



THREAT
FABRIC

Clarity on Australian Scam Regulations

by Ken Palla





Table of Contents

Executive Summary	2
Who Is Protected by The Regulation?	4
Definition of a Scam that Is Included	5
Activity Excluded	6
Which Entities Are Required to Participate in the Regulations?	7
What Do the Regulations Cover and How Will the SPF Work?	8
SPF Principal 1: Governance	9
SPF Principal 2: Prevent	10
SPF Principal 3: Detect	10
SPF Principal 4: Report	11
SPF Principal 5: Disrupt	11
SPF Principal 6: Respond	12
How Will Dispute and Reimbursement Work?	13
How Will Government Penalties Work?	14
Summary	16
Final thought	18
Acknowledgements	18



Executive Summary

In September 2024, the Australian Government has come out with its second consultancy on protecting Australians from financial scams. It is called the Scam Prevention Framework (SPF or simply “the framework”). This consultancy contains draft legislation describing the proposed controls. The proposed legislation is very broad and will initially require mandatory participation from three business sectors: financial institutions, telecommunications providers and digital platform services. It will require these entities to have various controls in place to prevent financial scams. This legislation will become amendments to the Competition and Consumer Act of 2010. Once the legislation is approved (receives Royal Assent), the sectors will have a defined period of time to deploy the controls.

If the entities do not properly deploy the scam controls, as defined in the proposed legislation and in future sector-specific SPF codes, then there are two outcomes:

1. The business entity can be fined for breached of the framework. This can be as high as AU\$50 million or 30% of the entity’s turnover (revenue) during the period in breach of the framework.
2. Customers who have become victims of a financial scam can request reimbursement from the sector entity/entities involved in the customer’s scam, IF it can be shown that the involved entities did not have the proper SPF controls in place. This will be resolved via an internal or external dispute resolution process.

Unlike the UK’s mandatory APP scam reimbursement program, effective in October 2024, just involving financial institutions (with also strong controls required, but where the quality of the controls are not tied to the reimbursement assessment), the Australian approach involves financial institutions, telecommunications providers and digital platform services adding strong controls to prevent scams. And if these strong controls are properly in place, scams will be dramatically reduced and there will be no reimbursement. If, however, these sector entities do not properly deploy the defined SPF controls, then Australian scam victims can be eligible for reimbursement.

It is important to note that these three sectors have already added some levels of controls to help protect Australians and reduce scams. In 2023, the Australian Bankers Association introduced the Safe-Scam Accord, which will add scam controls including Confirmation of Payee. The telecommunication sector introduced the Reducing Scam Calls and Scam SMS Code in 2022 which requires telecommunications providers to take steps to identify, trace and block scam calls and messages. The Australian government also just passed legislation in August 2024 for SMS Sender ID Register that will check whether messages being sent under a brand name match the legitimate registered sender.

The Digital Industry Group Inc (DIGI) introduced in July 2024 the voluntary Australian Online Scam Code. This DIGI Code is a holistic response that spans blocking and takedown of suspected scams, includes advertiser verification measures and increased collaboration with Australia’s National Anti-Scam Centre.

This proposed legislation is historic in that it combines the three primary business sectors involved in facilitating consumer scams. Sure, the fraudster is out there making these scams work. Oftentimes the actual scammer may be imprisoned in a scam center themselves in Asia or other



countries. But make no mistake, this is large scale organized crime using text messages, social media platforms and bank payment rails to execute these scams. This legislation is out to dramatically reduce what Australian consumers lose to scammers. In 2023, Australian consumers lost \$2.7 billion to scammers.

The Australian consultancy documents contain about 200 pages of proposed legislative text and explanation. So, let's unpack this detailed content to see what is included.



Who Is Protected by The Regulation?

The legislation defines who is protected by this proposed legislation. It introduces the concept of an “SPF consumer”. An SPF consumer is a natural person who is:

1. In Australia (e.g. visitor), ordinary resident in Australia, an Australian citizen, a permanent resident
2. A person who carries on a business having less than 100 employees and a principal place of business in Australia

A person can be a “SPF customer” of a regulated service of one of the SPF regulated entities. This can be:

- Where customer has a direct relationship with the regulated entity (e.g. a customer of the bank or telco carrier).
- Where a customer does not have an existing relationship with a regulated entity (e.g. victim gets solicited to a scam where victim does not have an existing relationship with the service described in the scam; or where victim receives a call from a scammer using a carriage/carrier service provider or intermediary where the victim does not have a relationship).



