Scam Risk Management:

The Path to Regulation in Australia and the Response By Global Banks

Scams are a persistent issue in Australia and globally, affecting individuals and businesses alike. Reports of scams have surged over the years, with Australians losing billions annually. This **International Fraud Awareness Week** (17-23 November 2024), we look at the difference between fraud and scams, who is most vulnerable and the shift towards regulated scam risk management in Australia. We also explore how global banks are preventing and detecting scam payments, highlighting common gaps and a bank 'wish list' to improve scam management.

What is the Difference between Fraud and Scams?

In simple terms, fraud is unauthorised, whereas scams are payments processed by customers.

Fraud: Involves unauthorised access to accounts (e.g., identity theft) and is covered by the ePayments Code in Australia.[1] Banks usually compensate customers for these losses, with some offering a "fraud money-back guarantee."

Scams: Customers are duped into making a payment, believing it to be valid. As these payments are authorised, customers in Australia typically incur the scam loss.

Who is Most Vulnerable to Scams and How?

In 2023, Australians lost a reported $2.7 billion[2] to scams according to the Australian Competition and Consumer Commission ('ACCC'), who identified the following scam trends:[3]

Older Australians suffered most harm from scams

This was mainly from investment scams, with people over 65 reporting $120 million in scam losses - 13.3% increase from 2022.

Most common contact methods by scammers

- Phone calls - $116 million lost
- Social media - $93.5 million lost
- Text messages - 37.3% increase from 2022

Job scams led to $24.3 million in losses

Individuals disproportionally targeted for fraudulent work were those:

- from culturally or linguistically diverse communities
- seeking part-time work or additional income to alleviate cost of living pressures.

How is Scam Risk Management in Australia Becoming a Regulatory Regime?

In April 2023, the **Australian Securities and Investments Commission ('ASIC') issued their Report 761**[4] into scam prevention, detection and response by the four major banks. ASIC followed this up in August 2024 with **Report 790**[5] looking at anti-scam practices of 15 banks outside of the four majors. Interestingly, these reports found banks consistently lacked a fully documented scam strategy, the ability to delay potential scam payments, coherent approaches to determining liability and prompt responses to scam victims. Many banks have been working to respond to ASIC's findings.

In response to escalating scam losses to Australians, in May 2023 the Australian Government announced an $86.5 million budget package to combat scams and online fraud, with the establishment of the **National Anti-Scam Centre** ('NASC') in July 2023.[6]

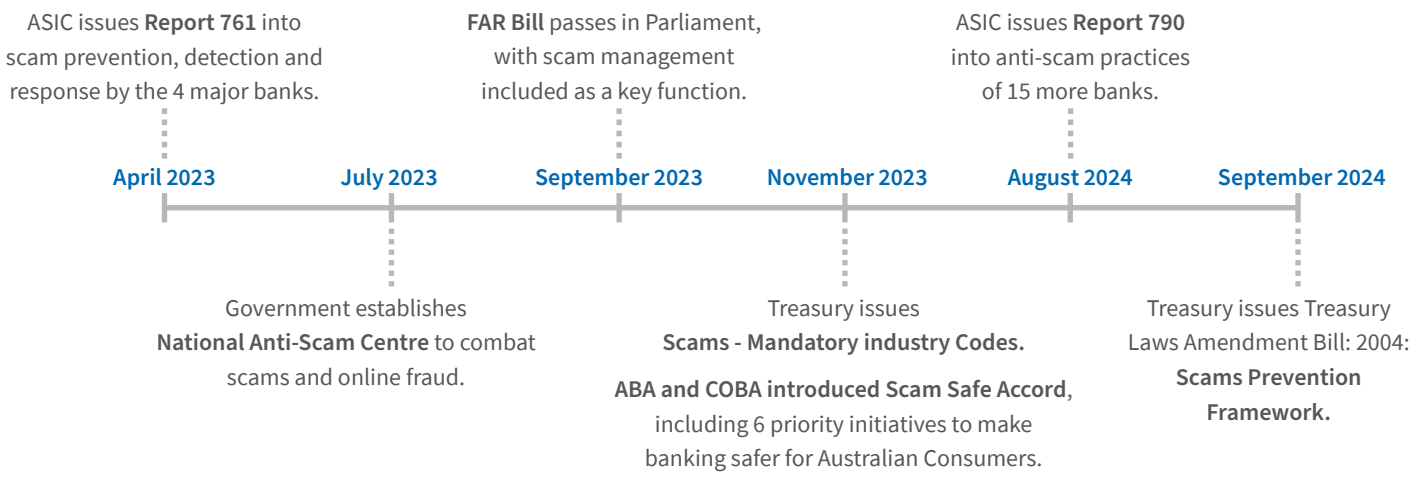
In September 2023, the **Financial Accountability Regime ('FAR') Bill**[7] was passed in Parliament. Scam management was included as a Key Function requiring an Accountable Person to have *"primary conduct of, or key decision-making power in relation to, the overall development, maintenance, oversight, review or execution of one or more aspects of"* scam management.[8] Directors and senior executives of Australian Prudential Regulation Authority ('APRA') regulated entities may be financially sanctioned, having at least 40% of their variable remuneration deferred for a minimum period of 4 years for any non-compliance with their accountability obligations.[9] There will be reporting obligations, especially for entities above a certain threshold in the form of accountability statements and accountability maps.[10]

In November 2023 and September 2024, **Treasury issued a Scams Mandatory Industry Codes** and a **Treasury Laws Amendment Bill: 2024: Scams Prevention Framework** respectively, setting out proposed changes to enhance governance, prevention, detection, reporting, disruption and response efforts against scams, including:[11]

- Introducing a wide-range of protections for Australians, visitors to Australia and Australian small businesses with fewer than 100 employees.
- Imposing mandatory obligations on initial designated sectors: banks, telecommunication providers and digital platform services (initially, social media, paid search engine advertising and direct messaging services). These obligations will be tailored to scam activity relevant to these designated sectors.
- Penalties for non-compliance of up to $50 million for entities and $2.5 million for individuals, as well as establishing pathways for consumers to be compensated for being scammed.
- A multi-regulator approach to enforcement, with the Scams Prevention Framework administered and enforced predominately by the ACCC, but also ASIC and the Australian Communications and Media Authority ('ACMA').

