Australian Government
The Treasury

Scams Prevention Framework

Protecting Australians from scams

January 2025

treasury.gov.au

Manager
Media Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

In the spirit of reconciliation, the Treasury acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples.

Contents

Background

The Government introduced the *Scams Prevention Framework Bill 2024* into the Parliament on 7 November 2024 to establish world-leading protections against scams. The Scams Prevention Framework (SPF) lifts the bar across the economy by setting out consistent and enforceable obligations for businesses in key sectors where scammers operate. This will better protect consumers and make Australia one of the toughest places in the world for scammers to target.

The SPF is a key pillar of the Government's response to the rising threat of scams. Over $180 million has been invested since 2022 to combat scams, including to:

- establish the National Anti-Scam Centre (NASC) as a partnership between regulators, law enforcement and industry to detect, disrupt and prevent scams,
- begin establishing a registry for SMS sender IDs to prevent criminals impersonating a well-known brand or service,
- boosting regulators abilities to take down scam websites.

Why is action needed?

Scams present an unacceptable threat to the Australian community and have had a devastating impact on thousands of Australians. In 2023, 601,000 Australians reported $2.74 billion in losses to scams. Regardless of the value stolen, the impacts on the victim can lead to undue stress, psychological and emotional harm. Urgent action is required to keep Australians safe.

A more digital economy has brought significant benefits but has also allowed scammers to reach a growing number of Australians. Technology that lets us easily connect with our friends and family also enables scammers to connect with ordinary Australians. Technology that lets us instantly buy things online can also lead to Australians losing everything at the same speed. Australians must be able to retain trust in the digital economy or will lose the benefits of technology, a significant cost to bear and one that is borne by all.

As the number of scams have grown over the past decade, our laws have not kept pace. Businesses often (but not always) have vague or non-existent policies to protect their customers from scams. This means that everyday Australians are often required to wear the risk of scams on their own. Fighting the battle against scam activity requires everyone, including businesses, to play an active role.

The reforms in the SPF address the need for urgent action. The SPF introduces strong protections for consumers across the economy and seeks to reduce the harms caused by scams. This is vital to ensure that Australians are safe and secure.

The Scams Prevention Framework in action

Everyone has a role to play in preventing scams

Scams are an economy-wide problem and demand an economy-wide response. Government services, law enforcement, regulators, the private sector, and the community all need to work together to combat scammers. Scammers will otherwise shift and adapt to exploit the weakest link in the chain.

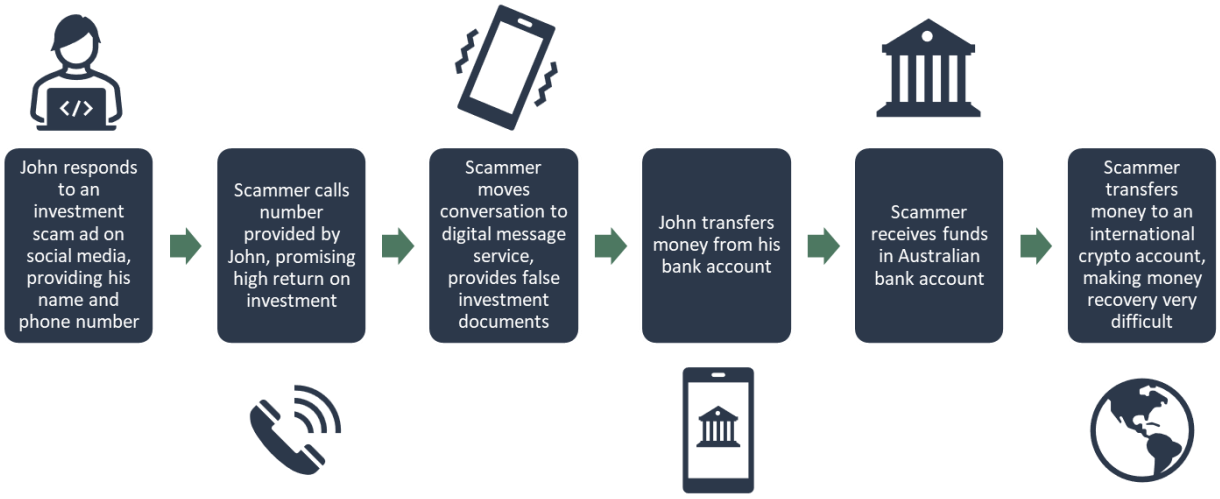
The NASC has brought together the expertise of regulators, law enforcement and industry to stop scammers reaching consumers. Their united efforts are working, with scam losses reported to Scamwatch falling by 41 per cent in the first 12 months after establishing the NASC.

