Deloitte.

Scams Prevention Framework

Deloitte response to exposure draft legislation
4 October 2024

Deloitte.

Deloitte Touche Tohmatsu
Quay Quarter Tower
50 Bridge St
Sydney NSW 2000
ABN 74 490 121 060
www.deloitte.com.au

4 October 2024

Scams Taskforce
Market Conduct and Digital Division
Treasury
Langton Crescent
PARKES ACT 2600

Submission via E-mail

Dear Assistant Treasurer, the Hon Stephen Jones MP, and
Minister for Communications, the Hon Michelle Rowland MP

Deloitte response to exposure draft legislation on Scams Prevention Framework

We are pleased by the recent release of the draft legislation to implement the Scams Prevention Framework (SPF). The SPF is a welcome, necessary and substantial step forward in Australia's response to societal harm from scams.

Deloitte is committed to playing a role in Australia's initiative to reduce societal harm from scams. Deloitte has organised a team to focus on scams consisting of local and global subject matter experts in fraud, identity, financial crime, cyber, privacy and customer response and outcomes. Each of these domains are pertinent not only in their direct relevance to combatting scams, but also with respect to the lessons learned across their maturity journeys.

With that background, we offer insights and opportunities that we see to implement the SPF in a manner that will drive an effective and efficient cross-sector response to scams.

We would welcome the opportunity to further discuss any of our observations as part of the continued consultation process, including providing access to any of our local and global subject matter experts.

Kind regards

LDobbin

Lisa Dobbin
Partner | Australia & APAC Financial Crime Lead
Deloitte Touche Tohmatsu

Mandy Green
Partner | Regulatory Risk & Forensic
Deloitte Touche Tohmatsu

Overall Observations

The principles-based draft Scams Prevention Framework (SPF) published on 13 September 2024 is clearly structured and includes a strong focus on cross-industry collaboration, intelligence sharing protocols, and consumer protection. There are however key areas within the published draft framework that require further clarity, a greater consideration of potential implementation or operational impacts, and provide more detail on the roles and responsibilities of participants in the end-to-end scam value chain. To provide constructive feedback on the framework's overall effectiveness, these points are examined in more detail below.

1. Definition of a Scam

Whilst the published *Summary of reforms* document supporting the draft SPF notes that *the proposed definition is not intended to capture unauthorised fraud,* our concern is that the definition of a scam as referenced in the draft SPF (s58AG) is too broad to be operationally effective in its current form. This is critical as the definition of scams impacts how fraud and scams generally must be managed in regulated industries. As an example, the current definition may force regulated entities to treat all potential fraud cases as scams, until proven otherwise, in order to meet compliance obligations. In financial services, this could result in significant operational, workforce, and expenditure challenges, particularly for institutions outside of the 'Big 4' banks.

In the UK, the definition of scams differentiates between 'authorised fraud' and 'unauthorised fraud.' This distinction helps focus effort and investment towards the unique responses needed to identify and mitigate Authorised Push Payment scams, especially those involving social engineering and victim manipulation. Under the current draft SPF definition, responses to implementing the draft SPF requirements will vary among entities, depending largely on historical investments in data and technology modernisation, counter-fraud detection, and cybersecurity. In our opinion, a more refined definition of scams will help industry participants implement the changes effectively.

2. Cross-Sector Implementation Challenges

The SPF is effectively fast-tracking deep integration of three key industries: financial services, telecommunications and social media. For telecommunications and social media in particular, significant operational, regulatory and privacy challenges are likely to exist when implementing this given their existing fraud prevention, detection and response capabilities are typically more limited in scope and capability when compared to financial services. The cross-border nature of many scams adds additional complexity again, particularly for the social media industry, as platforms must manage scam activities originating from different jurisdictions.

Given this is effectively seeking to achieve something that has not readily been done before in Australia, for this to be effective we encourage government to undertake a consultative co-design process with industry to ensure the legislation is both forward looking in intent (to stimulate cross sector collaboration and technology investment) and functionally achievable given the challenges and limitations that exist currently. To be feasible and effective, the anticipated Sector-specific Codes must be interoperable.

3. SPF – Intelligence, Reporting and Disruption

The draft SPF includes provisions for scams intelligence, reporting, and the disruption of scam networks targeting Australia. Acknowledging that mature banking participants have demonstrated being able to effectively disrupt fraud networks leading to reduced incidents and losses, this approach could theoretically be equally effective in other sectors.

However, developing mature private sector intelligence capabilities capable of disrupting scams demands significant enhancements in workforce skills, systems, and operating models. Many organisations covered by the proposed legislation lack mature intelligence capabilities, with some having no existing capability. From our experience, it takes three to five years to build such capabilities, which may affect an entity's ability to meet regulatory timelines. This must also be considered within Treasury's 'Expected Compliance Costs'.

