AUSTRALIA'S PROPOSED SCAMS PREVENTION FRAMEWORK

Date: 11 February 2025

Australia Finance Alert

By: Claudine Salameh, Tamsyn Sharpe

In response to growing concerns regarding the financial and emotional burden of scams on the community, the Australian government has developed the Scams Prevention Framework Bill 2024 (the Bill). Initially, the Scams Prevention Framework (SPF) will apply to banks, telecommunications providers, and digital platform service providers offering social media, paid search engine advertising or direct messaging services (Regulated Entities). Regulated Entities will be required to comply with obligations set out in the overarching principles (SPF Principles) and sector-specific codes (SPF Codes). Those failing to comply with their obligations under the SPF will be subject to harsh penalties under the new regime.

WHY DOES AUSTRALIA NEED A SPF?

Australian customers lost AU$2.7 billion in 2023 from scams. Whilst the monetary loss from scams is significant, scams also have nonfinancial impacts on their victims. Scams affect the mental and emotional wellbeing of victims—victims may suffer trauma, anxiety, shame and helplessness. Scams also undermine the trust customers may have in utilising digital services.

Currently, scam protections are piecemeal, inconsistent or non-existent across the Australian economy. The SPF is an economy-wide initiative which aims to:

- Halt the growth in scams;
- Safeguard the digital economy;
- Provide consistent customer protections for customers engaging with Regulated Entities; and
- Be responsive and adaptable to the scams environment.

WHAT IS A SCAM?

A scam is an attempt to cause loss or harm to an individual or entity through the use of deception. For example, a perpetrator may cause a target to transfer funds into a specified bank account by providing the target with what appears to be a parking fine. However, financial loss caused by illegal cyber activity such as hacking would not be a scam as it does not involve the essential element of deception.

©2005-2026 K&L Gates LLP. All Rights Reserved.

SPF PRINCIPLES

The Bill sets out six SPF Principles which Regulated Entities must comply with. The SPF Principles will be enforced by the Australian Competition and Consumer Commission (ACCC) as the SPF General Regulator.

The SPF Principles are outlined in table 1 below.

SPF Principle	Description
1. Governance	Regulated Entities are required to 'develop and implement governance policies, procedures, metrics and targets to combat scams'. In discharging their obligations under this principle, entities must develop and implement a range of policies and procedures which set out the steps taken to comply with the SPF Principles and SPF Codes. The ACCC is expected to provide guidance on how an entity can ensure compliance with their governance obligations under the SPF.
2. Prevent	Regulated Entities must take reasonable steps to prevent scams on or relating to the service they provide. Such steps should aim to prevent people from using the Regulated Entity's service to commit a scam, as well as prevent customers from falling victim to a scam. This includes publishing accessible resources which provide customers with information on how to identify scams and minimise their risk of harm.
3. Detect	Regulated Entities must take reasonable steps to detect scams by 'identifying SPF customers that are, or could be, impacted by a scam in a timely way'.
4. Report	Where a Regulated Entity has reasonable grounds to suspect that a 'communication, transaction or other activity on, or relating to their regulated service, is a scam', it must provide the ACCC with a report of any information relevant to disrupting the scam activity. Such information is referred to as 'actionable scam intelligence' in the SPF. Additionally, if requested by an SPF regulator, an entity will be required to provide a scam report. The appropriate form and content of the report is intended to be detailed in each SPF Code.
5. Disrupt	A Regulated Entity is required to take 'reasonable steps to disrupt scam activity on or related to its service'. Any such steps must be proportionate to the actionable scam intelligence held by the entity. As an example, for banks, appropriate disruptive activities may include: ▪ Contacting customers to warn them of popular scams; ▪ Introducing confirmation of payee features on electronic banking services; and ▪ Placing a hold on payments directed to an account associated with scam activity to allow the bank time to contact the customer and provide them with

©2005-2026 K&L Gates LLP. All Rights Reserved.

	information about the suspected scam.
6. Respond	Regulated Entities are required to implement accessible mechanisms which allow customers to report scams and establish accessible and transparent internal dispute resolution processes to deal with any complaints. Additionally, Regulated Entities must be a member of an external dispute resolution scheme authorised by a Treasury Minister for their sector. The purpose of such an obligation is to provide an independent dispute resolution mechanism for customers whose complaints have not been resolved through initial internal dispute resolution processes, or where the internal dispute resolution outcome is unsatisfactory.

Table 1

WHAT ARE 'REASONABLE STEPS'?

We expect that SPF Codes will provide further clarification regarding what will be considered 'reasonable steps' for the purposes of discharging an obligation under the SPF Principles. From the explanatory materials, it is evident that whether reasonable steps have been taken will depend on a range of entity-specific factors including, but not limited to:

- The size of the Regulated Entity;
- The services of the Regulated Entity;
- The Regulated Entity's customer base; and
- The specific types of scam risk faced by the Regulated Entity and their customers.

