Piper Alderman

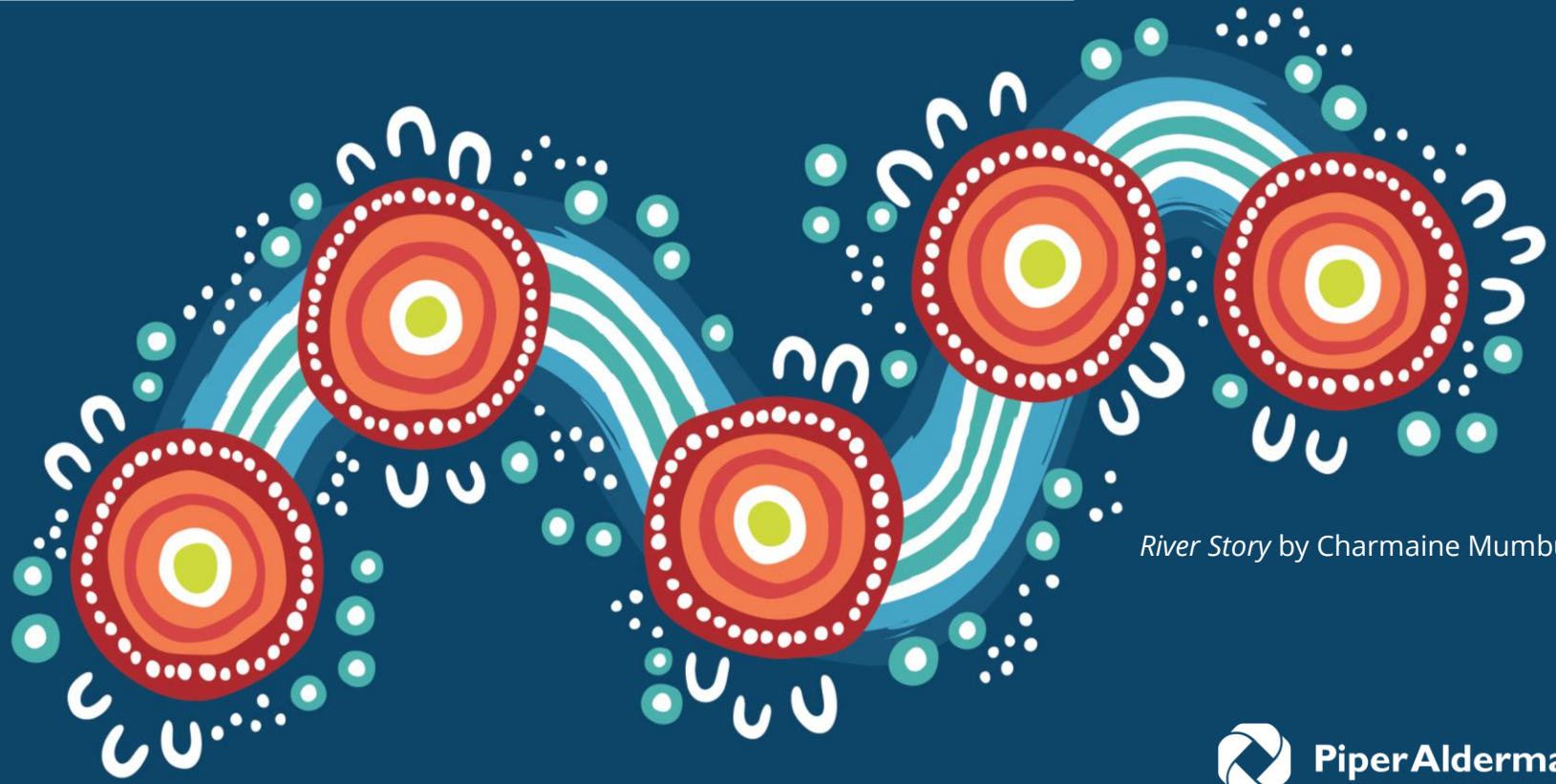
Unveiling the Scam Epidemic - Australia's Fight Against Fraud

