provisions in Subdivision C of Division 2 of Part IVF of the Act; and

(b) 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 Subdivision.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

(2) Without limiting subsection (1), the entity's systems and processes must include that the regulated entity must:

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

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

(c) 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.

2-7 Brand impersonation

(1) A regulated entity for a regulated sector must have reasonable systems and processes to prevent its brand, brand assets or likeness from being used to facilitate scams (***brand impersonation***).

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

(2) Without limiting subsection (1), the entity's systems and processes must include that the regulated entity must:

(a) inform SPF consumers of the entity's regulated service about the regulated entity's official communication channels for customer engagement; and

(b) protect the communication channels for customer engagement from brand impersonation; and

(c) monitor the internet for brand impersonation; and

(d) for websites containing brand impersonation material—promptly send a request to the publisher of the website to remove the material.

(3) In determining what is reasonable for the purposes of subsection (1), regard must be had to the following factors:

(a) the risk that a scam relating to, connected with, or using a regulated service of the entity will be committed considering:

(i) the type and scale of regulated services provided by the entity; and

(ii) scams relating to, connected with, or using the regulated service that have previously been committed;

(b) the types of SPF consumers who use or are likely to use a regulated service of the entity;

(c) how the entity's regulated services are provided;

(d) the current and emerging threat of scams occurring in the regulated sector;

(e) whether the amount invested by the entity to comply with its obligation under subsection (1) is commensurate with the type and scale of regulated services provided by the entity;

(f) the appropriateness of using contemporary technologies to counter scam threats;

(g) mechanisms for continuous improvement;

(h) consistency with relevant industry standards and practices;

(i) the magnitude of potential loss or harm to SPF consumers if scam activity occurs.

2-8 Consumer awareness

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

Note: This subsection is a civil penalty provision (see section 6-1).

(2) Without limiting subsection (1), the information must:

(a) include:

(i) common types of scams related to the entity's regulated service; and

(ii) 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

(iii) website links and contact details for other publicly available resources about scams; and

(b) be easy to understand and locate, including for a person with disability or from a culturally and linguistically diverse background; and

(c) be regularly updated to reflect current scam risks and incidents.

Example: The Scamwatch website includes publicly available resources about scams. In 2026, the Scamwatch website could be accessed at scamwatch.gov.au.

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

2-9 Reasonable systems, processes and resources

A regulated entity for a regulated sector must have reasonable systems, processes and resources (including financial, technological and human resources) to ensure compliance with:

(a) the provisions in Subdivision D of Division 2 of Part IVF of the Act; and

(b) 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 Subdivision.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

2-10 Identifying an activity as a scam

(1) A regulated entity who has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity must identify whether or *not* the activity is a scam.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Under subsection 58BN(1) of the Act, a regulated entity for a regulated sector 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 during the 28-day period starting on the day that the intelligence becomes actionable scam intelligence for the entity.

(2) The entity must identify the activity as a scam if the entity has reasonable grounds to believe that the activity is a scam.

(3) Without limiting the factors to which a regulated entity may have regard when considering whether or *not* the activity is a scam for the purposes of subsection (1), the entity must have regard to:

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

(b) characteristics of the activity shared with other scams; and

(c) the number of reports submitted to the entity in relation to the activity; and

(d) the presence of common indicators of consumers at high risk of scam activity; and

(e) any known systemic or widespread scam issues or risks.

2-11 Recording information about investigation

(1) Subject to subsection (3), a regulated entity for a regulated sector 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.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) Without limiting subsection (1), the information recorded must include the following:

(a) whether or *not* the regulated entity identifies the activity as a scam;
(b) information supporting the entity's consideration of the factors mentioned in subsection 2-10(3);
(c) the method used to initiate contact with SPF consumers of the entity's regulated service, such as telephone calls, text messages, emails and social media;
(d) if the entity identifies the activity as a scam:
  (i) the type of scam; and
  (ii) 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.

Note: Identifiers includes those relating to any relevant person involved in the activity.

(3) However, the entity is *not* required to record information if the information can only be obtained from an SPF consumer of the entity's regulated service and the entity has been unable to obtain that information from the SPF consumer.

2-12 Identifying affected SPF consumers

(1) A regulated entity for a regulated sector 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.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

Note 3: Under section 58BO of the Act, regulated entities must take reasonable steps within a reasonable time to identify the persons who were SPF consumers of that service at the time when the persons were or may have been impacted by the activity.

