

OPTUS

Submission in response to
The Treasury consultation

**Treasury Laws
Amendment Bill 2024:
Scams Prevention
Framework**

Public Version

October 2024

EXECUTIVE SUMMARY

1. Optus welcome the opportunity to provide comments on the Treasury Laws Amendment Bill 2024: Scams Prevention Framework (SPF). Optus also supports the Communications Alliance and Australian Mobile Telecommunications Association submissions on the proposed SPF.
2. The SPF introduces a multi-sectorial framework (initially relating to banks, digital platforms and the telecommunications sector) aimed at ensuring businesses adopt scam prevention actions to address the risk to Australian consumers from fraudulent scam activity.
3. Optus supports these efforts and supports the Government's desire to adopt a coordinated, whole of ecosystem approach to preventing and disrupting scam activity. Scams operate across multiple different sectors and scammers change their approach to exploit different vulnerabilities in different sectors.
4. While it may not be possible to completely eradicate scams, Optus agrees that some sectors require immediate uplift and others need more consistent uplift to reduce the effectiveness of scams and make Australia an unattractive target for scammers.
5. The telecommunications industry has led the way in implementing measures to detect and prevent scam activity, including an enforceable industry code, which has significantly reduced the number of scam calls and SMS reaching Australian consumers. The industry also has in place a range of industry-specific direct regulation that already addresses the majority of the obligations proposed in the SPF.
6. Telecommunications companies have also developed a range of technical solutions that would assist other companies in identifying if their customer was at high risk of fraudulent transactions, particularly where companies rely on SMS as a security protocol, despite never being designed as a security tool. However, take-up of these by other companies has been slow or inconsistent in sectors.
7. Because of this, Optus supports a flexible framework approach, whereby the SPF contains principles to guide the development of subordinate regulation which can be targeted at the specific issues and deficiencies identified in designated sectors. Optus supports this approach as:
 - (a) it ensures the subordinate regulation can be targeted at critical deficiencies in a specific sector to deliver immediate real-world benefits in an efficient and streamlined way;
 - (b) it avoids increased complexity from duplicated obligations; and
 - (c) does not prohibit the development of future innovative responses and solutions to disrupt scam activity and can better respond to changes in a highly technical and dynamic industry such as telecommunications as scammers constantly evolve their approach.
8. A flexible framework would also streamline and minimise complexity in relation to:
 - (a) enforcement of sector-specific obligations, where there is a sector-specific regulator in addition to the general SPF regulator; and

- (b) dispute resolution, liability and compensation arrangements, particularly where a sector-already has an existing sector-specific external dispute resolution (EDR) scheme.
- 9. As currently drafted, the proposed framework contains broadly drafted obligations some of which could be impractical to implement; and could have unintended consequences such as inadvertently assisting scammers and negative impacts on consumers, for example, overloading them with scam notifications. Such outcomes would undermine the overarching aims of the SPF.
- 10. Optus also supports a holistic policy approach to addressing scams in each sector, particularly where there are additional actions that Government or regulators could take that would have immediate, real-world benefits in addressing scams.
- 11. As such, Optus supports the timely finalisation of a mandatory SMS Sender ID Registry (following the legislation that has been passed by the Government) as this can immediately provide confidence to recipients as to the legitimacy of an SMS. In addition, Optus also considers work needs to be urgently progressed on clarifying the rights of use of numbers.
- 12. Finalising and implementing both of these projects should be a priority in tackling scams, prior to designating the telecommunications sector under the SPF as these would have a direct impact on disrupting scam activity and complement existing activities of the telecommunications industry.
- 13. There has been significant work already done by the telecommunications sector to protect telecommunications services, its consumers and more broadly prevent and disrupt scam activity. Where appropriate this is governed by existing regulations. Industry also actively participates in collaborative government-led initiatives, such as the National Anti-Scam Centre (NASC).
- 14. Optus urges Treasury to implement a flexible framework that:
 - (a) Contains guiding principles to support targeted obligations in subordinate regulation to address gaps or identified issues, rather than containing broad, general overarching obligations in the primary legislation, given the different roles and existing regulation of key sectors;
 - (b) Minimises complexity by avoiding duplication of obligations in the primary legislation with existing industry regulations or external dispute resolution schemes;
 - (c) Does not discourage or slow innovative technical solutions to scam activity, particularly where this may require collaboration across sectors;
 - (d) Enables obligations in subordinate regulation to commence at the time designating a sector occurs to address concerns about slow or inconsistent action in a sector; and
 - (e) Complements other policy initiatives or work that may better address issues related to scams, such as, the SMS Sender ID Registry or work on clarifying the rights of use of numbers in the telecommunications sector.
- 15. Optus also recommends that care is needed in designating any liability to compensate customers for financial or other loss. The use of SMS, for example, as a security tool to authenticate financial transactions should not make telecommunications providers liable