Legalwise Australian Cybersecurity Summit

13 June 2024

Andrea Beatty

Acknowledgment of Country



River Story by Charmaine Mumbulla

Piper Alderman

Today's Session

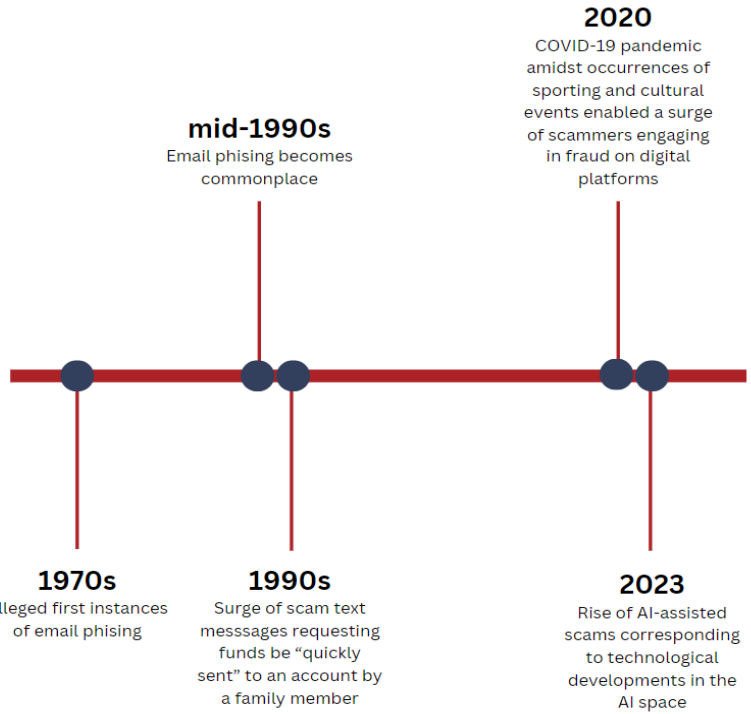
- Background of the scams landscape in Australia and the current epidemic of scams
- Recent initiatives of the Australian Government to address scams
- Global governmental and legislative responses to scams
- The proposed introduction of a new Scams Code Framework in 2024 including:
  - describing the role of the Scams Code Framework and how this addresses scams;
  - key features and proposed obligations of the Scams Code Framework; and
  - the impact of the Scams Code Framework on different industries

Piper Alderman

The Australian Scams Landscape

Piper Alderman

Scams: An Overview

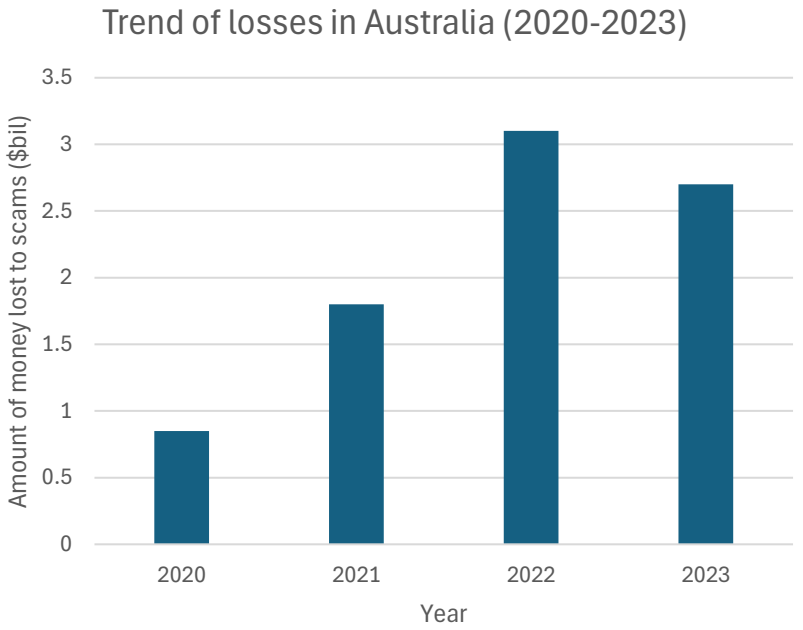


- ➔ Scammers are able to adapt in line with advances in technology
- ➔ The most prolific types of scams include phishing, false billing and online shopping scams and were mostly delivered by text message
- ➔ The types of scams that cost Australians the most include investment scams, dating & romance, and false billing and were mostly delivered by telephone communication
- ➔ Individuals aged 18-24 years are more likely to fall victim to scams than other age groups, with most instances and losses taking place on Facebook and Instagram. In 2023, Australians lost $93.5 million to scams initiated through social media platforms such as Facebook Marketplace

PiperAlderman

Trend of losses in Australia

- Scam activity was reported to have peaked in 2022
- In 2022, scams resulted in financial losses totalling at least $3.1 billion, representing an 80% increase on losses recorded in 2021
- In 2022, 65% of Australians (i.e.,13.2 million people) were exposed to a scam attempt, with scammers no longer discriminating between ages, digital assets or digital platforms
- Scam activity slightly decreased in 2023 to a total of $2.74 billion, likely due to collaboration between government entities, law enforcement, consumer organisations and industry groups – however, this is still a 320% increase since 2020



PiperAlderman

Scams: An Overview (Cont.)