Definition of a Scam that Is Included

The legislative language defines a scam as an attempt to engage an “SPF consumer” of a regulated service that involved deception and would, if successful, cause loss or harm including financial or personal information. There are four ways deception can occur:

1. deceptively represents something to be (or to be related to) the regulated service; or
2. deceptively impersonates a regulated entity in connection with the regulated service; or
3. is an attempt to deceive the SPF consumer into facilitating an action using the regulated service; or
4. is an attempt to deceive the SPF consumer that is made using the regulated service.

The Explanation Document lists several examples of scams included. Here are some of these examples below:

- an imposter bond scam, where a scammer impersonates a financial advisor and makes a false representation in relation to an investment product or bond offered by a banking service that in fact does not exist.
- an impersonation scam where a consumer receives a text message using the alphanumeric tag from a well-known banking entity appearing in the existing chain of text messages from that entity. The text message notified the consumer that an irregular payment had been detected with a phone number to contact. The consumer was told their account had been compromised and their funds needed to be transferred to a safe account and was told to transfer the money to a specific new account that had been opened. The consumer transferred \$60,000 to the scammer.
- (where paid search advertising services are designated as a regulated sector), this would include false advertisements that trick consumers into providing their personal information or transferring money.
- text messages or phone calls are used to initiate contact between a scammer and an SPF consumer to deceive the consumer.

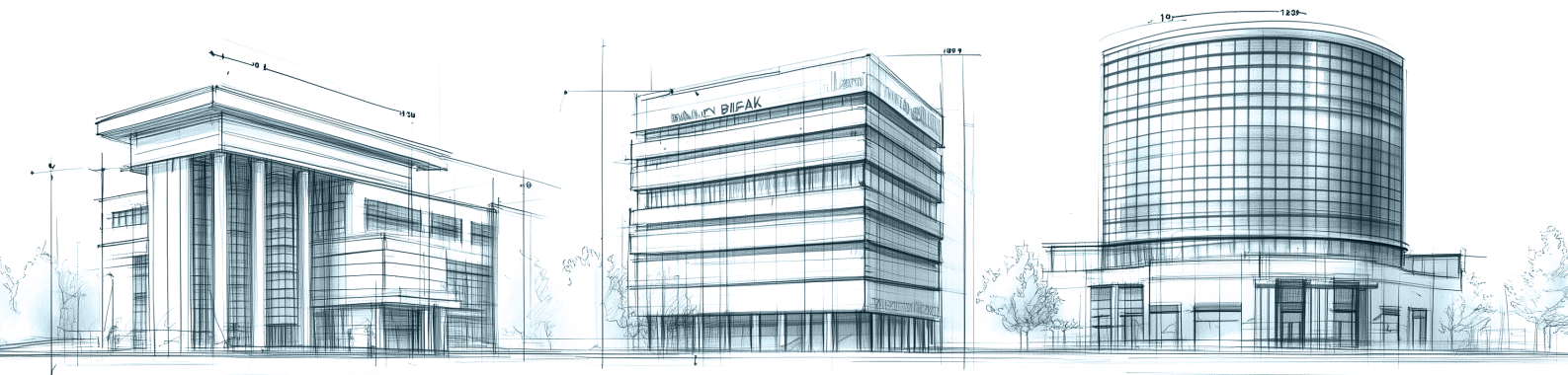


- an SPF consumer receives a message on their social media account from a profile seeking a relationship. The profile, operated by a scammer, fosters a fake relationship with the consumer and takes the communication “offline” to SMS. Over weeks or months, the SPF customer is deceived to believe they have built a relationship and trust with the scammer who encourages the SPF consumer to invest in fake investments. The scammer then discloses that they have been in an accident and urgently need money, which is paid by the SPF consumer to the scammer via bank transfer.

Activity Excluded

Any conduct already regulated by existing consumer law is excluded from the SPF framework. As an example, misleading or deceptive conduct as defined in schedule 2 of the Competition and Consumer Act of 2010 (CCA) is not considered a scam for the purposes of the SPF. Nor is fraud that does not involve any action by the consumer.

The Treasury Minister can also exclude specific activities that are not covered by the SPF.