for loss because this service was never designed as a security tool and financial institutions can and should invest in more robust solutions.

16. Optus believes such an approach will still be able to achieve timely success in uplifting standards where needed without adversely impacting sectors that already have significant sector-specific capabilities and regulation in place, to ensure Australia is an unattractive target for scammers.

PROTECTIONS ARE INCONSISTENT ACROSS SECTORS

17. Optus welcomes the Government's recognition that a whole of eco-system approach is needed in relation to scams and that some sectors require immediate uplift and others require a more consistent approach in an effort to tackle scams.
18. In considering how best to legislate a scams prevention framework, it is important to remember that some sectors are considerably more advanced in terms of efforts and regulation at addressing scams. In addition, there are very different scam issues prevalent in each sector, scams evolve and change their approach and interact with sectors in different ways. While there is a common overarching policy intent, the role each sector has to play and how this is achieved in each sector may need to be addressed differently.

Telecommunications has strong regulatory obligations for addressing scams

19. Scams can affect the telecommunications industry in two ways:
 - (a) telecommunications services can be used by scammers in an attempt to contact customers as part of a scam; or
 - (b) telecommunications services themselves can be a target for scammers because SMS continues to be used by a range of companies (such as banks or other service providers) as a security protocol for accounts (e.g. one time codes) even though SMS was never designed nor intended to be used in this way.
20. As Treasury would be aware, the telecommunications industry has numerous existing regulations that address issues around telecommunications account security, customer identification, and scam protection, including:
 - (a) the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* (MFA Determination) which requires multi-factor customer authentication for certain high-risk transactions and prevents scammers from taking over telecommunications accounts;
 - (b) the *Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020* requires industry to conduct stronger identity checks to stop mobile porting fraud; and
 - (c) the *Reducing scam calls and scam SMS Code* (Reducing Scams Code) which aims to identify and stop scam calls and SMS based on certain characteristics.
21. These regulations have been particularly successful in increasing telecommunications account security and reducing the number of scam calls and texts reaching consumers.
22. Telecommunication providers, including Optus, have a range of built-in protections on our networks that are automatic, such as SMS and Scam Call Firewalls, and these have blocked huge quantities of scams from reaching our customers.
23. Across the telecommunications industry, 2.1 billion scam calls have been blocked since 2020 and over 668 million scam SMS have been blocked since the Reducing Scams Code was updated to include SMS in 2022.¹ While it may not be possible to completely

¹ <https://www.acma.gov.au/publications/2024-08/report/action-scams-spam-and-telemarketing-april-june-2024>

stop all scam traffic, through these measures, which have been in place for many years, Australia is a more difficult place to send successful scam communications traffic.

24. Further the industry already has well-established internal dispute resolution regulation and an external dispute resolution scheme in place, with:
 - (a) the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018* (Complaints Handling Standard), which sets out obligations for dealing with customer complaints; and
 - (b) the Telecommunications Industry Ombudsman scheme, which Carriage Service Providers (CSPs) are required to join.
25. The industry also participates and works collaboratively across Government-led initiatives such as:
 - (a) the National Anti-Scam Centre (NASC);
 - (b) the Australian Financial Crimes Exchange (AFCX) including the Anti-Scam Intelligence Loop, and
 - (c) the Security & Fraud Alliance Forum, an initiative of the telecommunications sector that brings together all major carriers, banks, crypto currency providers, large Australian brands and organisations, State, Territory and Federal police agencies, the Australian Financial Crimes Exchange (AFCX), ID Care and law enforcement agencies, to exchange information in a highly operational context and cooperative environment.

