Submission to the Senate Economics Legislation Committee: Inquiry into the Scams Prevention Framework Bill 2024

Introduction

My name is Norvan Vogt. I have over 29 years of experience in Information Technology. My expertise is in digital strategy, data governance, and implementing solutions for critical sectors such as healthcare, human services, and government. I have worked on projects that enhance security, improve system interoperability, and promote ethical technology use. Clearly, there is not enough protection against elaborate scams based on information technology for the Australian public. With the advent of easily accessible artificial intelligence legislation put forward in the Scams Prevention Framework Bill 2024 to be more "future-proofed" to protect a dynamic and changing environment. This submission is in response to the Senate Economics Legislation Committee's inquiry into the Scams Prevention Framework Bill 2024. It outlines a strategy to address the growing threats posed by scams in Australia. The approach includes regulatory updates, advanced technology solutions, and industry collaboration. These measures aim to protect consumers, empower industries, and make Australia a global leader in scam prevention.

Adaptive Regulation

The Scams Prevention Framework Bill 2024 must mandate regular reviews of regulated sectors. These reviews, conducted every two years, would ensure that government oversight keeps pace with emerging technologies and industries at risk of scams. Sectors that exhibit high levels of scam activity ought to be included in the regulated category unless exempted by a ministerial decision. Examples of areas requiring attention include AI-driven marketplaces, cryptocurrency exchanges, and decentralised finance (DeFi) platforms. (Greer & Trump, 2019). Dynamic evolution of Sender Policy Framework (SPF) codes is also essential. These codes ought to adapt to new threats with input from industry stakeholders, technology experts, and consumer advocates. The framework must include provisions allowing industries to deploy temporary measures to address urgent scam-related risks while ensuring accountability.

Advanced Detection Technologies

The Bill ought to require regulated entities to adopt real-time monitoring technologies powered by artificial intelligence. These tools would detect patterns of fraudulent behaviour, such as phishing attempts and unauthorised financial transactions. Sector-specific benchmarks ought to ensure consistency and effectiveness (Ma et al., 2023). For example, banks must meet minimum standards for fraud detection speed and accuracy, while digital platforms ought to use algorithms tailored to counter scams on their networks. Small businesses face significant cost barriers when accessing advanced technologies. To address this, the Bill ought to include provisions for shared platforms that enable small organisations to utilise sophisticated scam detection tools affordably. This approach would ensure that protections extend to all segments of the economy.

Proactive Threat Identification

The creation of a centralised scam database is a crucial element of the Scams Prevention Framework. This database ought to be operated by the government and accessible to the public and regulated entities. Machine learning could analyse the data to identify patterns and trends in scam activity and highlight demographics most at risk.
Mandatory information sharing between high-risk sectors is also essential (Lu et al., 2020). The Bill ought to facilitate collaboration between entities such as banks, telecommunications providers, and social media platforms. For example, banks could share data on suspicious transactions with telecommunication providers to block associated scam calls. Public-private partnerships ought to be encouraged to fund research and develop innovative tools, such as fraud detection systems for social media platforms.

Innovative Response Mechanisms

The Scams Prevention Framework ought to establish a victim support fund. This fund, financed by levies on regulated entities, would provide compensation to scam victims and support recovery initiatives, including counselling services. Businesses ought to also have opportunities to test new scam-prevention tools in controlled environments. These "regulated sandboxes" would enable companies to innovate without facing penalties for unproven solutions. This approach encourages experimentation while safeguarding consumers.

Sector-Specific Customisation

The Scams Prevention Framework must reflect the unique risks and needs of different industries. Sector-specific codes ought to be developed to address these variations. For instance, banks could strengthen customer verification processes for high-value transactions (Squicciarini et al., 2013). Telecommunications companies could implement caller ID authentication for all outbound calls. Social media platforms ought to enhance content moderation to detect and remove scam advertisements. The framework ought to also prioritise targeted protections for vulnerable groups, including seniors, small businesses, and rural populations. Customised measures for these groups would help ensure that protections are effective and equitable.

Continuous Education and Awareness

Education and awareness are vital components of scam prevention. The Bill ought to include provisions for national campaigns to educate consumers on recognising and responding to scams. These campaigns ought to utilise television, radio, social media, and print media to reach a diverse audience (Gao & Jiang, 2016). Scam prevention materials must be inclusive. Resources ought to be available in multiple languages and accessible to non-digital populations through phone hotlines and community outreach programs. Materials ought to also cater to people with disabilities, using formats like easy-read guides and sign language videos. Real-time alerts, delivered via SMS or push notifications, would help warn consumers about ongoing scams targeting specific platforms or demographics.

Global Collaboration and Integration

Scams are increasingly operating across borders. The Scams Prevention Framework must include provisions for international collaboration. Data-sharing agreements with foreign regulators and law enforcement agencies are essential for tracing and blocking cross-border scam networks. Agreements with global financial hubs could also allow authorities to freeze scam-related transactions in real time. Australia ought to strengthen its participation in global initiatives, such as partnering with Interpol and international fraud prevention networks. Aligning national regulations with global cybersecurity standards will ensure compliance from foreign businesses operating within Australia (Daiku et al., 2020).

Conclusion

This submission highlights the need for the Scams Prevention Framework Bill 2024 to adopt a comprehensive and adaptive approach to counter the evolving threat of scams. By integrating adaptive regulation, advanced detection technologies, sector-specific measures, and global collaboration, the Framework can protect consumers, empower industries, and position Australia as a global leader in scam prevention.

Thank you for considering this submission. I am available to provide further input or clarification on the recommendations.

Norvan Vogt

Sources:

Daiku, Y., Kugihara, N., Teraguchi, T., & Watamura, E. (2020). Effective forewarning requires central route processing: Theoretical improvements on the counterargumentation hypothesis and practical implications for scam prevention. PLoS ONE, 15.
Gao, W., & Jiang, Z.-P. (2016). Adaptive Dynamic Programming and Adaptive Optimal Output Regulation of Linear Systems. IEEE Transactions on Automatic Control, 61, 4164–4169.
Greer, S., & Trump, B. D. (2019). Regulation and regime: The comparative politics of adaptive regulation in synthetic biology. Policy Sciences, 52, 505–524.
Lu, H., Chan, S., Chai, W., Lau, S. M., & Khader, M. (2020). Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. Crime Prevention and Community Safety, 22, 313–330.
Ma, K. W. F., Dhot, T., & Raza, M. (2023). Considerations for Using Artificial Intelligence to Manage Authorized Push Payment (APP) Scams. IEEE Engineering Management Review, 51, 166–179.
Squicciarini, A., Petracca, G., & Bertino, E. (2013). Adaptive data protection in distributed systems. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 365–376.