Which Entities Are Required to Participate in the Regulations?

The SPF has initially defined three business sectors to be included in the SPF regulations. More sectors can be added as needed. The initial sectors are:

- Banking businesses
- Telecommunication providers
- Digital platform services, initially including social media, paid search engine advertising and direct message services

The draft legislation also currently includes other sectors:

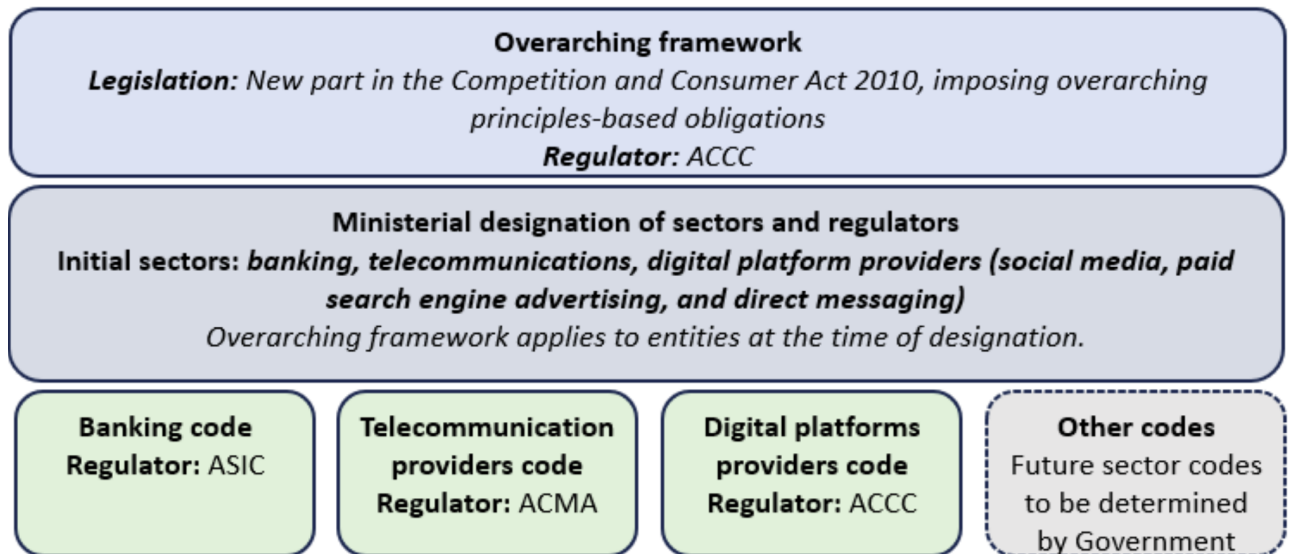
- Insurance businesses
- Postal and telegraphic services
- Broadcasting services

It is not clear these other sectors will remain in the final legislation.

What Do the Regulations Cover and How Will the SPF Work?

The Australian Treasury just added a summary document for the SPF proposal. It included a figure that helps explain the overarching framework of the SPF (See Figure 1).

Figure 1. Proposed scams prevention framework



Source: Scam Prevention Framework- Summary of Reforms document Australian Treasury September 2024

The Treasury has designated the Australian Competition and Consumer Commission (ACCC) as the general regulator for the Scam Prevention Framework (SPF). The ACCC also enforces the Competition and Consumer Act 2010 (CCA), within which this new legislation will reside.

There will also be a regulator for each initial sector:

- Banking-The Australian Securities and Investment Commission (ASIC)
- Telecommunications- Australian Communications and Media Authority (ACMA)
- Digital Platforms- Australian Competition and Consumer Commission (ACCC)

The business entities within these sectors are referred to as regulated entities.

Each regulator will need to create its own governance associated with the SPF. This governance will control how each regulator enforces the SPF with its sector’s regulated entities. The SPF sector regulator will be responsible for monitoring compliance with SPF codes and pursuing enforcement actions for suspected breached of entity required controls.

Treasury can add sector-specific SPF codes. These codes will add detailed regulation/controls above and beyond what is contained in the legislation. The SPF codes will be more prescriptive-type controls, but still allowing room for entities to interpret the code for final deployment and allow for addressing new scam variants. Treasury can also delegate the creation of sector-specific



SPF codes to any of the involved regulators. According to the government documents on the scam legislation, Treasury, or its delegate, must use “legislative instrument” to create SPF codes. This is the way in Australia to add additional controls and responsibilities for the sector-specific regulated entities, without having to formally go back and get legislation voted on. It gives the regulators flexibility to add and change controls over time.