Real-time sharing of actionable scam intelligence with regulators and ecosystem parties whilst critical to disrupting scams, presents practical challenges. In our experience, one of the primary challenges relates to data formats and ensuring the content of any shared information is actionable and readily ingestible by analytics systems used for this type of detection at speed and scale in an automated manner. Whilst refinement and maturity remain ongoing, this problem has already been solved to a degree by the Australian Financial Crimes Exchange (AFCX). We encourage Government to further consider and clarify the roles that the AFCX and the National Anti-Scam Centre (NASC) will play in collecting and exchanging actionable scam intelligence to facilitate real-time intelligence sharing and avoid duplication.

Importantly, we note that the content and format of intelligence required by industry for fraud and scam detection is markedly different to that used by government in its national security, regulatory and law enforcement intelligence contexts. Approaching the design and implementation of public-private intelligence exchange mechanisms through a traditional government intelligence perspective, without understanding the requirements of industry participants will be ineffective, as demonstrated through the AFCX predecessor, the 'Bank Intelligence Team'[1].

Effective disruption of organised fraud requires more than tactical intelligence reporting of easily replaceable identifiers like phone numbers or email addresses. Successful intelligence disruption must focus on identifying and investigating scam networks, leading to the identification of criminal coordinators and criminally tainted assets suitable for Criminal Asset Confiscation. Targeting intelligence towards scam network controller identification and subsequent asset confiscation is one of the fastest and most effective ways to disrupt organised scams and fraud. Complementing this with targeted financial sanctions through established international mechanisms provides a comprehensive deterrence strategy, as seen in recent global cybercrime cases. We strongly encourage the Australian Government to ensure criminal asset confiscation and targeted financial sanctions are available to it as disruption and deterrence tools in the proposed legislation.

4. SPF – Prevention and the role of Digital Identity

Identity is foundational to ensure trust and confidence in business processes and transactions. Validating that an identity exists and confirming the individual or entity's authenticity is crucial for preventing scams. Data breaches often provide material for large-scale scam attacks, which are becoming more personalised and sophisticated. Authenticating each transaction—whether creating an account, paying for an advertisement on social media, or starting a business interaction—is essential.

[1] A public-private partnership on technology enabled financial crime between the Australian Banker's Association member banks, the Australian Federal Police, and the then Australian Crime Commission).

Digital Identity services, like MyGovID, offer mechanisms to validate parties in transactions without exchanging or storing personally identifiable information. Including biometric identifiers can further verify high-risk transactions or aid data breach victims. The exposure draft of the legislation does not adequately leverage Digital Identity services to mitigate scams. Aligning the draft SPF with applicable legislation[2] could enhance scam prevention for businesses and government agencies.

Crucially, Digital Identity solutions such as MyGovID, should also be available to legal entities, not just individuals. This would enable authentication for activities like booking paid advertisements, which can attract scam victims. Linking a MyGovID account of a nominated employee to a business profile can facilitate this process. Given the numerous initiatives, evolving environment, and modernisation of Australian laws, detailed considerations and impact analyses are recommended.

5. SPF – Detection and Response

The challenge with scams, as with all digital frauds, is the need to see ‘end to end’ from the start of a scam (attack or compromise) through to the point at which an entity has sufficient information on the balance of probabilities to judge a specific action is fraudulent. This involves collecting, integrating, analysing, and responding to potential scams in time to prevent, detect, deter, or disrupt them. Achieving this requires significant investment in data and technology, integrating diverse datasets and systems, and utilising contemporary systems and data environments.

Further, this is not readily achieved with anything but contemporary systems and data environments. This must be considered in Treasury’s ‘Expected Compliance Costs’ – in our opinion, intelligence, detection and response capabilities are likely to comprise the majority of SPF compliance costs, which will be incurred on an ‘ongoing basis’ as regulated entities will need to continually uplift their capabilities in response to the ever-changing threat landscape.

Another critical factor is the tools needed to detect AI-generated voice, video, and text scams, which are becoming increasingly sophisticated. Scammers have been leveraging Generative AI (GenAI) to automate operations and create convincing scams with low risk and cost. GenAI enables impersonation in fake calls, tailored fake investment opportunities, and other criminal activities for even the most unsophisticated, amateur scammer. Given the trend towards full adoption of AI in scam operations, it is essential for the SPF and industry codes to include mandatory AI detection and prevention capabilities. The current draft SPF does not address AI-generated threats, which we see as a significant deficiency.