Telecommunications has measures that can assist other industries

26. Scammers continue to change their approach and exploit deficiencies in scam protections across the broader Australian ecosystem. Scammers adopt different communication channels, such as social media, messaging sites/apps and dating sites/apps, as well as false advertisements on social media sites and digital platforms and different approaches, from large scale mass scam texts or calls to targeted relationship building once initial contact is made.
27. Ultimately scammers are after financial reward which can be achieved in different ways, for example, convincing a consumer to willingly transfer money; impersonating a legitimate recipient of a money transfer and providing false details; or by account takeover whereby the scammer has enough security information to take over the consumer's bank account and transfer the money out of the consumer's bank account themselves. The overwhelming purpose of scammers trying to access or takeover telecommunications services is to use those services as a stepping stone to accessing consumers' bank accounts.
28. Optus and the broader telecommunications industry have a range of capabilities that are available to other industries, such as banks, to address impersonation scams and account takeover scams.
29. Protections against sender impersonation scams include:
 - (a) **Do Not Originate List:** For specified number ranges, where Optus is the originating network for legitimate calls, Optus blocks the numbers from entering the Optus network. We also ask other participating telcos to not allow their own directly connected customers to originate calls using the specified

numbers, and to block them from being received onto their network from anywhere other than Optus.

For protected originating customers of other networks, Optus only allows calls to enter the Optus network from the network that calls are authorised to originate those calls. It is then up to that originating telco to ensure that no one else on their network can originate calls using those numbers, or to use their network to transit such calls.

For all cases (even where there aren't any DNO arrangements) Optus has our network configured to not allow our directly connected customers to Spoof their CLI (Calling Line Identification).

- (b) **SMS Sender ID Protection:** Also known as “Trusted Sources”, which has evolved into ACMA’s SMS Sender ID Registry trial; this service allows participants to prevent their Alphanumeric Sender IDs (“alpha tags”) from being spoofed by unauthorised entities. The participating telcos (Telstra, Optus, TPG Telecom, & Pivotal) set their SMS Firewalls to only allow the specified alpha tags to arrive on their network where they come from the trusted source network. This primarily prevents Scam SMS from arriving in the same message thread as legitimate messages from the bank or other protected organisation. There are protection types available that offer higher levels of protection, such as applying restrictions to any SMS Sender ID that contains the protected word or words in a Sender ID.

This scheme has been available since 2021, and after all this time, take-up is disappointingly low..

- (c) **Optus Call Stop & Optus Text Stop:** Participating financial institutions provide details of Scam SMS that feature a Scam Callback number that impersonates the reporting entity. The Scam SMS will usually contain a claim that a financial transaction took place on the person’s bank account, and to immediately call a supplied number. At times, the Scam SMS may appear in the same message thread as legitimate messages of the impersonated entity (which further highlights the importance of SMS Sender ID protection).

There are currently 2 separate instances of Call Stop in operation. The first instance, with the AFCX, focuses on bank impersonation scams, with validated scam data supplied by the banks, and directly led to the creation of the AFCX Anti-Scam Intelligence Loop (“the loop”). The second instance uses validated data supplied by NASC and focusses on investment scams.

Once Optus receives the validated scam data, Optus then diverts any calls made to the Scam Callback number, to a recorded voice announcement (RVA) warning that “The number you have called has been reported as being used for scam activities. For more information, please visit optus.com.au/CallStop.” This immediately disrupts the scam for customers on the Optus network.

Optus then submits details of the Scam Callback number to the traceback process in the Reducing Scam Calls and Scam SMS Industry Code, and the offending service will be disconnected. This ensures that customers of other network will also benefit from Optus’ actions, although without the education piece of the warning message.

30. Protections against telecommunications account take-overs include:
- (a) **SIM Swap Notifications are available to companies who use SMS for security:** While the telecommunications industry has implemented multi-factor authentication capabilities for 'high risk customer transactions' transactions' (including SIM swaps) as required by the MFA Determination to protect telecommunications accounts from fraudulent takeovers it is difficult to prevent all fraudulent SIM swaps, especially where a scammer has sufficient stolen ID. information to be able to impersonate a customer.

The telecommunications industry created a data service through Jersey Telecom's 'JT Monitor SIM Swap Services', which can provide real-time information to banks on SIM swaps that have taken place. The key reason that scammers conduct a fraudulent SIM swap is in order to gain access to a victim's bank accounts by receiving and acting on one-time-codes received by SMS. This service can be used by companies, such as banks to raise red flags on any transactions that are requested subsequent to a SIM swap.