- Scammers and scams are posing a growing threat to Australian consumers and businesses. The increasing technological prowess of scammers has allowed them to evolve, exploit new vulnerabilities, and employ novel methods, to deceive businesses and consumers
- With the rise of AI technology, scammers have now used voice cloning and deepfake videos to create more sophisticated scams, for example, using data to create a persona of an individual to impersonate them on live video calls
- Scammers are often based overseas, with the top scamming countries being Nigeria, India, China, Brazil and Pakistan
- The impacts of scams are not restricted to direct financial loss and emotional or psychological stress associated with being a victim of a scam, but also costs associated with recovery of moneys lost, data loss, reputational loss for the affected entity and overall industry, and disruptions to normal business operation

Scams: Financial Services

- COVID-19 pandemic accelerated the use of digital banking channels such as bank mobile apps or digital payment platforms by 29%, which has also enabled new forms of scams occurring
- The sharp decline in individuals using cash for in-person transactions and the shift towards online banking (with 80% of Australians reported to prefer using digital banking services) is a key driver of the proliferation of online fraudulent activity since 2020
- In 2023, although less than 3% of reported scams were investment scams, they accounted for 61% of reported losses at $292 million
- The Australian Banking Association (**ABA**) is working with the Australian Financial Complaints Authority (**AFCA**) and other regulators to ensure legislation is up-to-date with technological developments and evolving scams
- Know-your-customer (**KYC**) failures are the most disruptive issue in the financial services sector, with identity theft and synthetic identity theft on the rise despite growing regulatory scrutiny

Common types of scams encountered in the banking sector

Bank scams refer to the wide range of schemes employed by cybercriminals to steal an individual's money or financial information

Investment Scams
Where scammers entice individuals into investing funds (usually a substantial amount) into schemes which promise high returns and extremely low risk

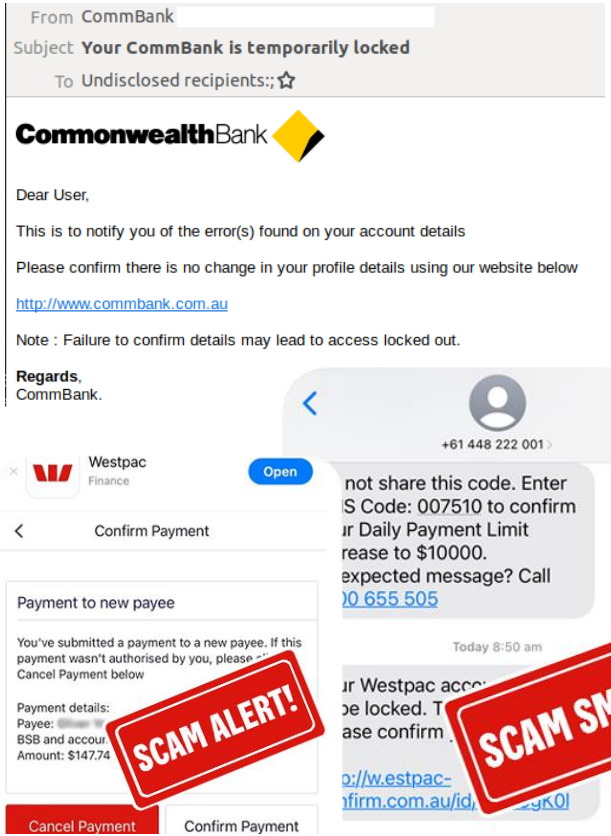
Phishing
Where scammers use text and emails to trick individuals into providing personal information, such as passwords and account numbers, so that they can access personal accounts

