Australian Government

acma

Australian
Communications
and Media Authority

Combating scams

Action plan summary

NOVEMBER 2019

Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 32
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700 or 1800 226 667
F +61 2 9334 7799

Contents

Executive summary

Scam activity on telco networks has a significant social and economic impact on Australians. The scale and effect of the activity is increasing. Australian Communications and Media Authority (ACMA) consumer research confirms it is a significant problem and people expect more to be done by industry and government.[1]

Scam activity is increasingly sophisticated and hard to detect. It usually originates offshore, readily adapts to disruption measures and ruthlessly exploits new opportunities and vulnerabilities. Australia, along with Canada, the United States and Europe, is targeted by scammers on an industrial scale.[2] There is a need for immediate tangible action given the scale and escalation of the harms.

The Australian Competition and Consumer Commission (ACCC) reports losses will exceed a record $532 million by the end of 2019.[3] The telephone remains the preferred contact method of scammers. In 2018, 46.8 per cent of scam reports concerned phone calls.[4] In response to the problem and a request from the then Minister for Communications and the Arts, the ACMA established the cross-agency Scam Technology Project (the Project) with the ACCC and the Australian Cyber Security Centre (ACSC) to explore ways to reduce scam activity. The Project's terms of reference are at Appendix A**.**

Since March 2019, a public discussion paper was released and extensive targeted consultation with key stakeholders has occurred. The Project's findings draw on experience, expertise and feedback from industry, government agencies and international regulatory partners.

The Project considered the problem of scams over telecommunications networks in several ways, including, crucially, in terms of the harms perpetrated on innocent people. This criminal activity impacts directly on the financial and emotional wellbeing of many Australians. It also undermines confidence in our telecommunications services. In this sense, telco providers and the broader community are also impacted by scam activity, even where they have not been direct victims.

Scammers perpetrate their crimes via a range of scam types (see Appendix C), obfuscation techniques and reliance on what is essentially 'safety in numbers' high-volume calling. Scammers are technologically adept, increasingly sophisticated and show no signs of stopping.

Scams are an international problem that challenge industry and regulators across the globe. There are several offshore initiatives currently being trialled or under development that attempt to address the various types of scams. The Project has therefore also considered a range of emerging and innovative global initiatives and their applicability domestically.

[1] ACMA, *'Unsolicited calls in Australia: Consumer experience'*, 2018, viewed 11 September 2019.

[2] ABC, *Four Corners - Meet the Scammers*, 2019, viewed 30 October 2019.

[3] Scamwatch, 'Record losses expected as scammers target Australians', 2019, viewed 23 August 2019.

[4] ACCC, *Targeting Scams Report of the ACCC on scams activity 2018*, 2018, viewed 23 August 2019.

While the Project has focussed on industry-led technological solutions, these solutions are likely to be ineffective in isolation. Promoting information-sharing across industry and between industry and government is vital, supported by strategic coordination, improved consumer awareness and regulatory enforcement.

The Project notes that there are a range of robust scam reduction initiatives underway, many a direct result of the Project. Any telco provider-level scam reduction activity, however, needs to be scaled to be consistent and industry-wide, underpinned by robust scam verification measures and information sharing across telco providers and between telco providers and government.

To achieve this, new obligations are required for telco providers to act on scam calls. Obligations that are enforceable by the ACMA. These are, in large part, about ensuring the legitimate use of calling line identification (CLI).

Legitimate use of CLI can be facilitated by ensuring calls that originate within Australia are subject to robust rules that verify their legitimacy (specifically, a call should not originate on an Australian network unless the CLI is a legitimate number and the caller holds the rights to use it).

The Project, in consultation with key stakeholders, has found several specific initiatives and mechanisms that can potentially identify offshore illegitimate traffic to facilitate blocking by telco providers.

In this context, the scam reduction actions proposed by the ACMA provide a framework that supports legitimate use of numbering, while providing disincentives for illegitimate use.

The proposed establishment of a scam telco action taskforce to progress scam reduction initiatives and monitor future developments should not only have the desirable impact of reducing scam calls being carried on Australian networks (and send a clear message to scammers that Australia is not a soft target) it should also build consumer confidence and trust in calls they are receiving.

The last appendix to this report contains a glossary of terms (Appendix D).

A brief note about this report. This is a summary of the full Action plan. Specific details have been removed throughout to ensure they are not used by malicious actors.

Action plan overview

In response to the Project findings, the ACMA proposes a three-point action plan to form a joint government-industry taskforce; develop new enforceable obligations and immediately trial new scam reduction initiatives.

	Action	Timing	Lead
ACTION 1:	**Establish a Scam telecommunications action taskforce to provide government and industry coordination and oversight of telecommunications scam minimisation strategies**	**Q4 2019, thrice annually**	**ACMA**
ACTION 2:	**Develop enforceable obligations for telco providers to:** **2.1 share scam call data across industry** **2.2 verify, trace and block scam calls** **2.3 prevent carriage of domestic originating calls where the caller does not hold the rights of use to the number** **2.4 minimise carriage of international originating calls using illegitimate calling line identification** **2.5 refer scam calls and/or perpetrators to authorities** **2.6 implement and update SMS filtering technology** **2.7 monitor broader technological development and international initiatives for potential implementation** **2.8 provide advice and information to customers**	**Q2 2020**	**Telco industry/ ACMA**
ACTION 3:	**Immediate trials of industry-wide scam reduction initiatives:** **3.1 implement a trial ‘Do Not Originate’ list** **3.2 identify and block ‘Wangiri’ call-back scam calls** **3.3 block traffic from providers carrying a high-volume of scam calls using commercial interconnect arrangements**	**Q4 2019 to Q2 2020**	**Telco industry**