(2) Without limiting subsection (1), the entity's systems and processes must enable the entity to do the following as soon as practicable after the intelligence becomes actionable scam intelligence for the entity:
(a) identify direct SPF consumers of the regulated service;
(b) take reasonable steps to identify SPF consumers who are *not* direct SPF consumers of the regulated service.

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

2-13 Reasonable systems, processes and resources

A regulated entity for a regulated sector must have reasonable systems, processes and resources (including financial, technological and human resources) to ensure compliance with:

(a) the provisions in Subdivision F of Division 2 of Part IVF of the Act; and

(b) a provision of an instrument made under Part IVF of the Act that relates to the matters covered by that Subdivision.

Note 1: This section is a civil penalty provision (see section 6-1).

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

2-14 Notify affected SPF consumers

(1) A regulated entity for a regulated sector 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.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Section 2-12 requires a regulated entity to have reasonable systems and processes to identify SPF consumers that are, or may be, affected by the activity.

(2) A notification under subsection (1) must:

(a) be given as soon as practicable after the intelligence becomes actionable scam intelligence for the entity; and

(b) be relevant and proportionate to the risk of loss or harm arising from the activity; and

(c) if the entity has contact details for the SPF consumer:

(i) be given to the SPF consumer using the most appropriate contact details; and

(ii) explain the reason why the entity suspects the SPF consumer is, or may be, affected by the activity.

2-15 Risk assessment for disruptive actions

(1) A regulated entity for a regulated sector who 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.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Under subsection 58BX(1) of the Act, the entity must 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. Under subsection 58BX(3) of the Act, the steps taken should be proportionate to the actionable scam intelligence that the entity has about the activity.

Note 3: This subsection does *not* prevent the entity from taking disruptive action immediately after receiving or identifying 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.

Note 4: This section does *not* apply in relation to a regulated telecommunications provider (see sections 1-5 and 2-1).

(2) Without limiting subsection (1), the risk assessment must include:

(a) whether the entity suspects or reasonably believes that the activity is a scam; and

(b) the likelihood and severity of potential loss or harm caused by the activity; and

(c) the nature of the activity and the presence of any high-risk indicators of a scam; and

(d) known systemic or widespread scam issues or risks (including information shared by SPF regulators); and

(e) if the activity is suspected, but *not* yet identified, to be a scam:

(i) the strength of the actionable scam intelligence; and

(ii) the potential loss or harm to SPF consumers of the regulated service and persons carrying on the activity if disruptive action is taken and the activity is *not* a scam; and

(iii) 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.

2-16 Reverse disruptive actions if *not* a scam

(1) This section applies to a regulated entity for a regulated sector if:

(a) the entity has taken disruptive action to disrupt an activity that, at the time the entity took the disruptive action, the entity suspected was a scam; and

(b) the entity identifies that the activity is *not* a scam.

(2) The entity must, to the extent reasonably practicable, reverse the disruptive action as soon as practicable after the entity identifies that the activity is *not* a scam.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: 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:

(a) the entity identifies that the activity is *not* a scam; and

(b) it is reasonably practicable to reverse the action.

Note 3: This section does *not* apply in relation to a regulated telecommunications provider (see sections 1-5 and 2-1).

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

2-17 Reasonable systems, processes and resources

A regulated entity for a regulated sector must have reasonable systems, processes and resources (including financial, technological and human resources) to ensure compliance with:

(a) the provisions in Subdivision G of Division 2 of Part IVF of the Act; and

(b) 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 Subdivision.

Note 1: This section is a civil penalty provision (see section 6-1).

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

Subdivision A—Scams reporting mechanisms

2-18 Requirements for reporting mechanisms

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

(a) 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;

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

(c) include multiple options for a person to report an activity that is or may be a scam;

(d) include an option for a person to access assistance from an individual within a reasonable time after the person requests the assistance;

(e) for the option mentioned in paragraph (d)—be easy to understand, locate and use;

(f) be able to receive reports at any time.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Paragraph 58BZH(a) of the Act provides that the SPF code for a regulated sector may include provisions setting out conditions that must be met for a reporting mechanism.

Note 3: Each of the multiple options mentioned in paragraph (c) is *not* required to be available to receive reports at any time for the purposes of paragraph (f).