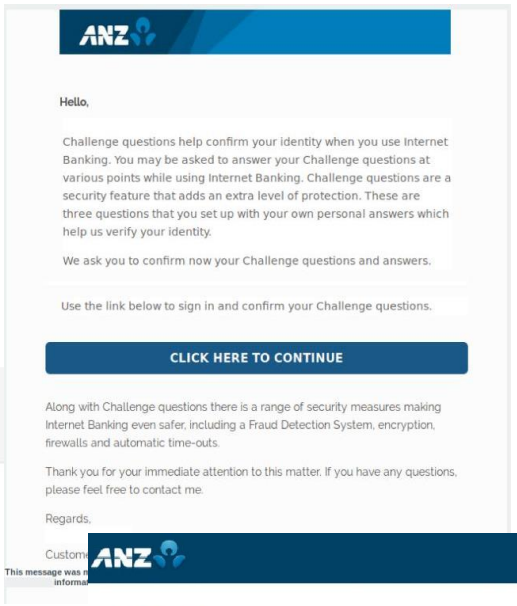
Impersonation Scams
Where a scammer makes direct contact with an individual by impersonating a bank to gain access to the individual's personal information and/or money

Identity Theft
Where a scammer extracts or gains access to personal documents to steal an individual's identity, allowing them withdraw money or apply for financial products in the victim's name

Piper Alderman

Examples of banking scams





Case Study: Tim Watkins

- ➔ Watkins received a SMS message in a thread with other correspondence from his bank stating that $850 had been withdrawn from his account
- ➔ Watkins was provided with a number to call if he didn't make the transaction
- ➔ Watkins called the number, spoke with someone who claimed that they worked at the bank and followed instructions to protect his account
- ➔ He was provided with a one-time code which allowed scammer to access his NAB account
- ➔ Money was stolen over 10 transactions, totalling $222,000

Piper Alderman

Case Study: FACC

- Fischer Advanced Composite Components AG (**FACC**) is an Austrian aeronautics company
- In 2016, hackers posed as FACC CEO, Walter Stephan, in an emailing requesting an employee of FACC's financial department to transfer 50 million euros to an account in relation to a fake acquisition project
- The account was an attacker-controlled bank account
- Whilst FACC was able to stop the transfer of 10.9 million euros, the rest of the money had already disappeared into Slovakia and Asia
- Not only did the scam cause a direct financial loss to FACC, but it caused an additional operating loss of 18.9 million euro compared to the prior year
- FACC's share price also plummeted by 17% due to decreased market confidence resulting from reputational damage

Piper Alderman

Case Study: Arup

- Arup is a leading British consulting engineering firm
- In January 2024, an employee received a phishing message regarding a "confidential transaction" from an individual claiming to be Arup's UK-based chief financial officer (**CFO**)
- The employee then joined a video conference call, where deepfakes impersonated the CFO and other senior managers, and was convinced to make 15 transfers totalling $200 million Hong Kong dollars (i.e., approximately $37 million Australian dollars) from company funds to five separate Hong Kong-based bank accounts
- Scammers likely used deepfake technology to modify publicly available video footage and audio recordings and digitally create the demeanour, appearance, and voice of the CFO and senior managers known to the employee

Piper Alderman

Recent Government Initiatives

Piper Alderman

Current regulatory framework for scam-prevention

- ➔ Presently, there is no comprehensive regulatory framework that clearly delineates the roles and responsibilities of the government, regulators and the private sector in combating scams
- ➔ Scam-prevention measures vary across industries and there is a lack of collaboration between the government, regulatory bodies, law enforcement, and importantly, between sectors themselves
  - ❖ Not all sectors have industry codes to outline its responsibilities in relation to preventing scam activity
  - ❖ Currently, there are no specific requirements on banks and digital platforms to address scams
  - ❖ The lack of coherency between treatments of scams across stakeholders means that efforts to respond to scams are siloed and irregular
- ➔ To date, the current framework has been inadequate in dealing with the complexities of modern scams and requires further enhancements

Piper Alderman

Involved government and regulatory bodies

- Australian Banking Association (**ABA**)
  - Launched an industry-led 'Scam-Safe Accord' outlining the anti-scam measures which will be implemented across the banking sector to target and respond to scams
- Australian Competition and Consumer Commission (**ACCC**)
  - Leads the National Anti-Scam Centre
  - Conducts ongoing work and reporting as part of the Digital Platforms Services Inquiry
- Australian Communications and Media Authority (**ACMA**)
  - Launched and maintains the SMS Sender ID Registry
  - Enforces the Reducing Scam Calls and Scam Short Messages (SMs) Code in relation to telecommunications providers
  - Provides de-identified consumer complaint data to telecommunication providers to assist with industry efforts to identify and disrupt scams

Piper Alderman

Involved government and regulatory bodies (Cont.)