The proposed legislation changes include a mechanism to enable expansion to other sectors. For example, superannuation funds, digital currency exchanges and other payment providers, given scammers target customers through these channels. The Australian Government is seeking stakeholder feedback on the proposed changes and considering its assessment of the privacy and compliance cost impacts of the proposed framework.

The Regulatory Path for Scam Management in Australia



How are Global Banks Effectively Preventing and Detecting Scam Payments?

As scam risk management moves towards a regulatory regime, many banks, telecommunications and social media providers in Australia are not waiting for the legislation but are enhancing efforts to uplift their Scam Prevention Framework in line with the expectations in the ASIC reports and draft legislation.

Banks globally are already using a number of effective approaches to prevent and detect scams, including:

Scam Prevention

Payment profiling

Used to pause or block transactions, but some banks won't stop the payment from being processed.

Risk-based bank intervention

Contacting the customer and delaying processing the transaction.

Real-time inbound monitoring and blocking of mule accounts

Controlled by scammers to wash and withdraw scam monies.

Preventing transfers to crypto-exchanges

Blocking transfers above a certain value to cryptocurrency exchanges.

Scam Detection

Use of AI

Authorised fraud modelling for detection and behavioural biometrics .

Improved dynamic warnings

Killing the scam payment journey.

Real-time network analysis and modelling

Identifying mule accounts/ inbound scam receipts detection.

What are the Gaps in Banks' Scam Prevention Efforts?

Globally, FTI Consulting has identified several common gaps:

- Not all banks are doing scam risk assessments.
- Lack of detection rules specific to scam modus operandi ('MO').
- Absence of real time network analysis.
- No monitoring to identify if customers are on the phone whilst banking.
- Insufficient protection against bank brand spoofing by scammers.
- Missing orchestration layers to aggregate risk scoring for scam transaction monitoring technologies.
- No monitoring of operating costs to manage scams.
- Failure to identify customers vulnerable to scams and tailor responses accordingly.
- Deep fake and bank spoofing customer awareness and detection. This is particularly important as digital account opening, often done with a selfie, may be susceptible to being deep faked. Bank spoofing techniques are becoming more sophisticated, with scammers replicating bank hold music and recorded messages. More customer education is needed to help prevent these scams.
- Many banks are manually gathering data points from different sources and deploying large scale fraud operations teams. This is instead of using more automated and AI-Powered investigations to improve the effectiveness of pulling together disparate data points, guide alert handlers and draft preliminary case findings.

How are Banks Globally Seeking to Enhance Their Fight Against Scammers?

Banks have outlined a wish list of potential game changers, including:

— Consortium data sharing, seen as critical, with an integrated payment network to identify threats and enable destination account monitoring.

— More engagement by social media platforms. Currently the banks report payment scams to the platforms, but there is room for improvement with more proactive monitoring by social media platforms to identify and block scammer accounts and activity.

— Consideration of a "cooling off" period before recipient banks release funds that wash through accounts. Faster payments have resulted in challenges with scam monies quickly washing through mule accounts and offshore, making recovery challenging. The ability to slow this down would assist in scammed monies recovery.

— A government campaign on scam awareness akin to the 'Slip, Slop, Slap' historic skin cancer awareness campaign to help educate the public and 'break the spell' of the scam. Banks are launching scam awareness campaigns, however acknowledge that individuals who don't bank with them may disregard the messaging. Hence the need for an impactful scam awareness campaign by government.

— The ability to report scam MOs globally, with more information sharing on typologies coming down the line. Scams often start in one market and if proven effective at generating income, are rolled out globally as part of the scammers' business model. Facilitating global information sharing would enable banks to better tailor awareness campaigns and transaction monitoring systems, enhancing their ability to prevent and detect emerging scam typologies.

How FTI Consulting Can Support Your Scam Risk Management

FTI Consulting brings decades of experience in helping organisations prevent and detect fraud and scams. Our team assists with uplifting your scam operating models, undertaking enterprise-wide, business area or product-focused scam risk assessment. We also assess and help you comply with scam regulation and frameworks. Contact Natalie Faulkner below for more information.

[1] ePayments Code, ASIC, 2 June 2022

[2] Scam losses decline, but more work to do as Australians lose $2.7 billion, ACCC, 28 April 2024

[3] ibid

[4] Scam prevention, detection and response by the four major banks, ASIC, April 2023

[5] Anti-scam practices of banks outside the four major banks - Report 790, ASIC, August 2024

[6] ACCC welcomes funding to establish National Anti-Scam Centre, ACCC, 15 May 2023

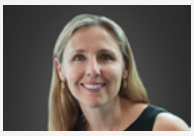
[7] Financial Accountability Regime Bill 2023, Australian Government, 14 September 2023

[8] ADI Key Functions descriptions, (Key Function 14 relates to scam management), APRA, March 2024

[9] Financial Accountability Regime Bill 2023, Australian Government, 14 September 2023

[10] ibid

[11] Scams Prevention Framework, Summary of Reforms, The Treasury, Australian Government, September 2024



NATALIE FAULKNER
Senior Managing Director
+61 412 076 877
natalie.faulkner@fticonsulting.com