Most organisations are still maturing in linking their internal customer, transaction, cybersecurity, and fraud detection systems. This maturity journey requires changes in operating models, processes, and workforce, amounting to significant organisational transformation. For telecommunications companies, implementing real-time scam detection and reporting systems poses substantial financial and technical burdens. Smaller providers across all sectors may struggle with the costs of upgrading their systems to meet compliance requirements, potentially leading to market consolidation as smaller players face barriers to entry. Social media platforms face similar challenges with content moderation and scalability and will require substantial investment in automated and manual scam detection systems to fulfil the obligations.

[2] Examples might include the Digital ID Act 2024, Telecommunications Service Provider (Customer Identity Authentication) Determination 2022, Telecommunications Amendment (SMS Sender ID Register) Act 2024, Anti-Money Laundering / Counter Terrorist Financing Act 2006, Identity Verification Services Act 2023, Security of Critical Infrastructure Act 2018, Taxation Administration Act 1953, Superannuation Act 1922, State / Territory Land Titles legislation and others.

Integrating data between businesses in companies regulated under the draft SPF adds further costs and complexity. While we support the proposed SPF Detection and Response requirements, we urge the Australian Government to balance these goals with what is practically achievable with 2024 technology, considering potential unanticipated consequences for telecommunications, financial services, and social media industries and recognise that achieving this outcome may be a medium-long term activity.

6. SPF - Unanticipated Consequences

At Deloitte, we have extensive experience working with clients across the various impacted sectors on compliance, security, and integrity issues. We consider the following points are also worthy of further consideration as part of the SPF implementation.

Market Competition

In Australia, large organisations have markedly more mature capabilities to prevent, detect and respond to scams in comparison to small and medium sized businesses. Increasing compliance costs and the nature of the complex threat environment requires greater expenditure on technology, data and other uplifts required to mitigate these threats. A precursor to effectively preventing, detecting, and responding to a broad range of scam, fraud and cybersecurity threats is modern technology and data infrastructure – many contemporary fraud or scam detection systems don't work on legacy infrastructure. Further, highly capable specialist teams are also required which are both limited in availability on the market and come at significant cost. It stands to reason that not all players currently in the market will be able to bear these costs, or to bear these costs within the timeframe required to either comply with the legislation or remain competitive.

As consumers, we want a competitive, thriving economy which serves the needs of all Australians whilst also protecting Australians from scams. In the current economic environment, achieving both outcomes will require innovative solutions such as shared infrastructure amongst small players in a sector (without breaching anti-competition law). In our view, the SPF should be drafted in a manner that addresses the outcome of reducing scam risk, but which do not adversely constrain or impact market competition or inadvertently drive market consolidation. Noting the importance of cross-sector cooperation and information sharing, Industry Codes applying to those upstream in the scam prevention, detection and response process (i.e., telecommunications and social media) MUST include requirements to collect and communicate the data points required by downstream parties (e.g., banks) to fulfil their SPF prevention, detection and response obligations.

Product and Service Rationalisation

Through the combination of our client work and our expertise, we know that some financial services products and services are considered higher risk to scams compared with others, e.g. typically those which are either older products, not digitally enabled (e.g. accessed through branch interactions), or run on legacy technology infrastructure. We are already seeing financial services organisations review whether products or channels which inadvertently create vulnerabilities to scams need to be closed, and / or whether they remain financially viable on a commercial basis once technology uplifts have been completed to facilitate scam prevention, detection and response.

It is important to acknowledge that as a result of such actions customers could inadvertently be forced onto products or channels which are not their preference, or which may not be fully accessible to them. Further, it is possible that products and services used by vulnerable Australians may be disproportionately affected. As part of the implementation of the SPF, consideration must be given to the consequences of service providers rationalising the breadth and range of services offered to consumers.

Customer de-risking

We saw with the evolution of AML/CTF legislation globally the trend of 'de-risking', where service providers closed customer accounts and offboarded business which posed an increased compliance risk. This practice has been criticised by regulators globally. We are already seeing the same trend occurring as a result of the risk of scams, i.e. where customer sectors who are deemed high-risk are either being offboarded or suffering service degradation.

Whilst it would be hard to help reduce the vulnerability of individual customers, this could feasibly be achieved for small-medium businesses who meet the definition of an SPF Consumer (s58AH). A range of additional resources and training materials should be made available to complement that available through the Australian Cyber Security Centre, so that businesses can easily understand how to assess their scams risk and take steps to better protect themselves, complemented by gentle encouragement under the Corporations Act, partnerships / associations / charity legislation, Australian Government grant terms and conditions, industry licensing, and other similar schemes.