- Australian Financial Complaints Authority (**AFCA**)
  - Handles complaints, including those arising from a breach of legal requirements
  - Considers breaches of industry and voluntary codes
  - Determines whether compensation can be paid by financial firms to consumers for direct loss or damage caused by the firm's breach of obligation
  - Assists with claims for direct financial loss
- Australian Securities and Investments Commission (**ASIC**)
  - Collaborates with the Government to identify and take down investment scam websites
- National Anti-Scam Centre (**NASC**)
  - Manages the ScamWatch website to assist with coordinated intelligence-sharing and action to combat scams
  - Collaborates with the Australian Financial Crimes Exchange (AFCX) and other key businesses to better coordinate information-sharing

National Anti-Scam Centre

- Aim is to enable sharing of scams intelligence across government, law enforcement and private sector
- Disruption initiatives:

ASIC's website takedown service

Bank action on cryptocurrency exchanges

Scam indicator tool and payment prompts

PiperAlderman

National Anti-Scam Centre

The ACCC-led National Anti-Scam Centre was established to coordinate experts from government, law enforcement and the private sector to disrupt scams and raise consumer awareness

- ➔ Leverages collective expertise and intelligence across government, law enforcement, industry and consumer groups to disrupt scams, empower consumers and find solutions to scam prevention
- ➔ Collects scam reports and monitors losses through the ScamWatch reporting service
- ➔ To facilitate ASIC's website takedown service, the National Anti-Scam Centre identifies and shares the URLs from investment scams reported to ScamWatch or identified by the National Anti-Scam Centre and its partners to ASIC for removal

ASIC's Website Takedown Service

ASIC has engaged in activities to identify and shut down investment scam websites, and has currently removed 2,500 websites between July 2023 and November 2023

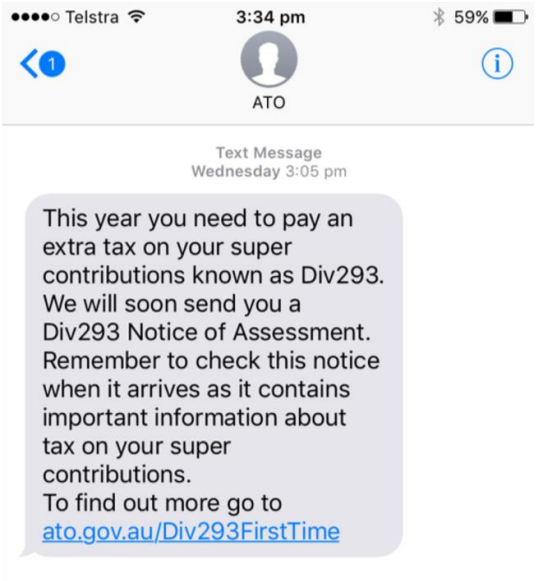
- Between July 2023 and December 2023, ASIC disrupted scam activity by initiating the removal of more than 2,500 investment scam and phishing websites
- The types of scam websites targeted by ASIC include fake investment platforms, crypto-asset scam websites and imposter scam websites which impersonate legitimate financial services businesses
- ASIC is focussing on investment scams in light of the current cost-of-living crisis, where individuals are more vulnerable to scams which promise an often-easy way to 'make ends meet'
- ASIC has coupled this capability with an investor list which highlights suspicious entities to help inform consumers

Piper Alderman

Sender ID Registry

ACMA is working on Australia's first SMS Sender ID Registry to prevent scammers from imitating trusted industry/government brand names

- Registry protects alphanumeric message heads (e.g., ATO, MyGov, NAB) from SMS impersonation
- Participating telcos include Telstra, Optus, TPG Telecom and Pivotel – past 15 months, reported blocking 336.7 million scam SMS under ACMA-registered rules
- Pilot launched on 15 December 2023 with CBA and NAB as its participating brands
- Voluntary pilot phase will test operation and effectiveness of Registry before Government moves towards finalised scheme in 2024, involves consolidating existing sender ID protections with well-known brands and agencies



PiperAlderman

Scam-Safe Accord

ABA launched a new Scam-Safe Accord on 24 November 2023, outlines a comprehensive set of anti-scam measures across the banking industry

- ➔ Collaboration between Australian community owned banks, building societies, credit unions and commercial banks
- ➔ Measures include a new confirmation of payee system, warnings and delays to protect customers, expansion of intelligence sharing across the sector, and limiting payments to high-risk exit channels
- ➔ The confirmation of payee system is an $100 million investment by the banking industry to help reduce scams by ensuring individuals can confirm that they are transferring money to the intended recipient, and will be rolled out over 2024 and 2025
- ➔ The Scam-Safe Accord includes a major expansion of intelligence sharing across the banking sector, where banks will act on scams intelligence from AFCX and join the Fraud Reporting Exchange

New Mandatory Industry Codes

$67.5 million in 2024-2025 Budget

Outlines the responsibilities of the private sector in relation to scam activity.