Consumers also need more tools to arm themselves against scammers. To tackle this, the Government is funding a campaign commencing in 2025 that will improve community awareness of scams and help Australians identify, avoid and report scams.

Individuals have been bearing the brunt of the responsibility to combat scammers for far too long. While the steps taken by some organisations over the last few years are welcomed, it is time for the private sector to consistently step up its efforts. The SPF will set mandatory obligations on certain businesses so everyone plays their part in protecting Australians from scams.

Banks, certain digital platforms (including social media), and telecommunications providers (telcos) will be the first sectors required to comply with the SPF, as these sectors are where the greatest harms to consumers are currently occurring. Overwhelmingly, scammers contact their victims through the telco network and via digital platforms. The target is often the victim's money – their bank account.

Example of scam operating across different sectors – the SPF aims to stop the scam at each stage



The SPF is not set and forget. It allows protections to evolve in response to changing threats to consumers. The Government will also be able to expand SPF coverage to other sectors targeted by scams, such as superannuation funds or cryptocurrency wallets.

By hardening defences against scams across the ecosystem, the SPF will provide the Australian community with the toughest protections against scams in the world.

Scams are always evolving

Scam activity quickly changes and can vary from simple to sophisticated.

Scams can cause harm to consumers – whether or not successful, whether or not a significant sum of money was lost, and whether or not the scam attempt involved a single call or ongoing contact.

What is a scam under the SPF?

- An attempt to deceive a consumer into making a payment to a scammer using a regulated service, such as a bank transfer.
- An attempt to deceive a consumer into giving personal information to a scammer using a regulated service, such as a phishing scam on a direct messaging app.

These are considered scams even where they are not successful and do not lead to a loss. For example, a scam text message that a consumer does not engage with.

What is not a scam under the SPF?

- Fraud that involves dishonestly obtaining a benefit without any consumer action. For example, credit card fraud and identity theft where the consumer has had no direct engagement with a scammer.
- Cybercrime, such as obtaining personal information through a data breach or hack.
- Transactions involving faulty products, such as where a product does not function as intended, fit the sellers' description or is poor quality. This is regulated under other areas of consumer law.
- Transactions performed under the threat of imminent violence, such as a burglary or mugging.

Who is protected under the SPF?

The SPF will protect individuals and small businesses in Australia. It will also protect Australian residents overseas using regulated services provided by regulated entities based in Australia (such as Australian banking apps).

Prevent scams to protect consumers

The SPF aims to prevent scams from impacting consumers. The emotional, psychological, and financial costs of scam activity can be high. Stopping scams is the only way to protect consumers from these harms.

The SPF stops scams by requiring regulated businesses to take reasonable steps to prevent, detect and disrupt scams.

- **Prevent:** Businesses must take reasonable steps to prevent scams. This aims to stop scams from reaching consumers in the first place. For example, this could require telcos to block scam text messages before they reach consumers, social media companies to block the posting of investment scam ads (such as those with fake celebrity endorsements) and banks to proactively warn customers of recent scam trends.

- **Detect**: Businesses must take reasonable steps to detect scams as they are happening or after they have happened. This will help businesses act against known or suspected scams. For example, this could include businesses implementing algorithms to detect suspicious activity on their platforms.

  Disrupt: Businesses must take reasonable steps to disrupt an activity suspected of being a scam and prevent losses to consumers. For example, this could require a social media company to suspend scam accounts and contact users that interacted with the account. For a bank, it could require adding frictions to high-risk payments.

Businesses that do not meet their obligations under the SPF can face fines up to $50 million.

What does it mean to take reasonable steps?

Reasonable steps means businesses need to actively consider what is practical, appropriate and proportionate. This recognises there is not a 'one size fits all' solution. Different organisations may need to respond to unique scam threats in different ways. For example, a bank with a high proportion of migrant customers may need to take extra steps to make sure warnings will be understood by customers who do not speak English as a first language.