Again, disappointingly this capability has not been taken up . The telecommunications industry has these tools available and we consider this a proactive measure that can provide an additional safeguard to financial institutions that rely on SMS as an authentication tool.
 - (b) **Number Porting Notifications:** While Pre-Port Verification (PPV) has significantly reduced instances of fraudulent porting, some scammers will find a way, such as through socially engineering their victim. To further protect Australians, the telecommunications industry provides real-time porting information (for all number types) as both a data feed service and a lookup service. This would enable companies, such as banks, to consider any recent porting activity in their risk profile for any financial transactions.
31. While some companies have done good work in implementing measures to disrupt scam activity, we note that ASIC has recently released a report (Report 790) showing the inconsistent take up by the banking industry of these protections.²
32. Report 790 examined the scam prevention, detection and response activities of 15 banks outside of the four major banks. ASIC found that there is a lack of protection by banks against brand misuse across all their telecommunication channels. Only one of the reviewed banks had fully implemented controls to minimise misuse of its telephone numbers and SMS alpha tags to prevent impersonation scams.
33. There also appears to be inconsistent use of the DNO List and Sender ID service, with ASIC findings that:
- (a) One bank had implemented both DNO List protection and SMS Sender ID protection;
 - (b) Seven banks had partially implemented the protections;
 - (c) Seven banks had not implemented either of the protections; and
 - (d) Seven banks had plans to implement or improve their protection status.

² ASIC, Report 790: Anti-scam practices of banks outside the four major banks, 20 August 2024. Available at: <https://download.asic.gov.au/media/eiahqnwn/rep790-published-20-august-2024.pdf>

34. This reflects Optus' observations and experience that there has been modest take up of these protection services.
35. Regarding protection against impersonation scams, we note again that only 5 banks have implemented SMS Sender ID protections since the scheme has been available since 2021. More broadly there are varying degrees of adoption of this across other key businesses and organisations, such as, essential services providers, large retailers, delivery services and government organisations. Optus considers that SMS Sender ID protections is a measure that all companies should have in place to provide confidence to consumers of the legitimacy of SMS.
36. It is clear there has been an inconsistent approach to uplifting protections in key sectors such as banking and digital platforms. While the telecommunications industry is already regulated to address issues identified in other sectors (such as, account protection or blocking scam contacts) a one size fits all approach across all sectors risks creating an unnecessarily complex regulatory landscape. Optus considers the framework should be flexible enough to support regulation appropriately tailored to the issues and characteristics of each sector.

A MORE FLEXIBLE FRAMEWORK IS NEEDED

37. Key elements of the SPF include:
- (a) 6 principles containing broad overarching obligations that would apply to a sector as soon as that sector is designated;
 - (b) An external dispute resolution (EDR);
 - (c) civil causes of action; and
 - (d) Provision for an SPF regulator and an industry-specific regulator.
38. Optus acknowledges the desire to immediately uplift actions in a relevant sector in a timely fashion (i.e. as soon as that sector is designated), but, has some concerns with the approach in the proposed framework. These concerns include:
- (a) The principles in the overarching framework contain broad obligations that can duplicate already existing industry-specific regulations in some sectors which increases the complexity of implementation and enforcement;
 - (b) Some of the obligations are potentially impractical to implement; and
 - (c) Some obligations could have unintended negative consequences on industry and consumers.

The framework should avoid duplicating existing obligations

39. As noted, the telecommunications sector already has a range of industry-specific regulations in place designed to prevent and disrupt scam activity and provide protections to consumers. This includes:
- (a) The Reducing Scams Code, which aims to identify and stop calls and SMS that are scam calls / SMS based on certain characteristics;
 - (b) The MFA Determination, which requires multi-factor customer authentication for certain high-risk transactions;
 - (c) The Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 requires industry to conduct stronger identity checks to stop mobile porting fraud; and
 - (d) The *Telecommunications (Consumer Complaints Handling) Industry Standard 2018* (Complaints Handling Standard), which sets out obligations for dealing with customer complaints.
40. The broad obligations in the proposed principles of the framework concern requirements regarding governance, prevention, detection, reporting, disruption and response (including internal dispute resolution) which largely duplicate the existing industry-specific obligations but in a broader way.
41. If the telecommunications sector is designated (as apparently intended by the Government) it would immediately become subject to these broad obligations which will create significant complexity in operation between these regimes particularly where there are multiple regulators.