Governments will provide regulators $37.4 million to administer and enforce industry codes

$12.4 million for ACMA over 4 years to oversee the review and improvement of existing processes and boost enforcement action

Focus on banks, telecommunication providers and digital platforms

Require groups to have measures in place to prevent, detect, disrupt and respond to and report scams

Piper Alderman

The Scams Code Framework

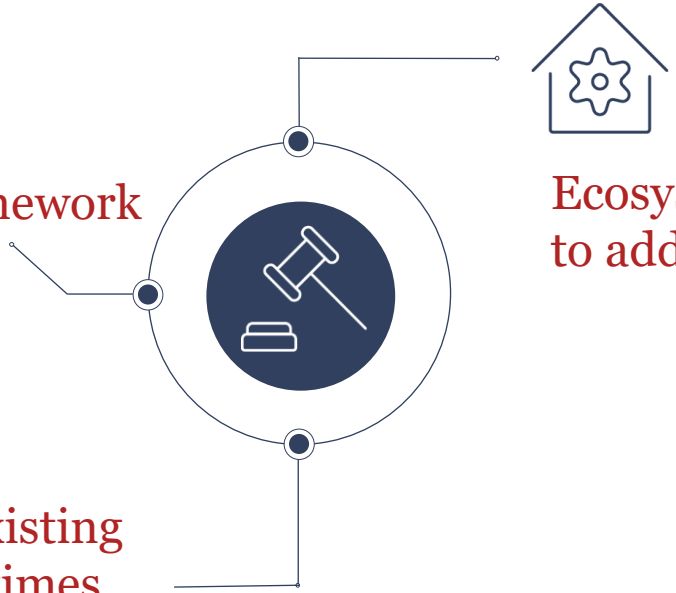
Piper Alderman

Proposed Scams Code 2024 – General

‘Scams – Mandatory Industry Codes’ – Consultation Paper

- On 30 November 2023, the Treasury released the ‘Scams – Mandatory Industry Codes’ Consultation Paper
- The Government pledged to introduce a new overarching scams framework and mandatory industry codes
- The primary objective of the proposed Scams Code Framework is to define distinct roles and responsibilities for the government, regulators and the private sector in tackling scams
- This involves ensuring that critical sectors implement measures to prevent, detect, disrupt and respond to scams, including the sharing of scam intelligence between sectors
- The banking, telecommunications and digital platform sectors have been specifically identified as the initial focus point for this implementation, as they are targeted most by scammers
- Superannuation and cryptocurrency sectors will be prioritised in subsequent phases, given the volumes of retail funds held in the superannuation system and the potential for digital asset platforms to provide a gateway for scam transactions (especially through cryptocurrency)

Guiding Principles of the Scams Framework



Flexible and responsive framework

Ecosystem approach to address scams

Complement existing interrelated regimes, systems and initiatives

Piper Alderman

Principle 1: Flexible and responsive Framework

- The Framework is to be sufficiently flexible and responsive to address the following matters:
  - scammers are prone to shifting their attacks on less regulated areas, such as cryptocurrency, within the scam ecosystem;
  - scammers are likely to leverage advancements in technologies and markets to devise new types of scams and harms;
  - scammers are likely to act fast when a new and emerging type of scam or harm is devised; and
  - differing nature and sizes of regulated businesses

Principle 2: Ecosystem approach to address scams

- A comprehensive and coordinated regulatory framework to ensure that scammers are less successful in exploiting gaps and loopholes in particular sectors (and parts of sectors) within the scams ecosystem
- This will include a unified effort across government, regulators and the private sector to:
  - prevent scams through key communication channels;
  - educate consumers;
  - recover payments;
  - offer support for victims; and
  - strengthen cyber and identity resilience

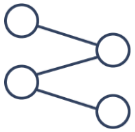
Piper Alderman

Principle 3: Complement existing interrelated regimes, systems and initiatives

- The Framework will complement and leverage existing interrelated regimes, systems and initiatives
- The Government aims to complement and leverage existing interrelated regulatory regimes and reform processes to reduce overlap and regulatory burden on sectors
- This includes but is not limited to:
  - work being progressed on the Australian Cyber Security Strategy 2023-2030;
  - reforms to the Government's digital identity accreditation framework;
  - reforms to strengthen Australia's privacy framework; and
  - the ACCC's ongoing work and reporting as part of Digital Platforms Services Inquiry and related ongoing work across portfolios