Treasury has added an interesting caveat on SPF codes: “In some cases, taking reasonable steps to meet one or more of the SPF principles may require a regulated entity *to take steps beyond the sector specific obligations set out in an SPF code.*” But later on in the Treasury Summary document, it says: “The codes will not set out an exhaustive list of obligations to satisfy compliance with the principles-based obligations, *but rather will include a set of minimum standards* that may be directed at addressing sector-specific harms related to scams.

The concept of “*reasonable steps*” and “*minimum standards*” will need to come into play as to how these regulated entities deploy controls. And later, when we get to the How Will Reimbursement Work section, these concepts will be important in determining if an entity has met its SPF obligations or not, in order to determine if compensation to the SPF customer is required.

Treasury has identified the primary areas of the SPF for regulated entities to support. These are:

1. **Governance:** arrangements required to develop and implement governance policies, procedures and metrics to combat scams
2. **Preventing scams:** have reasonable steps to stop scam activity from reaching customers
3. **Detecting scams:** detect scams as they occur
4. **Reporting Scams:** report scam activity and provide actionable scam intelligence with ACCC
5. **Disrupting Scams:** disrupt scams in process
6. **Responding to Scams:** Allow consumers to report scams and have an Internal Dispute Resolution (IDR) process and be part of an External Dispute Resolution (EDR) process

SPF Principal 1: Governance

Each entity in a regulated sector must create governance to support the SPF. This is where the work begins for the banking entities, telco providers and digital platforms. Each entity must develop, maintain and implement governance policies for managing the risk of scams. Below are some of the governance requirements:

- Write documentation for scam prevention, detection, disruption, response and reporting.
- Develop performance metrics and targets to measure effectiveness of the policies and procedures.
- Document how to identify and manage actionable scam intelligence.
- Document how to assess and address the risks of scams on an ongoing basis.
- Determine how to make information available on its measures to protect its customers from scams. This includes how consumers can report a scam, how consumers can make a complain about an activity relating to a scam, etc.
- Support governance that is defined in individual SPF codes.



Governance policies and procedures must be reviewed and approved by a senior officer in writing annually.

A regulated entity must keep records in relation to activities taken to comply with obligations under the SPF for six years.

SPF Principal 2: Prevent

Note: These next sections start to contain broad definitions on controls. They could become difficult for the regulated entities to comply with to reduce scams and still meet the internal goal of not having to unnecessarily reimburse SPF customers for scam losses (because the entity has failed to comply with the SPF). There will be aspects of “reasonableness” and “proportionality” of effect in creating the required controls. As entities establish the controls in the Prevent, Detect, Report, Disrupt and Respond sections, they will be asking themselves how they comply to fully meet the legislative requirements and the yet-to-be-published SPF code requirements.

This principal is based on prevent scams from occurring. The regulated entity must take reasonable steps to prevent a scammer from committing a scam against an SPF customer. Here are some of the requirements that will/may be required:

- Provide relevant resources (e.g. information, warnings, training) to SPF customers to help them identify scams and minimize their risk of involvement with scams.
- Identify its customers that have a higher risk of being targeted by specific scams and provide them with specific warnings (e.g. identifying crypto scams occurring and then focusing on customers doing crypto transactions and provide specific warnings).
- Introduce additional identity verification for new accounts (e.g. bank accounts, dating site accounts, adding ads on social media).
- Proactively seek out information from other sources on emerging scam activity.
- Do more than merely act on actionable scam intelligence from third parties. This should also involve active data collection from entity transactions and constantly monitoring scam trends and the forensics of these trends.
- Train staff on emerging scam activity.
- Introduce robust procedures that prevent scammers from accessing or using its platform.

SPF Principal 3: Detect

This principal involves taking reasonable steps in detecting scams, which includes identifying SPF customers that could be likely victims.

Some of the requirements:



- Detect scam activity through actionable scam intelligence received and through the entity's own internal mechanisms. Once actionable scam intelligence is obtained, the entity must use this information to prevent scams.
- Detect scams as they happen
- Detect scams after they happen

An example of failure of this principal would be that the entity had actionable scam intelligence and failed to take reasonable steps within a reasonable time to identify SPF consumers who are or could be impacted.