Findings and actions

⇨ **FINDING:** **Strategic oversight and collaboration are required to coordinate action on scams**

⇨ **ACTION 1:** **Establish a Scam telecommunications action taskforce to provide government and industry coordination and oversight of telecommunications scam minimisation strategies**

1. Telco industry submissions indicated that the project was welcomed, with most stating it had brought renewed focus to the issues. Broader stakeholder submissions also welcomed the project and reiterated the imperative for action.
2. Analysis of stakeholder feedback, the domestic context and international approaches indicates that technological solutions to scam disruption need to sit within a broader framework to be effective.
3. A multi-stakeholder forum for oversight, collaboration, coordination and monitoring impact is a key part of such a framework, especially given that disruption of scams and harm reduction will involve the concerted efforts of disparate stakeholders across industry, government, the broader commercial sector and consumer groups.
4. This report is recommending immediate trials of several initiatives to reduce and/or stop scam activity. While these initiatives will predominantly require action from industry, they are also dependent on input and engagement from government.
5. Overseas experience also shows that government-industry working groups are a key enabler of scam reduction activities. For instance, in 2015 in the United Kingdom (UK), the telecommunications regulator (Ofcom) formed a strategic working group to tackle nuisance and scam calls. The group, that includes nine major telco providers, has since implemented several successful scam reduction initiatives.[5]
6. One initiative identified by the Ofcom working group is a list of 'Do Not Originate' numbers, issued to Her Majesty's Revenue and Customs (HMRC) but which are never used for outbound calls. Telco providers automatically block a number on the list if it is identified as an outbound call on its network. HMRC reported reducing to zero the number of phone scams spoofing genuine inbound HMRC numbers.[6]
7. Additionally, a public/private coalition of 51 Attorneys-General and 12 phone companies in the United States (US) recently announced the implementation of a set of Anti-Robocall Principles.[7] These Principles (at Appendix B) deal with many of the issues discussed in this report, albeit in the US context.
8. Accordingly, forming a Scam telco action taskforce (the taskforce), led by the ACMA and comprised of representatives from the telco industry and relevant government agencies, along with observers from other sectors, is recommended as an immediate action.

[5] Ofcom, *Nuisance calls and messages - Update to ICO-Ofcom joint action plan*, 2019, viewed 23 August 2019.

[6] HMRC, 'Controls prevent phone fraudsters spoofing HMRC', 2019, viewed 30 October 2019.

[7] USTelecom, *Anti-Robocall Principles*, 2019, viewed 29 August 2019.

⇨	FINDING:	**Industry must act, and continuously and innovatively adapt, to reduce scam calls**
⇨	ACTION 2:	**Develop enforceable obligations for telco providers to:** **2.1 share scam call data across industry** **2.2 verify, trace and block scam calls** **2.3 prevent carriage of domestic originating calls where the caller does not hold the rights of use to the number** **2.4 minimise carriage of international originating calls using illegitimate calling line identification** **2.5 refer scam calls and/or perpetrators to authorities** **2.6 implement and update SMS filtering technology** **2.7 monitor broader technological development and international initiatives for potential implementation** **2.8 provide advice and information to customers**
⇨	ACTION 3:	**Immediate trials of industry-wide scam reduction initiatives:** **3.1 implement a trial ‘Do Not Originate’ list** **3.2 identify and block ‘Wangiri’ call-back scam calls** **3.3 block traffic from providers carrying a high-volume of scam calls using commercial interconnect arrangements**

Action 2—Develop enforceable obligations for telco providers

9. The ACMA proposes new enforceable obligations to require telco providers to undertake the activities proposed at Action 2 (above) and discussed in detail below.

Action 2.1—Share scam call data across industry

10. Multiple government and law enforcement agencies receive reports of scam activity. Sharing this scam report data wider would help telco providers improve scam call identification and blocking.

11. Promisingly, the project has encouraged a range of new initiatives to share scam call data. For example, over 2.9 million scam calls were identified and successfully blocked in July 2019 by Telstra.[8]

12. Effective scam reduction at an industry-wide level can only be achieved through industry and regulators working together to develop improved processes and infrastructure that support appropriate sharing of scam data and referral for regulatory or law enforcement action.

13. In relation to data sharing, it is specifically noted that the *Telecommunications Act 1997* (the Act) places obligations on carriers and carriage service providers to:

[8] A. Penn, ‘Tackling the changing face of our customer’, *LinkedinPulse*, 12 September 2019, viewed 24 September 2019.

> do their best to prevent telecommunications networks from being used in the commission of offences against the laws of the Commonwealth, States and Territories (subsection 313(1))

> give officers and authorities of the Commonwealth, States and Territories such help as is reasonably necessary for enforcing criminal law and imposing pecuniary penalties (subsection 313(3)).

Additionally, the project is recommending immediate development of enforceable obligations to support sharing of data across industry.