DISCLOSURE OF INFORMATION UNDER THE REPORTING PRINCIPLE

As indicated in table 1 above, the SPF reporting principle requires disclosure of information to the SPF regulator. It is clear from the explanatory materials that, to the extent this reporting obligation is inconsistent with a legal duty of confidence owed under any 'agreement or arrangement' entered into by the Regulated Entity, the SPF obligation will prevail. However, it is not expressly stated how this obligation will interact with statutory protections of personal information.

The *Privacy Act 1988* (Cth) (*Privacy Act*) imposes obligations regarding the collection, use and disclosure of personal information. Paragraph 6.2(b) of Schedule 1 to the *Privacy Act* allows an entity to use or disclose information for a purpose other than which it was collected where the use or disclosure is required by an Australian law. Arguably, once the SPF is enacted, disclosure of personal information in accordance with the obligations under the reporting principle will be 'required by an Australian law' and therefore not in breach of the *Privacy Act*.

SAFE HARBOUR PROTECTION FOR DISRUPTIVE ACTIONS

As noted in table 1, SPF Principle 5 requires entities to take disruptive actions in response to actionable scam intelligence. This may leave Regulated Entities vulnerable to actions for breach of contractual obligations. For

©2005-2026 K&L Gates LLP. All Rights Reserved.

example, where a bank places a temporary hold on a transaction, the customer might lodge a complaint for failure to follow payment instructions. To prevent the risk of such liability from deterring entities from taking disruptive actions, the SPF provides a safe harbour protection whereby a Regulated Entity will not be liable in a civil action or proceeding where they have taken action to disrupt scams (including suspected scams) while investigating actionable scam intelligence.

In order for the safe harbour protection to apply, the following requirements must be met:

1. The Regulated Entity acted in good faith and in compliance with the SPF;
2. The disruptive action was reasonable and proportionate to the suspected scam;
3. The action was taken during the period starting on the day that the information became actionable scam intelligence, and ending when the Regulated Entity identified whether or not the activity was a scam, or after 28 days, whichever was earlier; and
4. The action was promptly reversed if the Regulated Entity identified the activity was not a scam and it was reasonably practicable to reverse the action.

The assessment of whether disruptive actions were proportionate will be determined on a case-by-case basis. However, relevant factors may include:

- The volume of information received or available;
- The source of that information; and
- The apparent likelihood that the activity is associated with a scam.

SPF CODES

As a 'one-size-fits-all' approach across the entire scams ecosystem is not appropriate, the SPF provides for the creation of sector-specific codes. These SPF Codes will set out 'detailed obligations' and 'consistent minimum standards' to address scam activity within each regulated sector. The SPF Codes are yet to be released.

It is not clear whether the SPF Codes will interact with other industry codes and, if so, how and which codes will prevail.

It appears from the explanatory materials that the SPF Codes are intended to impose consistent standards across the regulated sectors. It is unclear whether this will be achieved in practice or whether there will be a disproportionate compliance burden placed on one regulated sector in comparison to other regulated sectors. For example, because banks are often the ultimate sender/receiver of funds, will they face the most significant compliance burden?

SPF REGULATORS

The SPF is to be administered and enforced through a multiregulator framework. The ACCC, as the General Regulator, will be responsible for overseeing the SPF provisions across all regulated sectors. In addition, there will be sector-specific regulators responsible for the administration and enforcement of SPF Codes.

©2005-2026 K&L Gates LLP. All Rights Reserved.

ENFORCEMENT

The proposed Bill sets out the maximum penalties for contraventions of the civil penalty provisions of the SPF.

There are two tiers of contraventions, with a tier 1 contravention attracting a higher maximum penalty in order to reflect that some breaches would 'be the most egregious and have the most significant impact on customers'. A breach will be categorised based on the SPF Principle contravened as indicated in table 2 below.

Tier 1 Contravention	Tier 2 Contravention
▪ SPF principle 2: prevent ▪ SPF principle 4: detect ▪ SPF principle 5: disrupt ▪ SPF principle 6: respond	▪ An SPF Code ▪ SPF principle 1: governance ▪ SPF principle 3: report

Table 2

In addition to the civil penalty regime, other administrative enforcement tools will be available including:

- Infringement notices;
- Enforceable undertakings;
- Injunctions;
- Actions for damages;
- Public warning notices;
- Remedial directions;
- Adverse publicity orders; and
- Other punitive and nonpunitive orders.

ASSISTANCE

The SPF is expected to commence later this year. In the meantime, Regulated Entities need to prepare for the commencement of their SPF obligations. K&L Gates is well equipped to assist Regulated Entities to understand the SPF requirements and update internal governance, policies and processes to reflect new obligations. To find out more about how we can support you, reach out to one of our skilled team members listed below.

The authors would like to thank paralegal Tamsyn Sharpe for her contribution to this legal insight.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



CLAUDINE SALAMEH
PARTNER

SYDNEY
+61.2.9513.2541
CLAUDINE.SALAMEH@KLGATES.COM



AYMAN GUIRGUIS
PARTNER

SYDNEY
+61.2.9513.2308
AYMAN.GUIRGUIS@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.