In the future, an SPF Code might describe a control defining reasonable steps and reasonable time for the purposes of identifying potential victims.

SPF Principal 4: Report

This principal places requirements on the regulated entity to provide information to the SPF regulators. Some of the requirements are:

- Actionable scam intelligence obtained by the entity must be timely (as soon as practicable) reported to the SPF general regulator. This intelligence must contain enough information to help disrupt the scam. The SPF regulator is obligated to provide this information to other regulated entities.
- A full scam report made by a customer about a scam activity. This can include personal and bank account information (e.g. sending and receiving bank accounts) and other key information (e.g. description of bogus ad and media platform where it was seen). The SPF regulator may also share this information, being respectful of the need to protect PII data.

The SPF regulator(s) may define formats for this information sharing.

SPF Principal 5: Disrupt

This principal requires regulated entities to have reasonable controls in place to disrupt scams.

Some of the possible controls:

- Share actionable intelligence with both consumers and the regulators.
- Share a report, in regulator approved format, about the outcome of an investigation relating to actionable scam intelligence.
- (Again, the entity must) take reasonable steps to disrupt scams based on actionable intelligence to prevent loss.
- Blocking phone numbers, accounts or content associated with scam activity.
- Introducing holds to payments and stopping payments in critical cases.
- Add confirmation of payee.
- Removal of content associated with scam activity.

- Possibly allowing SPF customers to freeze their own account or stop a transaction.

An example of failure of this principal would be that the entity receives a substantial number of similar reports of suspected scams and fails to take additional action such as pausing or delaying authorized push payments while the bank investigates the suspected scams.

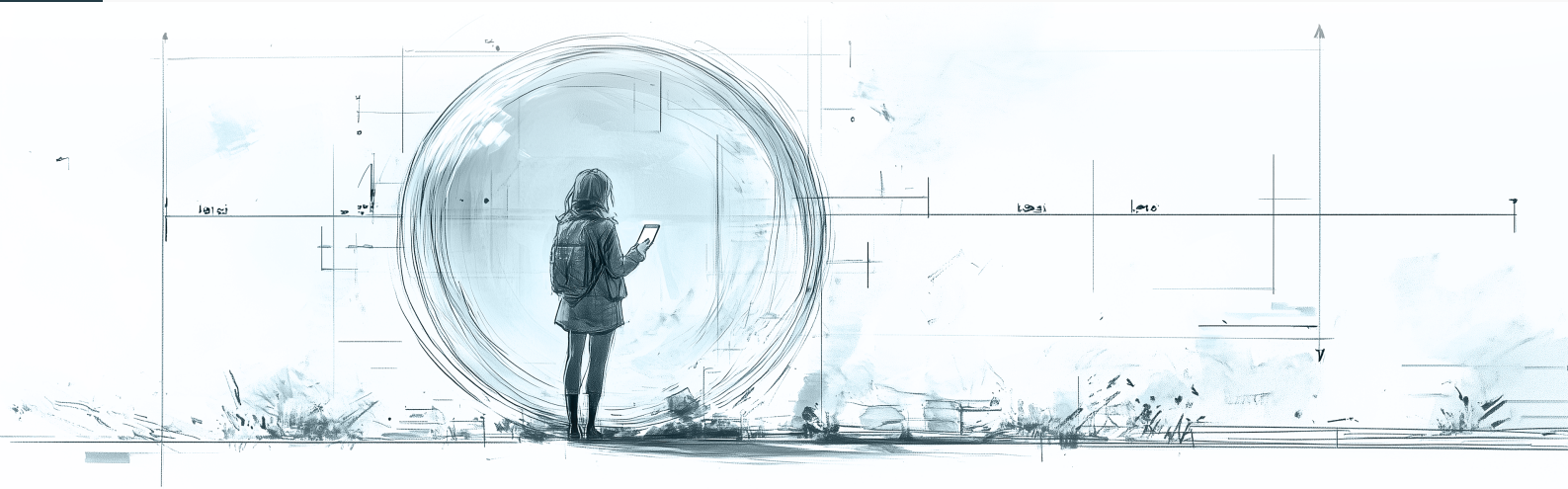
Entities are protected (safe harbor) from damages when taking certain actions to prevent scams, including reasonable and proportionate temporary disruptive actions taken by regulated entities. There are a number of additional considerations for this safe harbor.