Action 2.2—Verify, trace and block scam calls

14. Consultation with the telco industry has indicated a range of telco provider-level scam reduction activities are undertaken on a regular basis to block verified scam calls. Some telco providers are undertaking innovative action around disruption of specific scam call types, such as blocking 'Wangiri' call-back scam calls from global networks.
15. While these telco provider-level approaches are encouraged, they are not optimal given the volume of scam traffic being carried on Australian telecommunication networks and the harm it causes. The potential for scam traffic to circumvent telco provider level blocks means there is a need for industry-wide solutions to be developed and adopted.
16. International experience and submissions indicate that there is no single or simple solution (a 'silver bullet') to combat scams. For example, basic call blocking is a reactive, 'whack-a-mole' exercise where scammers often immediately present a new maliciously 'spoofed' CLI.
17. While the telco industry states that blocking is a relatively straightforward activity, verification of scam calls can be challenging. Currently, some telco providers use a range of data sources to identify scam calls while others use network traffic analysis.
18. There is a need for consistent protocols, processes and infrastructure to support sharing scam call data across industry.
19. Enforceable obligations are needed to ensure a consistent effective approach is taken to verify, trace and block scam calls.

Action 2.3—Prevent carriage of domestic originating calls where the caller does not hold the rights of use to the number

20. As discussed above, scams over telco networks lead to a lack of confidence in telephone numbering and a need to develop enforceable obligations to ensure legitimate use of CLI.
21. In 2016, Communications Alliance published an industry guidance note[9] to help clarify the range of uses and abuses of CLI and how to tackle the practice of inappropriate or malicious CLI spoofing. The overall objective of the guidance note is that customers making calls across networks can be uniquely identified from the CLI presented.[10]
22. In developing the industry guidance note, Communications Alliance acknowledged that the voluntary guideline represents the first step in addressing malicious CLI spoofing, and that further consideration should be given to:

[9] Communications Alliance, *Industry Guidance Note (IGN009) CLI Management*, 2016, viewed 26 August 2019.

[10] Communications Alliance, *Industry Guidance Note (IGN009) CLI Management*, 2016, viewed 26 August 2019.

> a guidance note or code of practice to enable telco providers to cooperate and have an agreed uniform approach to tackling CLI spoofing (short term)

> a rule in the Rights of Use of Numbers Code for all telco providers that are allocated numbers from the ACMA to respect and protect the originating CLI (medium term)

> representation at International Telecommunication Union (ITU) numbering fora to address unauthorised use or change of numbers to disguise originating CLI.

23. Noting these considerations, the ACMA proposes that the provisions in the voluntary guidance note be elevated into enforceable obligations, alongside other obligations to help reduce scam activity and restore confidence in numbering.

24. Crucially, this would restore confidence by:

> preventing carriage of domestic originating calls where the caller does not hold the rights of use to the number

> minimising carriage of international originating calls using illegitimate calling line identification (through blocking).

Action 2.4—Minimise carriage of international originating calls using illegitimate use of calling line identification

25. Overseas scammers use readily available and cheap technology to present calls with maliciously spoofed CLI to display a number more familiar or recognisable to the person receiving the call. This makes it more likely that the call will be answered. This can lead to consumers no longer trusting the number displayed on their phone when it rings.

26. The use of technology such as real-time call analytics combined with call blocking can significantly minimise carriage of illegitimate international traffic.

27. The project has identified specific initiatives and mechanisms that can potentially identify offshore illegitimate traffic and prevent it being carried on Australian networks, including the trials proposed in this report (see below).

Action 2.5—Refer scam calls and/or perpetrators to authorities

28. The desire for increased enforcement action against scammers was a common theme in submissions from stakeholders. While it is acknowledged that most scam activity originates overseas, there is evidence that some scam call syndicates may also operate domestically.[11]

29. Identified scam calls originating domestically are traceable. Additionally, numbers used by scammers for inbound calls, regardless of their location, are capable of being traced. Both types of scam calls can be referred to regulators or law enforcement.

30. Quality intelligence about serious harms is of interest to relevant enforcement agencies, including, potentially, the Australian Federal Police (AFP), Australian Transaction Reports and Analytics Centre, Australian Criminal Intelligence Commission, Australian Securities and Investment Commission, ACSC, ACCC, and the ACMA.

31. Enforcement action against overseas scammers can be achieved where quality intelligence can be provided to relevant law enforcement agencies through appropriate channels.[12]

[11] Austrac, 'The Fintel Alliance protects the most vulnerable from criminals', 2019, viewed 19 August 2019.

[12] 'Royal Canadian Mounted Police, CAFC information leads to the dismantling of 16 fraudulent call centres in India', 2018, viewed 20 August 2019.

32. Referral of scams through international channels is also available. One mechanism is through the Unsolicited Communications Enforcement Network (UCENet) via the ACMA, as a core member.[13]

33. UCENet is a global network of agencies and organisations engaged in combatting unsolicited communications. Its mission is to maximise collaboration and information sharing across the network to enhance unilateral, bilateral and multilateral compliance and enforcement approaches and actions. The ACMA has been a key participant in the development of information sharing mechanisms amongst members.[14]

34. More generally, given the international nature of scam activity and the challenge it presents to global regulators and industry, effective and holistic solutions will ultimately require significant global effort. As the International Institute of Communications has stated:

35. Unsolicited and nuisance communications have no regard for borders, yet policy and enforcement communities face roadblocks such as inconsistencies in legislation, technology that enables anonymity, and the specific needs of economies with varied levels of policy and enforcement experience … [It requires] the active participation and cooperation of all stakeholders, including regulators; enforcement agencies; the private sector; and interested third parties, such as academia and non-profit organizations.[15]

36. There is a need for ongoing telco industry and government engagement with the proposed taskforce to inform what intelligence is valuable and how it is best disseminated to relevant agencies.

Action 2.6—Implement and update SMS filtering technology

37. Although not as prolific as scam calls, scams delivered by SMS and email, including phishing SMS, cause significant detriment.[16]

38. Technology companies that provide fraud protection solutions to the telco industry have demonstrated comprehensive solutions at a network level that automatically detect and block scam messaging and emails.