Features of the Code

Overarching regime and sector-specific legislation



New definitions to aid in setting a consistent scope under Australian law

Principle-based obligations

PiperAlderman

Overarching Regime and Sector-Specific Legislation

- The Framework would be created by introducing an overarching regime under the *Competition and Consumer Act 2010* (Cth) (**CCA**)
- The intention is that the CCA would institute mandatory obligations for businesses in designated sectors to address scams which are carried out using their services
- The Framework would also introduce mechanisms (such as codes and standards) under sector-specific legislation
- The mechanisms would allow the Government or regulators to establish specific codes and standards for sectors – ensuring that appropriate additional and tailored obligations are on businesses to prevent, detect, disrupt and respond to scams

Definitions – ‘Scam’

- The Framework intends to introduce a definition of “**scam**” to aid in setting a clear and consistent scope of the types of harms that organisations regulated under the Framework are expected to address.
- The proposed definition of “**scam**” is:
  - *‘a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means.’*

Piper Alderman

Definitions – Initial Sectors

- The Framework also intends on introducing a definition for each of the initial sectors to be designated, namely:
  - "**Digital Communication Platform**" – covering all digital platforms that provide communications or media-type services that can be exploited to share this material
  - "**Bank**" – applying to a body corporate that is an Authorised Deposit-Taking Institution (**ADI**) under section 9 of the *Banking Act 1959* (Cth)
  - "**Telecommunications Provider**" defined as "Carriers and Carriage Service Providers" under the *Telecommunications Act 1997* (Cth)

Key Features of the Framework

Principle-based obligations

➔ The Framework aims to establish clear and enforceable principle-based obligations, ensuring a consistent and proactive approach to combat scams. The proposed obligations are broadly categorised as:

- **Prevention** – including the requirement to develop, maintain and implement an 'anti-scam strategy', the requirement to implement 'anti-scam systems' and ensuring sufficient staff training to identify and respond to scams
- **Detection and disruption** – including detecting, blocking and preventing scams from initiating contact with customers, as well as verifying and tracing scams
- **Response (obligations with respect to consumers)** – including taking all reasonable steps to prevent further loss to the consumer, and having user-friendly, effective, transparent and accessible complaints handling processes for consumers
- **Reporting (obligations to regulators and other businesses)** – including reasonable steps obligation to notify other business and relevant regulators of intelligence about suspected or identified large-scale scam activity, as well as rapidly emerging or cross-sectoral scam activity

Impact on the Banking Industry

A banking sector code would establish specific obligations on ADIs to prevent, detect, disrupt and respond to scams

Prevention

Detection and Disruption

Response

Commonwealth Bank

nab

Westpac

MACQUARIE

ANZ

Piper Alderman

Impact on the Banking Industry (Cont.)

Obligations on ADIs with respect to scams

- **Prevention** – including that ADIs must implement preventive processes to:
  - enable confirmation of the identity of a payee to reduce payments to scam accounts;
  - verify a transaction is legitimate where activity is identified as 'higher risk' or is likely to be a scam; and
  - detect higher risk transactions and take appropriate action to warn the consumer, block or suspend the transaction, and working with recipient banks to block scam accounts
- **Detection and Disruption** – including that the ADI must have processes to identify and share information with other banks that an account or transaction is likely to be a scam, and block or disabling scammer account(s) or transactions
- **Response** – including that an ADI has user-friendly and accessible methods for consumers to switch accounts when they have been hacked, assisting consumers trace and recover funds, and responding to information requests from ASIC within specified timeframes

Proposed Scams Code 2024 – Industry Concerns

75 submissions were received for the consultation and although they indicated that the Framework was overwhelmingly supported by industry stakeholders, they also identified the following concerns:

→ **Definition of 'scams'**

- The definition proposed in the Consultation Paper may cover other matters, like fraud
- Element of knowledge of and authorisation by the victim should be incorporated within the definition

→ **Constraints for information sharing**

- Cross and intro-industry sector sharing of scam and financial crime information may be limited by the *Privacy Act 1988* (Cth) and the tipping-off provisions under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**)
- Individual privacy issues from intelligence sharing indicate a need for clear guidelines around what information can be shared and with whom

Proposed Scams Code 2024 – Industry Concerns (Cont.)