SPF Principal 6: Respond

This principal requires regulated entities to have access mechanisms for their SPF customers to be able to report scams and submits complaints about scams or the entity's conduct relating to scams. Each entity must have an Internal Dispute Resolution (IDR) unit to receive and process complaints.

The current proposed legislation does not include much language around what is required of the IDR. I would expect much more in subsequent sector-specific SPF Codes.

Plus, each regulated entity must be a member of the Australian Financial Complaint Authority (AFCA), the single External Dispute Resolution (EDR) scheme for the three initial sectors defined in the framework. The purpose of the EDR is to handle SPF consumer disputes, including compensation for scam losses, "where a regulated entity has not complied with their obligations under the SPF." The EDR is intended to be "an independent, fair and impartial mechanism" for SPF customers when they are not satisfied with the IDR response.



How Will Dispute and Reimbursement Work?

This dispute process will take place when an SPF customer loses money in a financial scam and wants reimbursement. They will first go to its entity's IDR and if not satisfied with the outcome, proceed to the EDR.

According to the legislation, the only way an SPF customer will get reimbursed is if the regulated entity/entities associated with the scam transaction(s) have failed to meet the SPF controls (either from the legislation or from the sector-specific SPF Codes) for the specific sector (Banking, telecom or digital platforms). It will be the responsibility of AFCA to make the determination if the SPF customer is eligible for the refund and which regulated entity/entities must reimburse.

This is the point where the proposed scam legislation/SPF Codes hits its most difficult point. In this paper, we have spent 7 pages describing the obligations that regulated entities have associated with this scam legislation. After reading this summary, one can see how difficult it will be for a regulated entity to meet all of these requirements. And we do not yet have any general or sector-specific SPF codes defined.

So, how will the EDR, AFCA, deal with this issue. It will be extremely difficult. In essence, AFCA will have to review the controls for each registered entity involved in each SPF customer request for compensation and make a determination if each involved registered entity is in compliance with the regulations/SPF codes and by how much. Is it 100% compliance, 80% or 60% or simply not in compliance. Honestly, this could take countless hours to determine.

Maybe the primary regulator will require each sector regulator to score each sector-regulated entity on a quarterly basis and use this scoring for AFCA assessment. This is not in the current Treasury documentation at all. But this not unrealistic, as the sector regulator must monitor each regulated entity for compliance to the SPF and take action when an entity is out of compliance.

In a document from the Digital Industry Group, Inc (DIGI), DIGI says, “there could be a protracted examination through an external dispute resolution body of different companies’ relative roles in the scammers’ attack, in order to determine possible redress. Unlike the UK scheme, that could take years for any form of reimbursement for people who have lost their life savings because of the sheer number of different services scammers exploit in their complex attack chain.”¹ I do not think it will take years to ascertain liability and reimbursement, but nor will it take just days.

This part of the proposed scam legislation is undoubtedly the weakest part. I do not think it has been completely thought through yet and it will be extremely difficult for AFCA to do its job as the EDR, unless this will also involve the sector regulator for assessing the entities compliance of the scam controls.

How Will Government Penalties Work?

This proposal contains strong penalties for entities that fail to comply with the regulations. Figure 2 below comes from the Treasury summary of the scam proposal. Non-performance is broken into two categories: Tier 1 contravention and Tier 2 Contravention (see definitions in the Figure). It shows that Tier 1 non-performance can cost up to AU\$50 million or 30% of the turnover (revenue) during the period in breach. These are not trivial amounts.

Figure 2. Proposed Tiered penalty regime

	Tier 1 contravention	Tier 2 contravention
	<i>Breaches of the principles-based obligations in the primary law relating to preventing, detecting, disrupting and responding to scams</i>	<i>Breaches of the principle-based obligations in the primary law relating to reporting and governance and any breaches of the sector codes</i>
Penalty for an entity	The greater of: <ul style="list-style-type: none"> • \$50 million • three times the value of the benefit obtained, or • 30 per cent of the turnover during the period in breach 	The greater of: <ul style="list-style-type: none"> • \$10 million • three times the value of the benefit obtained, or • 10 per cent of the turnover during the period in breach
Penalty for an individual	<ul style="list-style-type: none"> • \$2,500,000 	\$500,800

Source: Scam Prevention Framework- Summary of Reforms document Australian Treasury September 2024

Also, the regulators have additional legal actions they can exercise. These can involve enforceable undertakings, injunctions, public warning notices about an entity’s contravention of



the SPF, remedial directions where an entity is failing to comply with the SPF, adverse publicity orders, non punitive orders and orders other than damages.

