Article Information

Authors: Steven Pettigrove, Luke Higgins
Service: Banking & Finance, Blockchain, Corporate & Commercial, Dispute Resolution & Litigation, Employment & Labour, Estate & Succession Planning, Intellectual Property & Technology, Planning & Environment, Projects Infrastructure & Construction, Property & Development, Restructuring & Insolvency, Superannuation, Taxation
Sector: Financial Services, Government, Health & Life Sciences, Infrastructure, IT & Telecommunications, Private Clients, Real Estate

---

Policing the digital economy: Australia proposes sweeping scam prevention obligations

Australia is stepping up its fight against scams announcing a consultation on legislation to introduce a "Scams Prevention Framework" (SPF), which aims to protect Australians, visitors, and small businesses (defined as SPF consumers) from the threat of scams in the digital economy. With the growing sophistication of scam operations targeting individuals and businesses alike, the Australian government hopes to take proactive measures to disrupt, detect, and prevent scams by imposing new obligations on digital platform and infrastructure providers in key sectors with tough penalties for non compliance.

The SPF is intended as a holistic and agile response to evolving scam threats focusing on industries that the Australian Treasury has identified as key in addressing scam risks. As formulated, the SPF would impose a significant compliance burden on designated sectors to identify and disrupt scams. It represents the latest example of Governments imposing increasing obligations on digital platforms as gatekeepers in policing the digital economy.

Key features of the Scams Prevention Framework (SPF)

The SPF introduces broad protections aimed at safeguarding Australians and businesses by requiring regulated entities to take certain actions against scams. Initially, three service sectors will be designated under the framework and will need to meet several key obligations under the SPF:

- banks;
- telecommunications providers; and
- digital platform services (including social media platforms, paid search engine advertising, and direct messaging services).

Scam Definition and the Nature of Scam Activities

An essential aspects of the SPF is its expansive definition of "scam." Under the framework, the definition intends to capture:

> *"…conduct involving an attempt, successful or otherwise, to deceive the consumer into performing an action that results in a loss or harm to the SPF consumer."*

This broad definition is intended to captures a wide array of scam activities, ensuring that scam attempts are addressed at all stages of their lifecycle. However, there is also concern that its breadth will extend to a wide variety of market

behaviour already regulated under Australian consumer laws and impose a significant burden on regulated platforms to identify conduct that may be labelled deceptive or cause “harm”.

Interestingly, the SPF distinguishes scams from other forms of fraud, such as cybercrime or unauthorised hacking, which do not involve consumer deception but may still lead to unauthorized payments. This distinction focuses the framework on the particular tactics used by scammers to trick victims into compliance.

It is specifically contemplated that the regime will cover scams involving cryptocurrency, loyalty and rewards points.

Obligations for regulated entities

The SPF imposes a number of principle-based obligations on regulated entities to protect consumers at various stages of scam activity. These principles include:

1. **Prevent**: regulated entities must take steps to prevent scams from reaching or affecting SPF consumers. This includes implementing robust systems to block scammers from accessing platforms and services and educating staff and consumers on identifying scams.
2. **Detect**: entities must monitor for potential scams and identify affected consumers. This applies not just to scams in progress but also to previous scams, even if a loss hasn’t yet occurred. For example, banks are tasked with developing processes to flag suspicious activity, such as large cash transactions with new payees, or payments into a crypto-asset.
3. **Disrupt**: entities must take reasonable steps to disrupt suspected scams in progress. This could involve adding friction or validations to prevent the scam from succeeding. The framework includes a 28-day safe-harbour period, allowing entities to take proportionate actions while further investigating scam activities.
4. **Report**: entities are required to report actionable scam intelligence to the Australian Competition and Consumer Commission (ACCC) and, if requested, share scam reports with the ACCC or other regulators. This obligation is likely to sit alongside existing obligations for reporting entities to report suspicious activity to AUSTRAC, the anti-money laundering regulator.
5. **Respond**: entities must provide accessible mechanisms for consumers to report scams and establish internal dispute resolution (IDR) processes. Additionally, all entities covered by the framework must be part of an external dispute resolution (EDR) scheme, such as the Australian Financial Complaints Authority (AFCA), ensuring consumers have independent avenues for redress if they feel their complaints are not adequately addressed.
6. **Governance**: entities must also implement governance policies and procedures to manage scam risks effectively.

Sector-specific codes and regulatory oversight

To address the unique challenges different sectors face, the SPF will introduce sector-specific codes that provide tailored obligations. These codes will be flexible in an attempt to allow adaptation as scam tactics evolve, and will include minimum standards to address sector-specific harms.

The multi-regulator model of the SPF means that the ACCC will oversee obligations in the primary law of the framework and the digital platform services sector, while the Australian Securities and Investments Commission (ASIC) and the Australian Communications and Media Authority (ACMA) will enforce codes for the banking and telecommunications sectors, respectively. This coordinated approach aims to maximise regulatory expertise and ensure a comprehensive, ecosystem-wide response to scam activity. However, it is important that the SPF functions in a way that does not cause unnecessary inefficiencies within the system – for example – in circumstances where administrative processes with one regulator lead to roadblocks in complying with the requirements of another.

The proposal includes tough new penalties for corporates and individuals who fail to implement the principles based obligations to prevent and disrupt scams and applicable industry codes comparable to breaches of civil penalty provisions under other laws.

Future expansion of the SPF

While the initial focus is on banks, telecommunications, and digital platforms, the SPF is designed to evolve over time, with additional sectors expected to be designated in the future. These may include superannuation funds, digital currency exchanges, and online marketplaces.

Conclusion

The SPF is another step in Australia’s increasing efforts fight against scams. The proposal would cast significant responsibility for that fight on platforms in the designated sectors imposing tough new obligations to identify and disrupt scam activity.

The consultation period closed on 4 October. Treasury specifically sought feedback on the compliance burden which would be imposed on industry, and interested parties were encouraged to contribute to the consultation.

As the Government has made fighting scams a key policy priority, it is likely that the SPF will be imposed in some form. Entities that operate within the designated sectors should consider the framework's obligations, and begin preparing to take increasing measures to combat scams in the digital economy.