auriemma roundtables

September 16, 2025
Re: Request for Information on Potential Actions to Address Payments Fraud

To: Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; and Federal Deposit Insurance Corporation

Submitted via: www. Regulations.gov

Auriemma Roundtables Comment to Request for Information on Potential Actions to Address Payments Fraud

Auriemma Roundtables is a consulting group that hosts roundtables for the top U.S. financial institutions, including roundtables focused explicitly on bank fraud, card fraud, fintech fraud, internal fraud, as well as tangential topics.

To facilitate these confidential discussions with our members, Auriemma Roundtables employs directors who are experienced and knowledgeable in fraud, fraud mitigation, and fraud trends. Further, by hosting roundtables in differing verticals, Auriemma has unique insights into the topics raised by this Request for Information, and we appreciate the opportunity to reply.

Sincerely,

Melissa Meggison,
General Counsel, Auriemma Roundtables

auriemma roundtables

Auriemma Roundtables Comment to
Request for Information on Potential Actions to Address Payments Fraud

Auriemma Roundtables appreciates the opportunity to comment on this Request for Information ("RFI"). As a consulting group that hosts roundtables for the top U.S. financial institutions, including roundtables focused explicitly on bank fraud, card fraud, fintech fraud, internal fraud, and tangential topics, Auriemma Roundtables has unique insights into the current fraud landscape. Using that insight, we offer the following comment, which reflects the opinion and thoughts of Auriemma Roundtables, not its clients:

Comments on the background information listed in RFI

"Payments fraud" RFI definition.

The RFI indicates that "'payments fraud' also includes scams, a subset of fraud." Auriemma Roundtables agrees that scams should be included within the 'payments fraud' topic. However, it should be noted that at many institutions, scam losses (losses that consumers are responsible for) are higher than fraud losses (losses for which financial institutions bear responsibility).

Rises in other types of fraud beyond check fraud

The RFI indicates that "the rise in check fraud is particularly notable." And that "Checks can be stolen, altered, or forged." While those statements are true, two crucial types of check fraud are missing: (a) counterfeited checks, and (b) theft of checking information itself (not just the check) that can be sold online by third parties. Auriemma Roundtables believes that the above issues should be included in future RFI's, guidance, and/or rulemaking to more fully describe the issues at play.

Collaboration, generally

The RFI states, "no agency or private-sector entity can address payments fraud on its own." Auriemma Roundtables agrees with this statement and believes that collaboration is the key to combating payments fraud. As described in more detail below in response to specific questions posed in the RFI, it is Auriemma Roundtables' position that there are other links in the fraud chain, such as social media providers and telecommunications companies, that should be included in collaboration discussions.

Comments to Specific RFI Questions

Question 1: What actions could increase collaboration among stakeholders to address payments fraud?

Fraudsters do not exist in a vacuum. They need tools and channels of communication to carry out their fraudulent activity. Currently, the channels used by fraudsters (e.g., social media companies, telecommunications platforms, search engines, and others) bear no responsibility to prevent fraud. Requiring stakeholders who provide the channels for fraudulent activity to share in the losses would increase collaboration. An example of required collaboration can be found in Australia's Fraud Prevention Framework, attached as Appendix 1 to this comment ("Australia's Fraud Framework").

Additionally, creating communication mechanisms where information can be easily shared across industries and channels would increase collaboration. Currently, there is no easy method to communicate with other stakeholders about known fraudulent activity. For instance, if a financial institution discovers a fake website mimicking it or a social media profile promoting blatant fraudulent activity, it can be challenging to persuade Google, Meta, or similar organizations to take it down. As a result, even when a financial institution knows about the scam, they have no easy path to shut it down.

Question 2: What types of collaboration, including standard setting, could be most effective in addressing payment fraud?

The most effective collaboration would bring in ***all*** links to the fraud ecosystem and require them to remove activity that promotes, recruits, and/or otherwise facilitates payments fraud. "All links" includes social media platforms, telecommunication companies, search engines, payment applications, video hosting sites, and or anywhere else people obtain information. The Australia Fraud Framework, referenced above, provides a roadmap to bring all links in the fraud ecosystem together.

The biggest challenges to creating this type of collaboration are technology, staffing, and a reluctance to share information. These third parties seem to engage in willful ignorance and generally put up a wall of "not my problem" when frauds are raised to their attention.

Meta has argued in federal court that it bears no legal responsibility to address fraud (see *Calise v. Meta Platforms, Inc.* 103 F.4th 732 (9th Cir. 2024)).

The following anecdote may provide additional insight into this issue: an Auriemma director, who is considered an industry expert when it comes to fraud, created an Instagram account to try to combat fraudsters. To do so, he used the hashtags used by the fraudsters to highlight the fraud. The fraudsters complained to Meta (Instagram's parent company) enough that Meta removed the Auriemma director's account, yet all the fraud accounts remained. When the director reached out to Meta, he was advised that Meta doesn't vet its complaints and operates by volume. Since his Instagram account received the requisite number of complaints, it was his account that was removed instead of the fraudsters.