39. The technology leverages off big data and the visibility of scam activity across multiple telco providers in multiple countries.

40. One domestic telco provider consulted demonstrated an impressive ability to monitor, analyse track and disrupt spam/scam SMS traffic on its network by implementing filtering technology supplied by a fraud protection provider.

41. Combining the technology with human analysis enabled the accurate identification and blocking of illegitimate SMS. Figure 1 shows the decline in spam/scam SMS traffic post implementation of the filtering technology for the telco provider concerned.

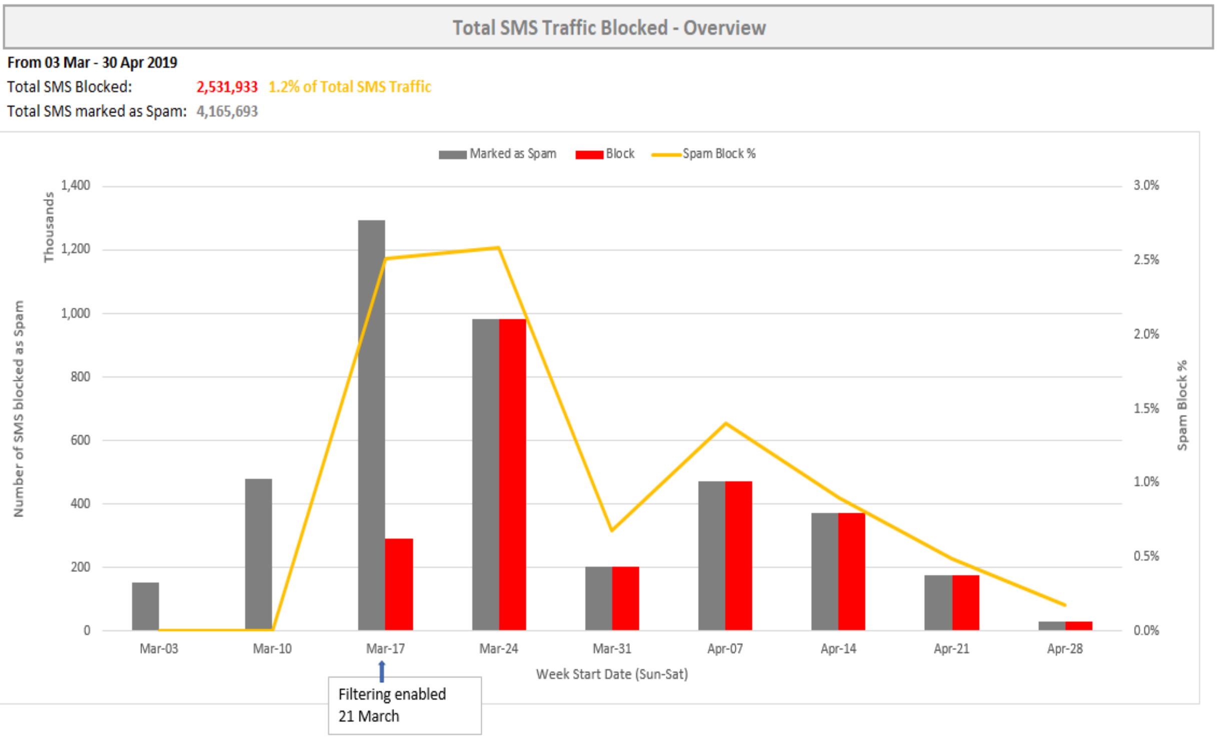
[13] Unsolicited Communications Enforcement Network (UCENet) is a network of global regulatory and enforcement agencies responsible for regulating unsolicited communications.

[14] UCENet Memorandum of Understanding on international cooperation, 2016, accessed 23 August 2019.

[15] CRTC, 'Collaborating to Eliminate Spam and Nuisance Communications', 11 October 2016, viewed 23 August 2019.

[16] Top scam contact methods in 2018: Email - 23.2% ($25.3 million lost), SMS - 14.4% ($2.1 million lost). ACCC, *Targeting Scams Report of the ACCC on scams activity 2018*, 2018, viewed 23 August 2019.

Figure 1: Reduction in scam SMS post implementation of filtering technology



Action 2.7—Monitor broader technological development and international initiatives for potential implementation

42. The project has considered a range of promising international innovations and technological solutions to reducing scams, including emerging initiatives such as:

> the development of authentication protocols to build confidence in telephony in the US (see discussion below)

> successful Do Not Originate list initiatives to reduce scams using the brands and telephone number assets of trusted entities like tax agencies in the UK and US

> measures to successfully identify and block ‘Wangiri’ call-back scams by some international telco providers and private entities.

43. The US and Canada have focused on CLI authentication as one means to combat scam calls. Since 2014, the Federal Communications Commission (FCC) has taken a co-regulatory approach and has encouraged the telco industry to develop a solution to prevent scam calls and over-stamped calling numbers.

44. The telco industry’s response has been to develop two new technical standards called STIR (Secure Telephony Identity Revisited)[17] and SHAKEN (Secure Handling of Asserted information using toKENs).[18] Under the STIR/SHAKEN framework, calls traveling through interconnected phone networks would have the CLI ‘signed’ as legitimate by the originating carrier and validated by other carriers before reaching consumers.

[17] STIR is a working group of the Internet Engineering Task Force (IETF).

[18] SHAKEN is formally known as the Alliance for Telecommunications Industry Solutions (ATIS) Standard on Signature-based Handling of Asserted Information Using Tokens. ATIS is accredited by the American National Standards Institute.