75 submissions were received for the consultation and although they indicated that the Framework was overwhelmingly supported by industry stakeholders, they also identified the following concerns:

→ **Sector-specific obligations**

- In recognising the necessary variations between sectors, some responses considered that the code should have uniform or comparable requirements, whereas others recommended tailoring the industry codes to their relevant sector in as much detail as possible regarding the imposed obligations

→ **Multi-regulator strategy**

- Although a multi-regulator strategy seeks to leverage the existing expertise of sector-specific regulators, the proposed approach may lead to the duplication of actions and penalties, and inconsistent or overlapping approaches across regulators and sectors
- Responses considered challenges arising from regulators' identification of multiple points of failure across different sectors when applying the regime

The Global Response to Scams

Piper Alderman

The UK's Approach

- **Occupational and Personal Pension Schemes (Conditions for Transfers) Regulations 2021**
  - Came into force on 30 November 2021 and introduced conditions that a pension transfer must satisfy before it can be approved and gave power to trustees to intervene when concerned about a potential scam
  - Trustees collect information about the transfer request and identify 'red' or 'amber' flags present and ask members questions to identify scam risk, where high risk transfer requests are halted and members are referred to the government's Money and Pension Service
- **Online Safety Act 2023**
  - Received Royal Asset on 26 October 2023, with the majority of its provisions entered into force on 10 January 2024
  - Empowers Ofcom (the UK's communications regulator) to require regulated businesses to implement "proportionate systems and processes" to protect users from illegal content online, including advertisements for investment scams and fraudulent products and services
- **Scam Ad Alert System**
  - Launched on 16 June 2020 and operated by the Advertising Standards Authority (**ASA**) in partnership with major online ad and social media platforms to target scam advertisements online
  - Users report potential scams via a quick reporting form, where Scam Ad alerts were sent to platforms to provide those advertisements

Piper Alderman

Hong Kong's Approach

- **Financial Intelligence Evaluation Sharing Tool (FINEST)**
  - In June 2023, Hong Kong Monetary Authority (**HKMA**) collaborated with the banking industry and law enforcement to launch FINEST
  - FINEST is a bank-to-bank information-sharing platform which enhances banks' ability to share intelligence in order to detect and disrupt scams
- **Overall regulatory oversight**
  - Since 2021, HKMA's supervisory requirements prohibit banks from sending SMS or email messages containing embedded hyperlinks directing individuals to their websites or mobile applications to conduct transactions
  - Banks are also prohibited from asking customers to provide sensitive personal information, such as passwords, via hyperlinks
  - On becoming aware of a scam, banks must promptly notify customers through the publication of press releases and report the matter to the HKMA

Singapore's Approach

→ **Shared Responsibility Framework (SRF)**

- On 25 October 2023, the Monetary Authority of Singapore (**MAS**) and the Infocomm Media Development Authority (**IMDA**) jointly proposed the introduction of a systematic approach to combating phishing scams within the financial institutions and telecommunications sectors
- The SRF assigns sector-specific obligations on financial institutions and telecommunication companies with sector-specific obligations and responsibilities and encourages cross-industry collaboration
- The SRF is set to be rolled out later in 2024

→ **Online Criminal Harms Act 2023**

- Came into effect on 1 February 2024
- Expanded powers for the government to order swift blocking of fraudulent accounts or content through the issuance of directions where it reasonably suspects that an online activity is contributing to the commission of a malicious cyber activity, including a scam
- Encourages collaboration between authorities and online services providers

Beating the Scammer

- It is important to recognise that although it is impossible to eradicate all scams, effective collaboration among government and regulatory bodies, law enforcement and the private sector would assist in better protecting Australians from scams and creating a more hostile environment for scam activity, consequently reducing scam losses and impacts on individuals and businesses
- Responses to the Consultation Paper indicated that the implementation of a Framework would be welcomed, but also called for greater cross-industry dialogue to ensure coherency in terms of strategy and actions

Piper Alderman

Disclaimer

The information contained in this presentation is for general information purposes only and should not be relied upon by any participant or reader of this presentation.

Piper Alderman takes no responsibility nor be held reliable for any such reliance on this information nor on the contents of any oral presentation associated with the topic or materials relating to the presentation.

Piper Alderman

Contact

Andrea Beatty

Partner

+61 2 9253 3818

abeatty@piperalderman.com.au

Mark Dehaini

Associate

+61 2 9253 3823

mdehaini@piperalderman.com.au

Piper Alderman

piperalderman.com.au

Adelaide | Brisbane | Melbourne | Perth | Sydney