Question 3: *Which organizations outside of the payments or banking industry might provide additional insights related to payments fraud and be effective collaborators in detecting, preventing, and mitigating payments fraud?*

As mentioned above, fraud does not exist in a vacuum; fraudsters use the channels available to them to carry out their activity. The following organizations would be effective collaborators:

- Search engines
- Social media companies
- Telecommunications companies
- Payment platforms
- Video hosting companies (e.g., YouTube and similar sites)
- Merchants

Question 4: Could increased collaboration among Federal and State agencies help detect, prevent and mitigate payments fraud? If so, how?

Increased collaboration among federal and state agencies would help detect, prevent, and mitigate payments fraud because each agency would have greater insight into the latest fraud trends as those trends change. In other words, by collaborating, federal and state agencies would be able to recognize trends faster and utilize information from each other to prevent and mitigate fraud.

Question 5: In general, what types of payments fraud education are most effective and why? Would different audiences (for example, industry and consumers) benefit from different types of payments fraud education?

Generally, real-time/in-the-moment education is the most effective because it stops people who may be about to engage with a scammer in their tracks. However, we believe the best approach is two-fold: mass proactive education to create initial awareness about issues, which is then complemented by in-the-moment education. Proactive education on its own is less effective than in-the-moment education; however, people need to know that the in-the-moment education exists, or it too loses its effectiveness. Proactive, random, "this may or may not happen to you" education is not digested. People (whether industry or consumer) can easily fall for the sense of urgency created in scams; thus it is Auriemma Roundtables' opinion that the key to prevention is an approach that utilizes both mass - proactive education and in-the-moment education.

Additionally, videos and other content related to awareness of scams are often buried within websites. In addition to the in-the-moment education mentioned above, Auriemma Roundtables believes that mass communication, such as commercials on primetime TV, with celebrity spokespeople, would be more effective than the current education practices.

To be effective, education needs to meet people where they are at and should be tailored to different audiences. For instance, when it comes to consumers, a video buried on a website will be far less effective than one on TikTok or another platform. Yet for industry, TikTok may not be effective; LinkedIn or industry publications may be a better solution.

Question 6: Would additional education informing consumers and businesses about safe payment practices be helpful to reduce payments fraud and promote access to safe, secure payment options?

Additional education is essential. However, the real key is about the timing and venues at which the education is communicated, so that people will remember to pause before sending their money. For example, education about spoofing or fraudulent websites would ideally make people wary enough to hit the pause button before they hit the send button.

Question 7: Which approaches could make existing payments fraud education more effective?

As described above, approaches that meet people on the platforms they're using would make education more effective. Additionally, targeting education for specific points in time at which someone is more likely to be subject to fraud would make it more effective.

Question 8: Are current online resources effective in providing education on payments fraud? If not how could they be improved?

No, current online resources are not effective enough in providing education. Current resources are often scattered and hard to find on websites. Instead of educating the masses, current resources only educate the people who seek them out, leaving large swaths of the population uninformed and thus vulnerable to payments fraud.

Online resources could be through proactive outreach on various channels where people consume content (e.g., primetime TV, TikTok, Facebook, YouTube, LinkedIn, etc.). Early education through these channels, before someone is in an in-the-moment situation, can help people hit the pause button before they hit send. Fraudsters capitalize on the sense of urgency. Education should teach people that nothing should be acted on immediately.

Questions 9-15: Regulations and Supervision questions

As mentioned above, regulations that require stakeholders outside the financial services industry to participate in fighting fraud may help mitigate payments fraud. Australia's Fraud Framework provides an example.

Question 16: Broadly, how could payments fraud data collection and information sharing be improved?

Fraud data collection and info sharing could be improved by clarifying whether requests under section 314(b) of the US PATRIOT Act can be used for fraud. If so, this would allow financial institutions to speak to each other to verify transactions and mitigate fraud. At the current juncture, stakeholders have expressed willingness to share known frauds, but it is unclear if the PATRIOT Act allows them to do so. Additionally, creating spaces for limited data collection and exchange (for example, a consortium listing of bad accounts) would improve the process.

Question 17: What barriers limit the collection and sharing of payments fraud data between industry stakeholders, and how could these barriers be alleviated?

Restrictions on info sharing to protect privacy have made it tougher to verify transactions.

Question 18: no response

Question 19: What types of payments fraud data, if available, would have the largest impact on addressing payments fraud? If these data are not currently being collected or shared, what entities are best positioned to collect and share such data?

A list or repository of known fraudulent accounts, names, SSN's, IP addresses and other unique identifiers would have the largest impact.

Question 20: No response

Question 21: No response

Question 22: No response

Question 23-24: No response

Question 25: No response

Thank you for allowing Auriemma Roundtables the opportunity to respond to this request.