45. The framework digitally validates the transfer of phone calls passing through a complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is from the originating caller.

46. The FCC in the US has set December 2019 as the industry-wide implementation date for STIR/SHAKEN. At a robocall summit in July 2019, industry representatives informed the FCC that the standards are at an advanced stage of implementation and that they were already seeing the benefits that STIR/SHAKEN provides to improve call analytics.[19]

47. Canada and the UK have endorsed this framework and the rate of international adoption is to be discussed at the 2019 Session Initiation Protocol Network Operators Conference (SIPNOC), an Internet Protocol (IP) system industry conference, in December 2019.[20]

48. STIR/SHAKEN standards are reliant on being deployed in an end-to-end IP network, therefore they have restricted application presently in Australia.[21] As networks continue to migrate from copper wire based PSTN networks to the National Broadband Network (NBN), implementation will increasingly become a realistic option to be considered by industry. It is recommended that the potential for application of these standards in the Australian context be actively monitored.

49. It is noted that technologies such as STIR/SHAKEN are not a 'silver bullet' solution to combating scams. They provide a marker of authenticity only. As one of the architects of the STIR/SHAKEN framework describes its application to scam calls:

50. It's more like email spam. It's still there, but it's more manageable now. We have the tools in place that the curve will peak and begin to go down to a manageable level.[22]

51. Apart from authentication protocols, scam disruption is an area ripe for further innovation. Artificial intelligence, algorithmic or code-based regulation and applications relying on crowd-sourced data may all inform effective future scam reduction initiatives. As scams are an international problem in origin and impact, it is important that overseas initiatives are monitored for potential implementation in the Australian context.

Action 2.8—Provide advice and information to customers

52. Scam activity has a significant social and economic impact on Australians. The ACCC's Scamwatch data shows reported losses will exceed a record $532 million by the end of 2019.[23] However, the total loss is likely to be higher as many scams go unreported.

53. The emotional distress caused by scams can also be devastating. As support charity, Life After Scams states:

> Behind these mind-boggling statistics are real human beings, who are crippled by debt, traumatised by their ordeal and stuck wondering how to rebuild their lives.[24]

[19] Federal Communications Commission, *'SHAKEN/STIR Robocall Summit'*, 2019, viewed 28 August 2019.

[20] SIP Forum, *'SIPNOC 2019 Focus on STIR/SHAKEN'*, 2019, viewed 30 August 2019.

[21] Under Universal Service Obligation (USO)agreements, Telstra is committed to operate and maintain its existing copper network in areas where the NBN fibre fixed line network will not be deployed until 2032. Telecommunications contract and grant registers, viewed 30 October 2019.

[22] L. Hay Newman, 'The Robocall Crisis Will Never Be Totally Fixed', *Wired*, 4 July 2019, viewed 19 September 2019.

[23] Scamwatch, *'Record losses expected as scammers target Australians'*, 2019, viewed 23 August 2019.

[24] Productivity Commission, '*Life After Scams Submission to Productivity Commission*', 2019, viewed 29 August 2019.

54. As noted by Telstra CEO Andy Penn on 13 September 2019:

> [P]erhaps the most effective response is informed and empowered consumers. Consumers who are alive to the risks and part of the response.[25]

55. It is therefore important that consumer awareness initiatives continue to be provided, if not expanded, in addition to implementation of new disruption measures. Consumers must have accessible educational and awareness raising material. It must be provided through a range of channels, to a range of audiences, including those in vulnerable circumstances.

56. Many telco providers are taking steps to raise customer awareness about scams generally, and, on a more targeted basis, about specific scams that may involve their networks and customers. For example, Vodafone provides a webpage that is regularly updated to detail current scams and provides information about where to report scams.[26]

57. There is general agreement that industry has a key role to play to keep their customers informed and aware, including about products or services that may assist them to manage scam calls.

58. Internationally, call blocking handsets, filters for landline services and call filtering applications for mobile phones are available and promoted by telco providers to their customers. Domestically, some telco providers also offer products to assist customers manage calls. For example, Telstra offers a range of products to assist management of unwanted calls, including its Call Guardian handsets that block numbers using a proprietary technology.[27]

59. This report proposes that new regulatory obligations include requirements for telco providers to offer information to customers to assist them to manage scams, including information about any products or services offered by the CSP. Ideally, this information would be provided at multiple points in the customer experience, including at point of sale, online, at billing and, potentially, via other contact channels (for example, SMS and social media).

60. The project also recognises that government, as a trusted information source, has a role to play in developing comprehensive and consistent advice. Scamwatch, Stay Smart Online and the ACMA all provide awareness raising material about scams to consumers, as do other government departments like the ATO and Department of Human Services. The ACCC's *Little black book of scams* is one particularly noteworthy and comprehensive example of scam awareness raising.[28]

61. The ACMA and ACCC will consider how to build on available material with additional information on 'How to block' unwanted calls for promotion and dissemination through industry and consumer group channels. This work may usefully leverage the consumer awareness material already provided by the ACCC and recent consumer material on how to manage unwanted calls developed by the Federal Trade Commission in the US.[29]

62. The latter materials (see Figure 2), include infographics targeted at landline, mobile and VoIP users as well as explaining malicious CLI spoofing. In the US, this initiative supports existing consumer resources provided by industry such as

[25] Telstra, *'Tackling the changing face of customer service'*, 2019, viewed 24 September 2019.

[26] Vodafone, '*Scams and hoaxes*', viewed 23 August 2019.

