

Scam Prevention Framework

Tata Consultancy Services Response to exposure draft legislation dated 13 September 2024

4 November 4, 2024

About Tata Consultancy Services (TCS)

Tata Consultancy Services (TCS) is an information technology services, consulting and business solutions organisation that has been partnering with many of the world's largest businesses for the past 50 years. TCS is a subsidiary of Tata Sons Private Limited (TSPL) which holds 71.8% in the Company on 30 June 2024. TCS Australia is a unit of TCS and is an Australian entity that provides technology and outsourcing engagements to Australian organisation. We have been in Australia for around 30 years and have an established proven model of delivering services from Australia and nearshore, offshore arrangements.

Our organisation structure is domain led and empowered to help provide customers a single window to industry specific solutions. This is coupled with a unique Global Network Delivery Model™ (GNDM™), spanning 40 global locations, which is today recognised as the benchmark of excellence in technology deployment.

We have over 25,000 associates supporting Australian organisations, 5,000+ of these are based in mainland capital cities of Australia and rest of the teams are working from offshore or near shore. TCS has expertise across an extensive range of technology and business services and receives strong endorsement from its customers.

TCS provides comprehensive financial crime services and solutions to multiple financial services organisations across all regions. These services include regulatory compliance advisory, strategic transformation and future business model design, solution health check, selection, development and deployment, and financial crime managed service. The variety of our engagements and client-led initiatives provide us with multiple opportunities to follow and trigger innovative approaches and concepts that benefit our clients and help us to ensure the services TCS provides are the top class and leading to improvement of the financial crime framework efficiency and effectiveness.

TCS also has a vast network of financial crime alliances. We strive to be technology agnostic helping our clients by defining their economic crime strategic and business requirements first – then, by helping them to choose the best fitting technology. At the same time, by having close relationships with different financial crime technology vendors we can continuously monitor the latest solution trends such as machine learning or artificial intelligence and advise our clients on solutions that best fit their needs.

In addition to our financial crime services, TCS has established a holistic risk management practice including financial risk, emerging risk, resiliency risk, regulatory compliance, enterprise risk and climate risk. Our risk experts and practitioners present multiyear financial services industry experience that comes from many successful run and change initiatives aimed at establishing, maintaining and improving the risk management framework. The financial crime risk management team will work with other risks across the practice to distil the best cross-risk practices and apply them for the benefit of our customers.

Executive Summary

We are grateful for the opportunity to comment on the recently published draft Scam Prevention Framework in Australia. TCS has been closely monitoring both Australian and global innovations in scam detection and prevention and is pleased to see the introduction of the Scam Prevention Framework.

Efforts to combat financial crime involve a combination of legal and regulatory frameworks, enforcement actions and international cooperation. TCS also believes that the development of technology is essential when combating economic crime. Our objective is to provide our clients with the support they need and enable their economic crime framework, maximise their benefits and minimise associated risks.

Financial crime remains a significant global concern. It continuously poses a threat to the stability and integrity of financial systems, as well as the global economy.

The global fraud and scam economy is costing more and more worldwide. With increasing consumer online presence and the use of digital payment methods, scammers and fraudsters target victims online. Today, bad actors have faster access to authorised payments and the ability to move payments through accounts at speed, making recovery more difficult.

Continuously evolving scam and fraud risk demands financial service institutions to constantly re-think their Fraud and Scam Risk Management Controls and look for new business and technology improvement opportunities.

We have observed that Financial Institutions are experiencing an influx in fraud volumes leading to a steady increase in the average fraud losses and spikes in false-positives (with rates of over 97%) putting a strain on existing fraud frameworks. New types of fraud risks are emerging constantly, leading to increased costs and the need for more effective preventative controls, and in-house case management tools are facing issues due to limited functionality, like an inability to report on key metrics accurately, not being leveraged universally throughout the organisation.

The Scam Prevention Framework regime and overarching principles will require significant investment in systems, processes and resourcing by financial institutions. We raise some concerns with the regime below for your consideration.

Scam Definition

The definition of a scam seems broad. The definition casts a wide net, encompassing anything from small scale frauds to sophisticated organised crimes. Different types of scams require distinct strategies for prevention, which is not emphasised in the definition. For reporting purposes, it is important that regulated entities are clear on what constitutes an individual scam, and how to report scams where multiple communications to multiple individuals are involved. There are also inconsistent definitions and classifications of scams across different government and private sector bodies, leading to confusion about how to effectively combat scams.

Failure to Include Complex and Emerging Scams

Scams are becoming more sophisticated and there is opportunity within the framework to address complex issues such as deep fakes, the rise of cryptocurrency fraud, and artificial intelligence enabled scams. Scams in the digital world are evolving rapidly and gaps in legal and regulatory frameworks and gaps need to be addressed.

Inadequate Support for Vulnerable Community Members

Those who are vulnerable in the community, such as the elderly, those with low digital literacy and non-English speakers, are particularly susceptible to scams. The framework focuses on general education that may not sufficiently cater to these populations who often require a more tailored outreach program.

Failure to address the need for a skilled workforce

The governance principle should include a requirement to detail the skills required to maintain an effective scam framework within a regulated entity organisation. A skills matrix should guide how recruitment is performed and is a crucial element to the effectiveness of detection and prevention efforts.

Compliance Certificate

While regulated entities will need to obtain a compliance certification to demonstrate they meet scam prevention standards, there is often insufficient oversight to ensure ongoing compliance. The framework could specify that the senior officer be an executive officer or that the board has sufficient oversight and sign off of the compliance certificate.

Compliance standards may vary across industries leading to inconsistent scam prevention practices. This variation in standards weakens the overall effectiveness of the scam prevention framework. Detailed framework guidelines should be in place to support framework design and operational effectiveness.

Cross Border Scams

Many scams targeting Australians originate from international locations, making enforcement difficult. The framework does not address the challenges of international jurisdiction or cooperation between countries when scams cross borders.

It is also unclear to what extent the regime is intended to apply outside Australia. It would be helpful if the legislation was amended to more specifically set out the intended extraterritorial operation.

Reporting obligations

The reporting obligations on scam activity will be time consuming and resource heavy. It appears that many regulated entities will be required to make large numbers of reports, and it appears that will be duplication with suspicious matter reporting.

It would be helpful if the SPF rules accommodated a concept of periodic batch reporting where appropriate.