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

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Under subsection 58BZF(1) of the Act, a regulated entity for a regulated sector must make publicly accessible information about the rights of SPF consumers under that entity's reporting mechanism.

2-19 Acknowledgement of scams report

(1) A regulated entity for a regulated sector who receives a report through its reporting mechanism about an activity that is or may be a scam must acknowledge receipt of the report within 24 hours after the report is received.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) The acknowledgement must:

(a) 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; and

(b) advise the person who made the report (the ***reporting person***) that they may nominate a preferred contact method or contact person and any accessibility requirements; and

(c) if the reporting person has nominated any accessibility requirements—advise that, as far as possible, those requirements will be accommodated; and

(d) 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

(e) be in the form the regulated entity considers to be most suitable, taking into account the way the report was made.

Note 1: Under subsection 58BZF(1) of the Act, a regulated entity for a regulated sector must make certain information about the rights of SPF consumers of its regulated services publicly accessible.

Note 2: The acknowledgement may be in the form of an automated response.

(3) If an acknowledgement is given orally, the regulated entity must also, where the reporting person has nominated an appropriate contact method, also give the reporting person the acknowledgement in writing as soon as practicable.

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.

Note: This section is a civil penalty provision (see section 6-1).

Subdivision B—Internal dispute resolution mechanisms

2-21 Requirements for internal dispute resolution mechanisms

(1) A regulated entity's internal dispute resolution mechanism must meet the following conditions:

(a) 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;

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

(c) 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;

(d) include an option for a person to access assistance from an individual within a reasonable time after the person requests the assistance;

(e) for the option mentioned in paragraph (d)—be easy to understand, locate and use.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Paragraph 58BZH(b) of the Act provides that the SPF code for a regulated sector may include provisions setting out conditions that must be met for an internal dispute resolution mechanism.

(2) A regulated entity for a regulated sector must *not* charge (or cause to be charged) a fee for a person to access information about the entity's internal dispute resolution mechanism.

2-22 Detecting and dealing with issues with internal dispute resolution mechanism

A regulated entity's required policies and procedures must:

(a) set clear accountabilities for the identification of issues with the operation of entity's internal dispute resolution mechanism; and

(b) require, enable and assist the entity's staff to promptly escalate possible issues with the operation of entity's internal dispute resolution mechanism; and

(c) deal with how issues with the operation of entity's internal dispute resolution mechanism will be identified and managed including, but *not* limited to, by requiring the entity to regularly analyse data held by the entity.

Note: This section is a civil penalty provision (see section 6-1).

2-23 Acknowledgement of internal dispute resolution complaint

(1) A regulated entity for a regulated sector who receives a complaint through its internal dispute resolution mechanism about an activity that is or may be a scam or the entity's conduct relating to such activity must acknowledge receipt of the complaint as soon as practicable.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) The acknowledgement must:

(a) 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; and

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

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

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

(e) 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; and

(f) 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

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

Note 1: Under subsection 58BZF(1) of the Act, a regulated entity for a regulated sector must make certain information about the rights of SPF consumers of its regulated services publicly accessible.

Note 2: The acknowledgement may be in the form of an automated response.

(3) If an acknowledgement is given orally, the regulated entity must also, where the complainant has nominated an appropriate contact method for written acknowledgement, give the complainant the acknowledgement in writing as soon as practicable.

Note: This subsection is a civil penalty provision (see section 6-1).

2-24 Timely resolution of complaints

A regulated entity for a regulated sector must have reasonable systems and processes to ensure that complaints received through its internal dispute resolution mechanism about an activity, or the entity's conduct relating to an activity, are dealt with as quickly as possible having regard to the complexity of the complaint and the scale of the activity.

Note 1: This section is a civil penalty provision (see section 6-1).

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

Note 3: A regulated entity need *not* deal with a complaint that is about the same activity, or the same conduct, that is the subject of an earlier complaint by the same complainant.

2-25 Notice if complaint *not* resolved within 30 days

A regulated entity for a regulated sector who receives a complaint through its internal dispute resolution mechanism about an activity that is or may be a scam or the entity's conduct relating to the activity must, if the entity has *not* resolved the complaint within 30 days after the entity received the complaint, provide the complainant with the following information:

(a) the reason why the complaint has *not* been resolved within 30 days;

(b) a summary of the complainant's rights under the SPF EDR scheme authorised for the entity's regulated sector and how the complainant may access the scheme.