42. For example, the Reducing Scams Code focuses on operational requirements to identify and block scam SMS and calls and is enforced by the ACMA. However, the proposed principles require companies to take reasonable steps to detect scams related to certain services (s. 58BN), to prevent scams from being committed (s. 58BK) and to disrupt scams and prevent loss or harm.
43. Similarly, proposed s. 58BZC requires an entity to have an internal dispute resolution mechanism for consumers to complain about scams. Yet, the telecommunications industry is already subject to the Complaints Handling Standard, enforced by the ACMA, which is prescriptive in its requirements regarding handling of customer complaints.
44. The broad drafting of these proposed framework obligations creates considerable regulatory uncertainty, particularly where there are multiple regulators enforcing the industry-specific regulations and the SPF.
45. It could conceivably lead to a scenario where a scam occurs and despite a telecommunications company being compliant with the requirements of the industry code or industry-specific regulation, another regulator may take the view that the company did not take reasonable steps as required by the overarching obligations in the SPF.
46. This leads to regulatory uncertainty and implementation complexity given the highly technical nature of providing telecommunications services and implementing scam detection, prevention and disruption measures.
47. In addition, liability and compensation arrangements need to be carefully considered. The SPF proposes that there be an external dispute resolution (EDR) scheme as well as civil rights of action.
48. Optus does not consider that telecommunications companies should be broadly liable or share the liability for financial or other loss, particularly where a telecommunications company has complied with its industry-specific obligations.
49. The use of SMS, for example, as a security tool to authenticate financial transactions, should not make telecommunications providers liable for loss because this service was never designed as a security tool and financial institutions can and should invest in more robust solutions.
50. Optus considers that liability should be limited to circumstances where a telecommunications company has failed to comply with its industry-specific obligations and the customer has suffered loss with that telecommunications company (for example, if a scammer has gained control of the customer's telecommunications account and obtained devices).
51. In addition, the SPF contemplates an additional external dispute resolution scheme. However, the telecommunications industry already has an external dispute resolution scheme, the Telecommunications Industry Ombudsman. Optus believes the SPF framework should be flexible such that if a sector already has an established EDR scheme (like telecommunications does with the TIO scheme) it should not also be subject to an additional EDR scheme.
52. Multiple EDR schemes applying to a sector, particularly where there are duplicative obligations, would also be complex, create confusion and raise industry costs. One EDR scheme for the telecommunications sector would ensure there is less confusion for telecommunications companies and consumers.

53. Optus considers that there should also be a safe harbour provision that where a telecommunications company complies with an industry code or industry-specific regulation the company will not be subject to enforcement action under the SPF Framework, via civil action nor via an EDR scheme.

Some obligations may be impractical to implement or have unintended consequences

54. There are further concerns about the practical implementation of some of the principles.
55. Proposed Principle 2 related to the prevention of scams requires a regulated entity to take reasonable steps to identify the classes of consumers of that entity's service who have a higher risk of being targeted by a scam relating to the service and provide warnings about such a scam to each consumer (s. 58BK(2)).
56. Given that companies regularly use SMS as a security protocol (as previously noted despite SMS not being designed nor intended to be used in this way) all users of telecommunications services are at risk of being targeted by scammers for account takeover to be used to gain access to other accounts (such as bank accounts) or in perpetrating other criminal activity.
57. Further, given the proposed broad definitions of 'scam' and 'actionable scam intelligence' it is conceivable that every SMS or call blocked in accordance with the Reducing Scams Code would be considered actionable scam intelligence.
58. This means telecommunications companies would need to send an alert/notification to users every time a scam call or SMS was blocked. In the April – June 2024 quarter telecommunications companies blocked in excess of **291.4+ million** scam SMS and calls (this would be on average more than 3.1 million contacts blocked **each day**).³
59. This is likely to lead to notification fatigue for consumers from the telecommunications industry alone, let alone in conjunction with notifications from any other sector.
60. We agree that consumer awareness and education is an important element of combatting scams and reducing their success, but the proposed notification obligations in the framework which would apply as soon as a sector is designated may not be the best approach.
61. In addition, proposed s. 58BF requires an entity publish information about the measures the entity has in place to protect its consumers. Such a requirement should be considered against the harm that could be caused if scammers have easy access to a company's changing protective measures, particularly where new innovative solutions are implemented. In that case, it is not clear any benefit would be outweighed by the potential harm.
62. Again, Optus considers a better approach would be for the framework to include the principles as guidance for any subordinate regulation with the capacity for some or all of that subordinate regulation to come into effect for a relevant sector as soon as that sector is designated, as achieving the same timely outcome in a more appropriately targeted way.