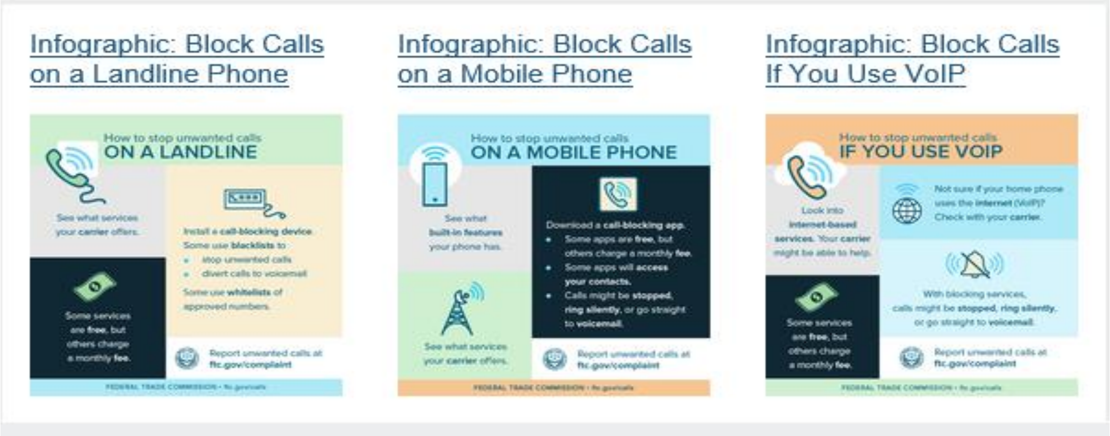
[27] Telstra, '*Unwanted call types*', viewed 23 August 2019.

[28] ACCC, '*The little black book of scams'*, 2016, viewed 23 August 2019,

[29] Federal Trade Commission, '*How to Block Unwanted Calls'*, 2019, viewed 19 August 2019.

the Cellular Telecommunications Industry Association's guide `How to Stop Robocalls'.[30]

Figure 2: Example of FTC 'How to block' consumer education material


Infographic: Block Calls on a Landline Phone
How to stop unwanted calls
ON A LANDLINE
See what services your carrier offers.
Install a call-blocking device. Some use blacklists to
stop unwanted calls
divert calls to voicemail
Some use whitelists of approved numbers.
Some services are free, but others charge a monthly fee.
Report unwanted calls at ftc.gov/complaint
FEDERAL TRADE COMMISSION • ftc.gov/calls
Infographic: Block Calls on a Mobile Phone
How to stop unwanted calls
ON A MOBILE PHONE
See what built-in features your phone has.
Download a call-blocking app.
Some apps are free, but others charge a monthly fee.
Some apps will access your contacts.
Calls might be stopped, ring silently, or go straight to voicemail.
See what services your carrier offers.
Report unwanted calls at ftc.gov/complaint
FEDERAL TRADE COMMISSION • ftc.gov/calls
Infographic: Block Calls If You Use VoIP
How to stop unwanted calls
IF YOU USE VOIP
Look into internet-based services. Your carrier might be able to help.
Not sure if your home phone uses the internet (VoIP)? Check with your carrier.
With blocking services, calls might be stopped, ring silently, or go straight to voicemail.
Some services are free, but others charge a monthly fee.
Report unwanted calls at ftc.gov/complaint
FEDERAL TRADE COMMISSION • ftc.gov/calls

63. It is also noted that provision of consumer awareness and safeguard information is considered in the Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Direction 2019 which requires the ACMA to determine an industry standard requiring all mobile carriage service provides to implement enhanced pre-porting identity verification measures. Optimally, consumer information about how to address scams will be consolidated and readily accessible.

Action 3—Immediate trial of Industry-wide scam reduction initiatives

64. Notwithstanding the proposed development of enforceable obligations, there is a need for, and opportunity to take, immediate action on certain scams types to accelerate reduction outcomes and reduce their impact on Australians in the short term.

65. The ACMA is proposing an immediate trial of three scam reduction initiatives identified in consultation with industry as having the potential to reduce scam activity in the short to medium term. The initiatives have been directly informed by international approaches.

66. The ACMA will work with industry and other key stakeholders to facilitate the trials, and their effectiveness will be monitored by the proposed taskforce.

67. The proposed scam reduction trials are discussed below at a high-level. Detail has been redacted from this public report.

Action 3.1—Implement a trial 'Do Not Originate List'

68. High-profile, trusted brands, including the ATO, have been secondary targets of scams that spoof numbers that have been issued to them. The approach is used by scammers to gain trust, e.g. that the number calling is from a verifiable and trusted party.

69. In cases where a party calls the number back, they sometimes direct abusive feedback to the otherwise unaware legitimate number holder. The problem is also evident when residential or business numbers are used by scammers and the legitimate entities receive abusive feedback and high call volumes.

[30] Cellular Telecommunications Industry Association, '*How to Stop Robocalls*', viewed 19 August 2019.

70. Overseas experience, and very limited trials in Australia, have indicated a DNO List may help reduce use of trusted brands to perpetrate scams and help eliminate impacts on innocent third parties.

71. This DNO list trial, involving the ATO, will explore industry-wide network solutions to:

> block scam calls using CLI issued to trusted brands/high profile targets where it can be verified they are being used by malicious actors

> restore consumer confidence in calls from trusted brands

> test future viability for wider roll-out, including, potentially to SMEs and consumers whose numbers have been used.