Note: This section is a civil penalty provision (see section 6-1).

2-26 Cooperation between regulated entities

(1) A regulated entity (the ***first entity***) for a regulated sector must have reasonable systems and processes to facilitate cooperation with other regulated entities

(including regulated entities for other regulated sectors) in relation to complaints received through any of the entities' internal dispute resolution mechanisms about an activity that:

(a) is or may be a scam; and

(b) relates to, is connected with, or uses a regulated service of the first entity; and

(c) relates to, is connected with, or uses a regulated service of another regulated entity (including regulated entities for other regulated sectors); and

(d) impacts the complainant at a time when the complainant is an SPF consumer of the first entity's regulated service.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

(2) Without limiting subsection (1), the entity's systems and processes must enable the entity to:

(a) respond to requests for information or queries from other regulated entities in relation to the complaint in a reasonable time; and

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

2-27 Vexatious or frivolous complaints

(1) A regulated entity for a regulated sector may decide *not* to deal with, or further deal with, a complaint received through its internal dispute resolution mechanism that the regulated entity reasonably considers to be frivolous or vexatious.

(2) 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.

(3) If a regulated entity decides *not* to deal with, or further deal with, a complaint that is frivolous or vexatious, 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.

Note: This subsection is a civil penalty provision (see section 6-1).

2-28 Recording information about complaints

(1) A regulated entity for a regulated sector must record the following information about each complaint made through its internal dispute resolution mechanism:

(a) details of the complaint, including the date it was made;

(b) a brief description of the type of activity giving rise to the complaint;

(c) the date when the complaint was acknowledged;

(d) the date when the complaint was finalised;

(e) a brief description of the outcome of the complaint.

Examples: Resolved, unresolved, withdrawn, escalated to an SFP EDR scheme.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) Information required to be recorded under subsection (1) must be kept in a way that allows data to be analysed for a particular period.

Examples:

(a) total number of complaints made;
(b) types of scams giving rise to complaints;
(c) average time taken to acknowledge complaints and resolve them;
(d) number of complaints escalated to SPF EDR schemes.

Part 3—Banking SPF code provisions

Division 1—Preliminary

3-1 Purpose of this Part

This Part sets out obligations that apply to a regulated bank in relation to:

(a) the themes or matters covered by Subdivisions B, C, D, F and G of Division 2 of Part IVF of the Act; and

(b) related or incidental matters.

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

3-2 Payee confirmation

(1) 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:

(a) enable the SPF consumer to do whichever of the following applies:

(i) if the SPF consumer provides a name, BSB and account number to the bank—verify whether the name, BSB and account number matches information held by, or provided to, the bank in respect of the BSB and account number;

(ii) 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) (the ***payee identifier***)—view the name associated with the payee identifier if the payee identifier has been registered for use for electronic funds transfer; and

(b) if the BSB and account number do *not* match the information held by or provided to the bank:

(i) notify the SPF consumer of that fact; and

(ii) notify the SPF consumer that they may be the subject of a scam; and

(iii) give the SPF consumer the option *not* to proceed with the transfer.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) A regulated bank must, on request by another regulated bank (the ***second bank***), provide the second bank with information required for the second bank to comply with subsection (1).

Note: This subsection is a civil penalty provision (see section 6-1).

3-3 Identity verification of SPF consumers

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

Note: This subsection is a civil penalty provision (see section 6-1).

[(2) For the purposes of verifying the SPF consumer's identity under subsection (1), the bank must…]

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.

Note 1: This section is a civil penalty provision (see section 6-1).

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

3-5 Targeted warnings

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:

(a) be relevant to the risk faced by the SPF consumer; and

(b) be clear, concise and timely; and

(c) 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.

Note: This section is a civil penalty provision (see section 6-1).

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 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.

Note: This section is a civil penalty provision (see section 6-1).

3-7 Limiting high-risk transactions and activity

(1) If a regulated bank identifies a kind of transaction or activity using the systems and processes required under section 3-4, the 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 or activity has been identified.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) The action must be proportionate to the risk that the transaction or activity is, or is facilitating, a scam.

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

3-8 Transaction monitoring

(1) A regulated bank must monitor transactions made using the bank's regulated service to identify actionable scam intelligence.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) Without limiting subsection (1), the regulated bank must monitor the transactions for:

(a) unusual transactions made using a bank account held with the bank, including transactions that are inconsistent with previous transactions made using the account; and

(b) attempts to make a transaction of a kind identified using the systems and processes required under section 3-4.