The SPF also enables mandatory codes of conduct to be made which will set out baseline obligations for each sector (see below). The high-level obligations to prevent, detect and disrupt scams are included in addition to the SPF codes as there may be cases where a business needs to go above and beyond a requirement in a sector code.

Sectors may have different obligations

Each sector has unique vulnerabilities that scammers seek to expose.

Mandatory industry codes of conduct will be introduced that set out specific obligations that lift the bar for each sector. There will be separate sector-specific codes for banks, telecommunication services and digital platforms. The SPF codes will set out the baseline steps that businesses will need to take to protect Australians from scams. These will be prescriptive requirements that support the principles-based obligations of the SPF.

Sector codes for the three initial sectors will be developed through consultation with industry and consumers in 2025.

Example obligations in the SPF codes to protect consumers from scams

Note: the below obligations are examples only to indicate how the SPF codes could work in practice.

Banks

- Implement technology to give customers greater confidence they are paying who they intended.
- Send specific consumer warnings for certain types of new payments, or high-risk payments.
- Adopt technology and controls to prevent identity fraud, including introducing biometrics checks for new customers opening accounts online.

- Provide outgoing transaction alerts to consumers on a real time basis, including where there has been the activation of a one-time passcode.
- Provide a 24/7 reporting channel for consumers to report suspected scam activity.

Digital Platforms

- Check all advertisers of financial products have an Australian Financial Services Licence (AFSL).
- Take specific steps in verification of new accounts.
- Provide help centre articles on how platforms are working to keep users safe and how users can keep themselves safe from scam activity.
- Take specific steps to identify scam advertisements and accounts.
- Freeze or block suspected scam accounts.
- Remove content identified as associated with scam activity.

Telecommunications service providers

- Implement an anti-scam filter to block SMS messages with known phishing links.
- Educate consumers on potential scams that may impact them.
- Implement processes and algorithms to actively monitor calls and texts for scam indicators, such as high-volume, short duration activity, and use of malicious URLs in text messages.
- Investigate and take appropriate action to block scam calls originating on their network.
- Have processes in place and cooperate with other providers to trace the origin of a suspected scam call.

Better and earlier intelligence sharing

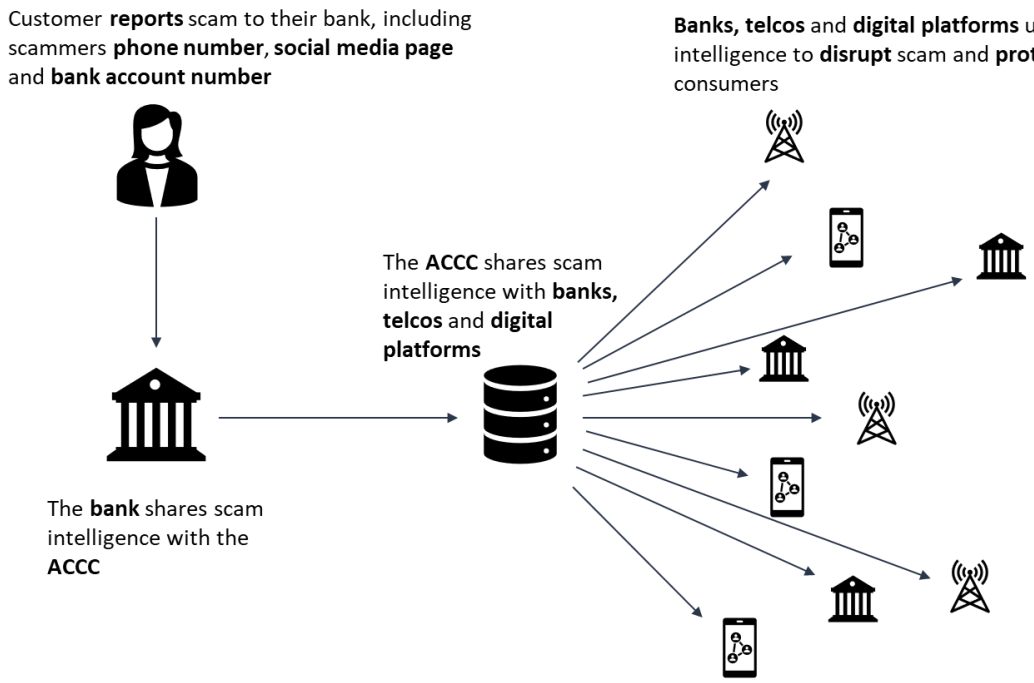
Businesses often only see one piece of the puzzle, which can make it harder for them to prevent and disrupt scams effectively. The SPF will require businesses to share scam intelligence with the ACCC, which will be able to distribute it to other businesses, law enforcement and international partners so they can take action to prevent, detect, and disrupt scams.