Action 3.2—Identify and block 'Wangiri' call-back scam calls

72. 'Wangiri' is a Japanese word meaning 'one ring and drop'. The 'wangiri' or call-back scam targets mobile phone users – cutting off the call just as the phone rings, leaving a missed call message, often from an international number.

73. When the phone user calls back, the call is routed to a premium-rate service, incurring high charges. The 'wangiri' scam is a global problem.

74. Due to the unique characteristics of 'wangiri' scam calls, technological solutions can potentially be used to identify and block the call. Wangiri scam calls are typically high-volume, short duration calls eliciting a call back.

Action 3.3—Block traffic from providers carrying a high-volume of scam calls using commercial interconnect arrangements

75. High-volumes of scam calls enter Australian from off-shore locations via a complex web of call routing/IP based traffic and supporting commercial interconnect arrangements.

76. In general, a carrier or CSP is only able to determine the previous provider that carried a call, whereas it may have travelled through many transit points from origin to termination.

77. To significantly reduce the amount of scam traffic that enters and/or is carried on Australian telecommunication networks via promoting disincentives. A supporting objective is to enable identification of carriers and CSPs with high-volume scam traffic.

78. Commercial interconnection agreements are already being used by some carriers in Australia to reduce scam activity. Internationally, major providers in the United States of America have recently adopted principles about tracing scam calls (see Appendix B).

Appendix A: Scam technology project – Terms of Reference

Context

The Australian Communications and Media Authority (ACMA) will, in consultation with key stakeholders, undertake a Scam Technology Project (the Project) to explore practical technological solutions to address the proliferation of scams over Australian telecommunications networks.

The Project addresses:

> a request for assistance from the Minister for Communications and the Arts (the Minister) to identify realistic options for addressing consumer harms caused by international scam callers

> Finding 10 of the ACMA's report to the Minister on the potential for industry self-regulation of commercial electronic messages, the Do Not Call Register and the Integrated Public Number Database

> Recommendation 3 of the Communications sector market study final report by the Australian Competition and Consumer Commission (the ACCC).

The ACMA's report found that 'scam unsolicited communications are a significant issue for consumers and ongoing work across government and industry is required to reduce the impact'.

The ACMA's 2018 consumer experience research[31] found that there was greater concern about scam calls than all other types of unsolicited calls, and more than half of Australian adults who reported receiving a scam call on their landline in the past six months were receiving them daily or weekly. The research also found that more than three-quarters of Australian adults feel not enough is being done to protect individuals from scam calls.

Consumer complaints about scams are the number one complaint type to the ACMA in relation to the *Do Not Call Register Act 2006* and the *Spam Act 2003*. In 2017–18, more than 26 per cent of complaints about telemarketing and spam concerned scams.

The ACCC's market study recommended that 'telecommunications industry members must, as a priority, collaborate with regulators and government agencies to develop and implement technical solutions at the network level to protect consumers from the significant harm that flows from spoofing and related scams'.

The Project will investigate what can be done to disrupt scam activity, including possible consumer or network-based solutions like call/message/email blocking, sharing of information, network traffic analysis and authentication protocols.

Terms of Reference

The ACMA will examine available and potential technological solutions that could disrupt and reduce the level and severity of scams being perpetrated over telecommunications networks. As part of its examination, the ACMA will consider:

[31] ACMA, '*Unsolicited calls in Australia: Consumer experience*', 2018, viewed 23 August 2019.

- existing and emerging technologies that enable scams to be perpetrated against Australians
- existing technologies that can reduce scam perpetration
- new or emerging technologies that could further reduce scams
- the costs and benefits of existing and potential solutions, implementation issues and timing
- international developments and approaches
- other relevant matters.

The Project recognises that many scams may involve a combination of contact methods. The Project will consider phone calls, SMS/OTT messages and email scams.

The findings will be made available to key stakeholders, including the Minister for Communications and the Arts. Public release of the findings, or extracts of the findings, will depend upon the commercial and security sensitivities of the matters canvassed.

Reference group

The ACMA will establish a reference group comprising representatives of the ACCC and the Australian Cyber Security Centre to support its undertaking of the Project. The Department of Communications and the Arts will participate in the reference group as an observer. Reference group members will provide strategic advice to the Project and insights from their associated work on scams.

The ACMA will also consult with other government agencies, the telco industry, large technology companies operating in Australia, organisations representing the interests of consumers, and international stakeholders with a role in addressing scams in the areas of telecommunications, consumer protection, law enforcement, cyber safety, cyber security and fraud.

Matters to which the ACMA will have regard

In undertaking the Project, the ACMA will have regard to:

- the importance of communications networks for the economic and social development of all Australians
- current policy and regulatory settings about scams
- international developments to reduce scams that are being supported by governments, industry and/or consumers
- any research on the concerns of consumers in relation to scams delivered over telecommunications networks
- advice from the reference group and other stakeholders
- the costs to consumers and industry of any potential solutions.

Out of scope

The following matters are out of scope for the Project:

- Scams perpetrated over the internet that are not initiated by an unsolicited electronic communication to a consumer (for example, online dating or shopping scams) and scams that are not perpetrated over communications networks (postal or in-person scams).

Reporting and timing

The ACMA will complete its preliminary examination by July 2019. A final report will be completed by December 2019.

Appendix B: Anti-Robocall Principles (US)

Principle #1. **Offer Free Call Blocking and Labelling**. For smartphone mobile and VoIP residential customers, make available free, easy-to-use call blocking and labelling tools and regularly engage in easily understandable outreach efforts to notify them about these tools. For all types of customers, implement network-level call blocking at no charge. Use best efforts to ensure that all tools offered safeguard customers' personal, proprietary, and location information.