3-9 Account monitoring

(1) A regulated bank must monitor activity (other than transactions) relating to bank accounts held with the bank to identify actionable scam intelligence.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) Without limiting subsection (1), the regulated bank must monitor the activity for changes to information associated with a bank account held with the bank, such as contact details, credentials or authentication settings.

3-10 Identifying SPF consumers and services affected by scams

(1) A regulated bank must have reasonable systems and processes to enable the bank 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:

(a) identify transactions and communications made using the bank's regulated service that relate to the activity;

(b) identify each bank account held with the bank that is involved in the activity, and the client identifier associated with the account;

(c) contact each direct SPF consumer of the bank's regulated service that is affected by the activity to verify the direct SPF consumer's identity and any transactions made by the direct SPF consumer using the bank's regulated service.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

[(2) For the purposes of verifying an SPF consumer's identity under paragraph (1)(c), the bank must…]

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

3-11 Payment recall requests

(1) If a regulated bank (the ***sending bank***) reasonably believes that a transaction made using the sending bank's regulated service is, or is facilitating, a scam, the sending bank must:

(a) 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

(b) 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.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) If the sending bank makes a request referred to in paragraph (1)(a) to an entity that is a regulated bank, the entity must take reasonable steps to assist the sending bank to reverse the effect of the transaction.

Note: This subsection is a civil penalty provision (see section 6-1).

3-12 Blocking accounts associated with scams

(1) If a regulated bank reasonably believes that a bank account held with the bank is being used to facilitate a scam, the bank must:

(a) stop the scam by taking one of the following actions, proportionate to the risk of loss or harm arising from the scam:

(i) closing the account;

(ii) freezing the account;

(iii) placing other restrictions the account; and

(b) if the account:

(i) is held by an SPF consumer who is *not* carrying on the scam; and

(ii) because of the scam, the SPF consumer has lost access to, or control of, the account;

return the SPF consumer's control of, and access to, the account, if possible, and as soon as is possible.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) For the purposes of paragraph (1)(a), matters relevant to whether the action is proportionate to the risk include:

(a) the potential loss or damage to SPF consumers if the action is *not* taken; and

(b) the potential loss or damage to SPF consumers if the action is taken and the activity is *not* a scam.

Part 4—Telecommunications SPF code provisions

[Telecommunications SPF Code provisions to be inserted here]

Part 5—Digital platforms SPF code provisions

Division 1—Preliminary

5-1 Purpose of this Part

This Part sets out obligations that apply to a regulated digital platform in relation to:

(a) the themes or matters covered by Subdivisions B, C, D, F and G of Division 2 of Part IVF of the Act; and

(b) related or incidental matters.

Division 2—SPF Principle 2: Prevent

5-2 Terms of service

(1) A regulated digital platform must include the following in its terms of service (and any standards, guidelines or policies that apply to users or classes of users) for a regulated service:

(a) 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;

(b) a summary of the digital platform's responsibilities under the SPF;

(c) a term to the effect that the digital platform will take action, which may include suspending or banning users and disabling digital platform accounts and content it reasonably suspects is a scam, including during and following an investigation.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: The terms of service must specify the matters set out in subsection (1), and may also specify other matters.

(2) The information mentioned in subsection (1) must be in writing, in plain-language, and easy to locate.

(3) If the terms of service (or any standards, guidelines or policies that apply to the user or classes of users, if applicable) mentioned in subsection (1) is altered, the digital platform must:

(a) provide SPF consumers of the digital platform's 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; and

(b) if the digital platform has contact details for the consumer—notify the consumer, by way of a reasonable method using the consumer's 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 digital platform's regulated service.

5-3 User verification

(1) For each new user of a regulated service provided by a regulated digital platform, the digital platform must take reasonable steps to verify:

(a) the identity of the new user; and

(b) that the new user has *not* previously been banned from using the digital platform's regulated service; and

(c) 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.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) When verifying that the new user has *not* previously been banned for the purposes of paragraph (1)(b), the digital platform must compare the details of the new user against:

(a) details of digital platform accounts that have been banned by the digital platform; and
(b) identifiers of digital platform accounts that have been banned by the digital platform.