There are advantages to a more flexible framework

63. Keeping in mind the desire for there to be a whole of eco-system approach to tackling scams and the need for there to be a timely uplift in some sectors, Optus believes this

³ <https://www.acma.gov.au/publications/2024-08/report/action-scams-spam-and-telemarketing-april-june-2024>

can be achieved while avoiding the issues that result from having broad, duplicative obligations in the primary legislation.

64. This could be achieved by making minor adjustments to the construction of the framework so that it is more flexible in its operation.
65. Specifically, the concerns noted above could be addressed by removing the obligations set out in proposed Principles 1-6 and instead have these as matters that must be addressed by subordinate regulation (e.g. a Ministerial Instrument, SPF Rules and/or Industry Code).
66. This would allow the subordinate regulation to address these overarching principles in a way that is targeted towards the key concerns in each sector, which ensures regulation is appropriately targeted and consistent with good regulatory practice. This would remove the complexity associated with having broad obligations duplicating existing Code requirements and allow Code obligations to be crafted appropriately in relation to other industry-specific regulations already in place and technical and/or operational considerations of that industry.
67. The framework could also provide the flexibility for subordinate regulation to implement obligations in a sector immediately upon designation (i.e. designation and obligations in subordinate regulation could be considered and come into effect concurrently). This would still support the timely uplifting of a sector's activity in relation to scams.
68. Ensuring the obligations are in subordinate regulation such as an industry code could also assist where there would otherwise be one regulator enforcing the obligations in the framework and an industry-specific regulator enforcing obligations in an industry code.
69. Further, given the highly technical and dynamic nature of the telecommunications industry, Optus believes an industry code is more advantageous than having obligations in primary legislation as an industry code can be more easily adapted over time in response to technical changes in the industry and the evolving nature of scam methods.
70. More broadly, such flexibility would allow the Government and regulators to pursue multiple solutions where the SPF complements other policy initiatives that are also likely to have a real impact on preventing scams. The evolving nature of scams means solutions will always need to adapt and a particular scam-related issue may need to be tackled by multiple industries and/or in multiple ways.
71. In particular, Optus encourages the timely implementation of a mandatory SMS Sender ID Registry, following the passage of the relevant legislation, as well as the clarification over the right of use of numbers.
72. While large numbers of scam messages are blocked by telecommunications companies, scammers are still able to evade these efforts. Therefore, multiple solutions are needed to prevent scam activity.
73. A mandatory SMS Sender ID Registry applying broadly across the Australian ecosystem would increase confidence amongst consumers as to the legitimacy of SMS and reduce the likelihood of consumers being duped by fraudulent messages, consistent with the policy objective of the SPF.
74. The SMS Sender ID Registry is already in train and implementing it is likely to have an immediate impact in delivering real world benefits to consumers in protecting them from scam activity.

75. In addition, Optus requests that urgent work be done by the ACMA to clarify the rights of use of numbers. Such work would assist in circumstances where numbers are spoofed to appear as though a scammer is calling from a trusted institution. Optus recommends that addressing issues related to the rights of use of numbers would assist in preventing such scam calls and further protect Australians from scams and again, is something that could be undertaken to deliver additional timely protections to Australian consumers.

Consumer education will continue to be important

76. Along with regulatory and policy measures, Optus also encourages continued education efforts by Governments and regulators on consumer awareness of scams. Investment scams continue to be the overwhelming source of loss for Australians⁴ and where scammers use more sophisticated approaches and tactics, education, awareness and financial literacy will continue to play an important role in minimising scam success.

⁴ <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>