Principle #2. **Implement STIR/SHAKEN**. Implement STIR/SHAKEN call authentication.

Principle #3. **Analyse and Monitor Network Traffic**. Analyse high-volume voice network traffic to identify and monitor patterns consistent with robocalls.

Principle #4. **Investigate Suspicious Calls and Calling Patterns.** If a provider detects a pattern consistent with illegal robocalls, or if a provider otherwise has reason to suspect illegal robocalling or spoofing is taking place over its network, seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name, terminating the party's ability to originate, route, or terminate calls on its network, and notifying law enforcement authorities.

Principle #5. **Confirm the Identity of Commercial Customers**. Confirm the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business.

Principle #6. **Require Traceback Cooperation in Contracts**. For all new and renegotiated contracts governing the transport of voice calls, use best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying its own customer if the call originated in its network.

Principle #7. **Cooperate in Traceback Investigations**. To allow for timely and comprehensive law enforcement efforts against illegal robocallers, dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from US Telecom's Industry Traceback Group. Identify a single point of contact in charge of responding to these traceback requests and respond to traceback requests as soon as possible.

Principle #8. **Communicate with State Attorneys General.** Communicate and cooperate with state Attorneys General about recognized scams and trends in illegal robocalling. Due to the ever-changing nature of technology, update the state Attorneys General about potential additional solutions for combatting illegal robocalls.

Appendix C: Common types of telephone scams

Automated messages or ‘robocalls’

Automated voice messages inviting a call back advising of imminent disconnection of telecommunications services such as broadband.

CLI over-stamping (malicious spoofing)

Scam calls may over-stamp the CLI of a call (which would generally display the number from which the call originates) to display a number that may be more familiar or recognisable to the person receiving the call. This makes it more likely that the call will be answered.

Fake offers

Scam callers may attempt to lure a consumer to transfer funds or give up personal information through fake offers for jobs, investments, products and charities.

Impersonation scams

Scammer present themselves as representing a government agency or known, trusted entity, in order to solicit information or money from the victim. Scammer will often maliciously spoof the CLI of the trusted entity they are impersonating to gain trust.

Mobile porting scams

Mobile porting fraud occurs when a scammer gains access to personal information and uses it to transfer a mobile phone number to them. The malicious actor then tries to use the number to impersonate the consumer for personal gain.

SMS phishing

Scam SMS/MMS use fake information, trusted/well-known brands and spurious links leading to malware or locations where criminals can steal personal information. Impersonation and gaining trust are a key tactic of phishing scams.

Threats, extortion and offers of assistance

Calls may include threats to extort money out of consumers (such as fake tax debt scams) or fake offers of assistance (such as remote-access computer assistance scams). These scams attempt to obtain personal information from consumers and/or have consumers transfer funds to the scammer.

‘Wangiri’ one ring scam

This type of scam involves many telephone calls of very a short duration (i.e. the call may ring once only) to entice a call-back, usually to an overseas number. The short duration of the call means most calls will go unanswered. Return calls incur a high charge—the longer the call, the higher the charge.

Appendix D: Glossary

ACCC (Australian Competition and Consumer Commission)
Commonwealth regulatory body with responsibilities derived from the *Competition and Consumer Act 2010 and administration of Scamwatch.*

ACMA (Australian Communications and Media Authority)
Australian Government statutory authority within the communications portfolio.

ACSC (Australian Cyber Security Centre)
Commonwealth Government's lead agency on national cyber security.

Communications Alliance (Communications Alliance Ltd)
Peak telecommunications industry organisation.

CLI
Calling Line Identification or caller ID enables telephone number of calling number to be displayed. Carriers and carriage service providers (CSPs) in the telco industry use CLI for the routing of telephone calls (e.g. for inbound calls) and billing of services.

Department of Communications and the Arts
Department of the Australian government responsible for communications policy and programs and cultural affairs.

IP (internet protocol)
Principal internet communications protocol tt defines the format of packets and provides an addressing system.

NBN (National Broadband Network)
Australian national wholesale-only open-access data network operated by NBN Co Limited.

Numbering plan
The *Telecommunications Numbering Plan 2015* which specifies telephone numbers for use in Australia and the arrangements for allocation, surrender and withdrawal of those numbers.

OTT (over-the-top applications)
Any app or service that provides a product over the internet bypassing the network operator.

Over-stamping (spoofing)
The practice of causing the caller ID to present as a number different from which the call originates. This can be used maliciously to make a call falsely appear to be from a trusted or local source.

phishing
The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, i.e. passwords and credit card details

PSTN
The public switched telephone network is the collection of traditional (or legacy) circuit-based telephone infrastructure operated by local, national and international carriers.

SHAKEN
Secure Handling of Asserted information using toKENs (SHAKEN)is a technical standard used for phone call authentication.

SMS (short message service)
A mobile telecommunications data transmission service that allows users to send short text messages to each other using a mobile handset.

spam
Unsolicited commercial electronic messages sent by email, SMS, MMS and/or instant messaging.

STIR
Secure Telephony Identity Revisited (STIR) are technical standards developed for call authentication.

telco provider
A company that provides consumers with access to a communication service.

UCENet
Unsolicited Communications Enforcement Network. A network of global regulatory and enforcement agencies responsible for regulating unsolicited communications.

VoIP—voice over internet protocol
Delivery of voice communications over the internet or some other connected network, instead of the PSTN.

Wangiri
Japanese word meaning ‘one ring and cut’.