(3) *[For the purposes of verification under paragraphs (1)(a) and (c), the digital platform must…]*

(4) The regulated digital platform must *not* activate a digital platform account for the new user if the digital platform is *not* satisfied on reasonable grounds that the new user meets the user verification requirements in subsection (1).

Note: This subsection is a civil penalty provision (see section 6-1).

(5) A regulated digital platform must re-verify the information mentioned in subsection (1) if the digital platform becomes aware that the information the digital platform used for verification purposes is *not* or may no longer be accurate.

5-4 Advertiser additional verification

(1) A regulated digital platform must verify the following 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 of the regulated service:
(a) that the advertiser has *not* previously been banned from using the digital platform's regulated service; and
(b) if a person is engaging with the digital platform on behalf of the advertiser—that the person is an authorised representative of the advertiser;
(c) 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 the advertiser holds the requisite licence to sell or provide the product or service in Australia;
(d) if the advertiser is, or purports to be, a registered charity—that the advertiser is included on the Australian Charities and Not-for-profits Register (within the meaning of the *Australian Charities and Not-for-profits Commission Act 2012)* as a registered charity.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) When verifying that a person is an authorised representative of an advertiser for the purposes of paragraph (1)(b), the regulated digital platform must check the information provided by the person against:
[(a) ASIC's Organisation and Business Names register; and
(b) the Australian Business Register
(c) registered trademarks
(d) other information the digital platform considers appropriate.]

(3) *[For the purposes of verification under paragraphs (1)(a), (c) and (d), the digital platform must…]*

(4) A regulated digital platform must re-verify the information mentioned in subsection (1) if the digital platform becomes aware that the information the digital platform used for verification purposes is *not* or may no longer be accurate.

5-5 Check advertisements

(1) 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.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

(2) Without limiting subsection (1), the digital platform's systems and processes must:

(a) verify the information required under subsection 5-4(1) in relation to the advertiser and an authorised representative of the advertiser (if applicable); and

(b) 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).

(3) *[For the purposes of verification under paragraph (2)(a), the system and processes must…]*

5-6 Targeted warnings

(1) A regulated digital platform must take reasonable steps to warn SPF consumers of the entity's regulated service who are likely to be at a high risk of being targeted by a particular type of scam activity, about the risk of engaging with that type of activity.

Note: This subsection is a civil penalty provision (see section 6-1).

(2) The warning must:

(a) be clear, concise and timely; and

(b) be provided through the digital platform's regulated service; and

(c) include information about educational resources relevant to that type of scam; and

(d) include information about how to report scams through the digital platform's reporting mechanism.

(3) When determining whether an SPF consumer is likely to be at a high risk of being targeted by a particular type of scam activity for the purposes of subsection (1), the digital platform must have regard to:

[(a) user behaviour; and

(b) content attributes].

Division 3—SPF Principle 3: Detect

5-7 Suspicious behaviour, content and messages

(1) Subject to subsection (3), a regulated digital platform must have reasonable systems and processes to monitor the digital platform's regulated service for activity that is or may be a scam, including:

(a) monitoring and analysing reports of suspicious user behaviour, content and messages; and

(b) monitoring suspicious user behaviour, content and messages.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

(2) In determining what is reasonable for the purposes of subsection (1), regard must be had to the following factors:

(a) the risk that a scam relating to, connected with, or using a regulated service of the digital platform may be committed considering:

(i) the type and scale of regulated services provided by the digital platform; and

(ii) scams relating to, connected with, or using the regulated service that have previously been committed;

(b) the types of SPF consumers who use or are likely to use a regulated service of the digital platform;

(c) how the digital platform's regulated services are provided;

(d) the current and emerging threat of scams occurring in the regulated sector;

(e) 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;

(f) the appropriateness of using contemporary technologies to counter scam threats;

(g) the magnitude of potential loss or harm to SPF consumers if scam activity occurs.

(3) However, if the regulated service is a designated instant messaging service, the systems and processes mentioned in subsection (1) are *not* required to decrypt encrypted messages.

5-8 Monitor and assess advertisements

(1) A regulated digital platform must have reasonable systems and processes to monitor and assess advertisements published or otherwise displayed to its SPF consumers.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

(2) Without limiting subsection (1), the digital platform's systems and processes must:

(a) monitor and assess reports made using the digital platform's reporting mechanism about advertising that is or may be a scam;

(b) re-verify the identity and authority of the advertiser verified under paragraph 5-5(2)(a) if any of the details have been changed; and

(c) monitor activity on its regulated service for suspicious content.