The first priority of this legislation is for all regulated entities to be on board, add the controls and help to stop these scams. But there is a big stick for the regulators for those entities who are not fully onboard or are having difficulty complying.



Summary


The Australian Government, and specifically Treasury, has produced a very effective cross-industry scam control proposal. Australia is the first government to propose mandated control across banking, telecom and digital platforms to help stop financial scams. There is much to like about this proposal. Timing wise, I think we could see this legislation implemented in early 2025.

We already see each of the three business sectors implementing scam controls on their own. And we know that much of this financial scamming is generated by various organized crime groups around the world, using the bank's payment rails, telco voice and text messages and digital platforms- oftentimes using all of these sectors as part of each scam. So, it is very important to have a unified approach to stopping these scams.

This proposal covers the important areas for each of these sectors. There is a strong definition around governance of the controls process. Plus, key focus on the scams themselves—Prevent, Detect, Report, Disrupt and Respond. It is clear this is a very different approach than exists in the UK. The UK's focus has been on the banks (the payment service providers) having strong controls and mandated reimbursement (effective October 2024) for APP scams. Australia has put the strong focus on mandating controls at the three critical business sectors involved in consumer scams. Then, it provides for robust penalties for failure to comply with the regulations, plus allowing customer who get scammed to get reimbursement from the affected entities, IF these entities are out of compliance for the scam controls.

With all good solutions, there can be caveats. The external Dispute Resolution (EDR) entity, AFCA, has a significant burden placed on itself to adjudicate the SPF consumer claims for scam reimbursement based on whether the regulated entity/entities have complied with the complete set of scam governance and controls. Here is what AFCA can do:

1. Determine which regulated entities are truly involved. Was there a text message or phone call involved? What bank/banks payment rail and accounts were used? Did it involve a



digital channel (e.g. a bogus advert or a dating site with a person impersonating a people connection).

2. For the involved regulated entities, has each entity followed the legislation and SPF Code governance and required controls? And what if some of the controls have been followed and other are weak or missing? This Step 2 is not a simple step. This amounts to a complete technical assessment of the entity's scam controls. This is hours/maybe weeks of work and requires scam control expertise to complete the assessment.
3. Based on the results of Step 2 (full compliance, partial compliance, no compliance), AFCA needs to then decide if reimbursement is warranted and how this should be split between the involved entities.

Note: AFCA will also need to take into account regulated entity claims of potential first party fraud.

This EDR assessment step needs to be really thought out with more robust framework and expectations defined. Also, the EDR, AFCA, will need to involve the sector regulator(s) to help determine if the involved entities in the claim are in compliance.

Over the coming months, the Treasury and the regulators will be adding sector-specific SPF Codes that will contain specific scam controls to prevent, detect and disrupt scam activities. These codes will become a core part of the SPF.

Final thought

The Australian government has significantly moved the needle for sound scam controls and needs to be complimented. More governments need to think about this approach. This is a very sound framework for creating and managing financial scam controls at the three most important business sectors- banking, telecom and digital platforms. There just needs to be more thought around the EDR reimbursement consideration. And it is very good to see each of the sectors has already been initiating controls to reduce scams.

Acknowledgements

Quotes without a reference come from the Australian SPF documents. Also, for specificity, some text has been copied from these government documents.

- Scams legislation welcome, but five key questions need answers, Digital Industry Group, Inc. September 17, 2024
 - https://digi.org.au/wp-content/uploads/2024/07/FINAL_-DIGI-industry-led-scams-code-_July-2024-1-1.pdf
- Exposure Draft- Treasury Laws Amendment Bill 2024: 4 Scams Prevention Framework
 - <https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-ed.pdf>
- Treasury Laws Amendment Bill 2024: Scams Prevention Framework (Exposure Draft Explanatory Materials)
 - <https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-em.pdf>
- Scams Prevention Framework Summary of reforms
 - <https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-summary.pdf>