Scam intelligence includes scam reports to businesses by consumers. For instance, a person might share the bank details and social media account of a known or suspected scammer with their bank. The bank will then be required to report this information to the ACCC. The ACCC can then send the information to other banks and the social media provider to enable them to disrupt the scam.

Businesses will also be required to share scam intelligence they have gathered themselves with the ACCC. For instance, a digital platform that blocks a scam ad may share the phone number from the ad with the ACCC. The ACCC can then send this to telcos to enable them to disrupt the scam by blocking calls and texts from that number.

Enhanced intelligence sharing requirements will enable businesses to see the bigger picture and take fast, effective, and targeted action to protect consumers.

Scam intelligence shared across the ecosystem will help businesses take fast action against scams.



Intelligence sharing in practice

A bank puts a temporary block on a $50,000 transfer of funds to an international bank account as it has reason to suspect it may be a scam payment. The bank contacts the customer to ask why they are making the payment and assess if it may be a scam. The consumer tells the bank they are moving the funds to an investment account, which they set up after seeing an ad on a social media platform. Following further investigation by the bank, the bank informs the customer that they believe this is a scam, and the customer agrees to cancel the payment.

The bank reports the suspected scam to the ACCC, including the receiving bank account details and details of the social media ad given by the customer. The ACCC shares the suspected account details with other banks, and information about the ad with the social media company.

Another bank has received intelligence about the scam bank account and blocks all payments to that account. This saves other potential victims from being scammed who were responding to the same ad on social media.

The social media company takes down the ad and suspends the account that posted it. The social media company also contacts users that interacted with the scam account to warn them.

Compensating consumers when SPF obligations are not met

Consumers currently have few avenues to seek compensation for their scam losses. This is driven by a lack of clear and enforceable obligations on businesses to prevent scam activity for consumer complaints to be assessed against. There are also different dispute resolution approaches across sectors.

The SPF enables consumers to seek compensation where businesses have not met their obligations and a consumer has suffered a loss as a result. Consumers will have clear and accessible pathways to report a scam or make a complaint to the business.

Consumers should first make a complaint directly with the business involved in the scam. The SPF will require businesses to have accessible and transparent internal dispute resolution (IDR) processes to manage consumer complaints.

As scams often involve several businesses, the policy intention is that complaints handling will be driven by a 'no wrong door' principle. This means consumers can make a complaint to any business connected to the scam and businesses will need to cooperate with one another to resolve complaints in good faith. If a business finds it did not comply with its obligations under the SPF and this led to the consumer suffering a loss, the business will be expected to provide compensation or other remedies to the consumer at the IDR stage.

Where a business is unable to satisfactorily resolve a complaint, consumers will have access to a single external dispute resolution (EDR) body. The Australian Financial Complaints Authority (AFCA) will deliver EDR for the three initial sectors. AFCA will be able to consider the actions of each business connected to a scam complaint and award compensation having regard to the business' proportionate responsibility for the loss.

A single EDR scheme for the three initial sectors offers consumers a holistic experience where businesses from multiple sectors are involved. It will also bring consistency in consideration of complaints and be less burdensome for consumers than accessing different schemes for each sector.

Further details and specific obligations relating to internal dispute resolution and EDR will be set out in subordinate legislation. These obligations will be developed in consultation with consumer groups and industry to ensure dispute resolution under the SPF is simple and user-friendly.

Consumers can also make a claim in court to recover losses or damages if a business did not meet its obligations. A regulator may also make a claim in court on behalf of consumers with their consent.

The SPF will drive reduced scam losses through a focus on prevention, and where businesses fail to meet their obligations, the SPF will ensure they are held accountable.