Appendix 1

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.

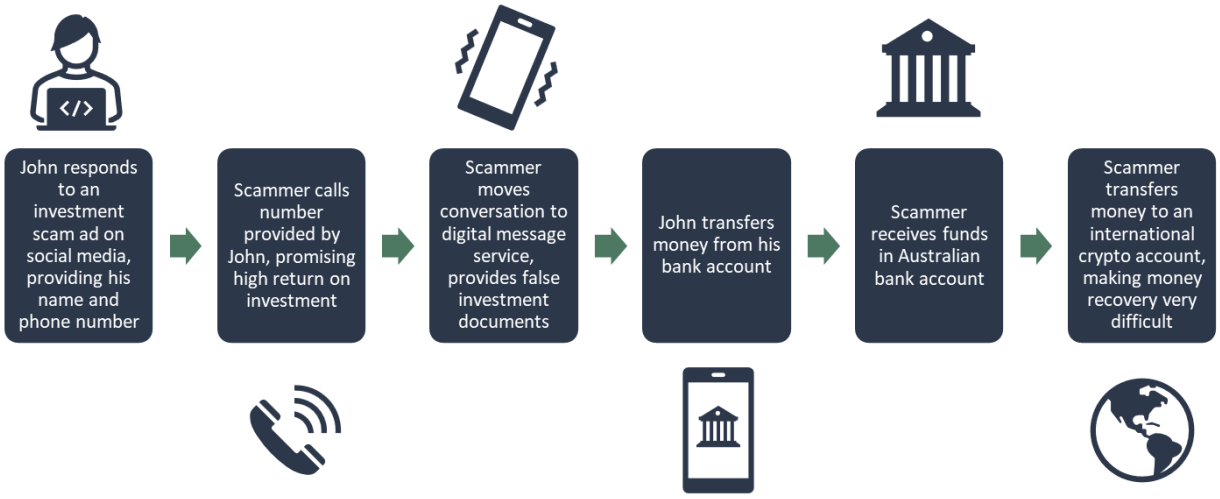
The NASC has brought together the expertise of regulators, law enforcement and industry to stop scammers reaching consumers. Their united efforts are working, with scam losses reported to Scamwatch falling by 41 per cent in the first 12 months after establishing the NASC.

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

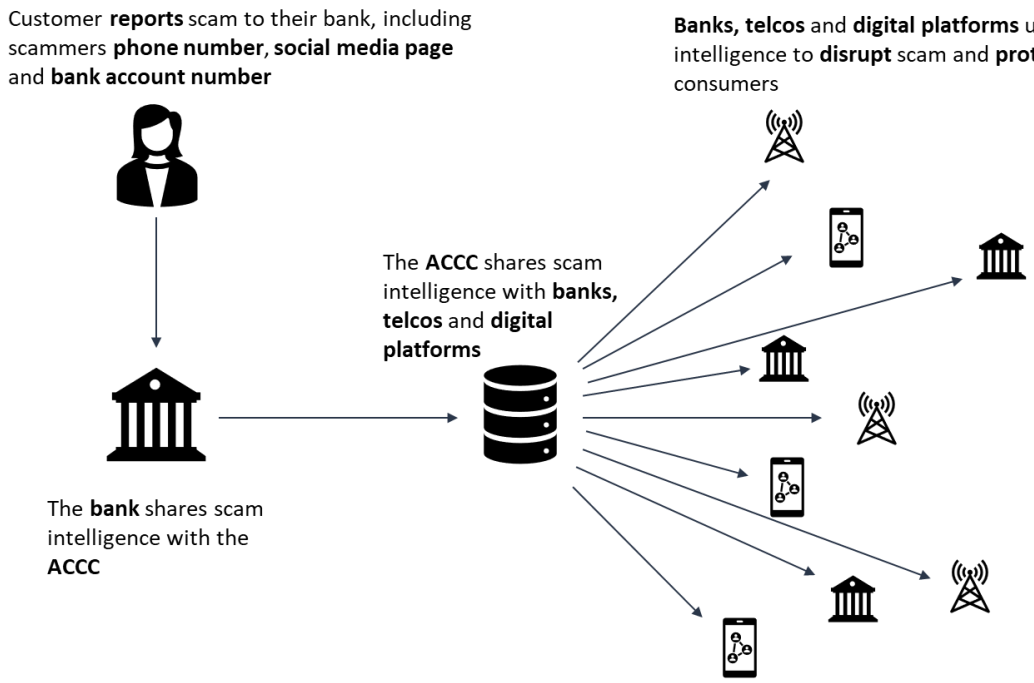
Businesses often only see one piece of the puzzle, which can make it harder for them to prevent and disrupt scams effectively. The SPF will require businesses to share scam intelligence with the ACCC, which will be able to distribute it to other businesses, law enforcement and international partners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