Division 4—SPF Principle 5: Disrupt

5-9 Disruptive action during investigation

A regulated digital platform who has actionable scam intelligence about an activity must:

(a) 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; and

(b) 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.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Under subsection 58BX(1) of the Act, the entity must 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. Under subsection 58BX(3) of the Act, the steps taken should be proportionate to the actionable scam intelligence that the entity has about the activity.

Note 3: In addition to the disruptive actions required under this section, a regulated digital platform may take other disruptive action informed by a risk assessment of the actionable scam intelligence in accordance with section 2-15.

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:

(a) remove content relating to the scam; and

(b) block other content originating from the same or a related person that is committing the scam; and

(c) block content that is the same or substantially similar to the scam; and

(d) disable digital platform accounts associated with the person (or an associate of the person) who is committing the scam.

Note 1: This subsection is a civil penalty provision (see section 6-1).

Note 2: Under subsection 2-10(2), the digital platform must identify the activity as a scam if the digital platform has reasonable grounds to believe that the activity is a scam.

5-11 Limiting scam advertising

(1) 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.

Note 1: This subsection is a civil penalty provision (see section 6-1).

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

(2) Without limiting subsection (1), the digital platform's systems and processes must include that the digital platform must:

(a) if the digital platform has actionable scam intelligence about an advertisement but has *not* yet identified the advertisement as a scam:

(i) suspend the display of the advertisement to its SPF consumers in Australia until the conclusion of the investigation into the advertisement; and

(ii) suspend a digital platform account suspected of facilitating the advertisement where the account has previously been found to have facilitated scam activity; and

(b) if the digital platform has identified that an advertisement is a scam:

(i) remove the advertisement from being displayed to its SPF consumers; and

(ii) block other advertisements containing content that is the same or substantially similar to the scam; and

(iii) ban persons and disable digital platform accounts associated with the person (or an associate of the person) who is committing the scam.

Section 6-1

Part 6—Miscellaneous

6-1 Civil penalty provisions

A provision of this instrument referred to in an item in the following table is a civil penalty provision (within the meaning of the Regulatory Powers Act).

Note: 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.

Provisions that are civil penalty provisions	
Item	**Provision**
1	Subsection 2-2(1)
2	Subsection 2-2(2)
3	Section 2-3
4	Section 2-4
5	Subsection 2-5(1)
6	Subsection 2-6(1)
7	Subsection 2-7(1)
8	Subsection 2-8(1)
9	Section 2-9
10	Subsection 2-10(1)
11	Subsection 2-11(1)
12	Subsection 2-12(1)
13	Section 2-13
14	Subsection 2-14(1)
15	Subsection 2-15(1)
16	Subsection 2-16(2)
17	Section 2-17
18	Subsection 2-18(1)
19	Subsection 2-18(2)
20	Subsection 2-19(1)
21	Section 2-20
22	Subsection 2-21(1)
23	Section 2-22
24	Subsection 2-23(1)
25	Subsection 2-23(3)
26	Section 2-24
27	Section 2-25
28	Subsection 2-26(1)
29	Subsection 2-27(3)
30	Subsection 2-28(1)
31	Subsection 3-2(1)
32	Subsection 3-2(2)

Provisions that are civil penalty provisions	
Item	**Provision**
33	Subsection 3-3(1)
34	Section 3-4
35	Section 3-5
36	Section 3-6
37	Subsection 3-7(1)
38	Subsection 3-8(1)
39	Subsection 2-9(1)
40	Subsection 3-10(1)
41	Subsection 3-11(1)
42	Subsection 3-11(2)
43	Subsection 3-12(1)
44	Subsection 5-2(1)
45	Subsection 5-3(1)
46	Subsection 5-3(4)
47	Subsection 5-4(1)
48	Subsection 5-5(1)
49	Subsection 5-6(1)
50	Subsection 5-7(1)
51	Subsection 5-8(1)
52	Section 5-9
53	Section 5-10
54	Subsection 5-11(1)
55	Section 6-2

6-2 Implementing, monitoring and reviewing systems and processes

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

(a) implement the system or process; and

(b) monitor whether the system or process is being followed; and

(c) regularly review whether the system or process remains fit for purpose.

Note: This section is a civil penalty provision (see section 6-1).