5.2 SCAM REDUCTION ACTIVITIES, INC. SENDER ID REGISTRY

LEAD/SUPPORT: JEREMY FENTON | TANYA FARRELL

The Australian Communications and Media Authority (ACMA) is working to disrupt scams before they reach Australians. We are exploring new disruption initiatives and enforcing anti-scam rules. We are working closely with industry, government agencies and international counterparts to protect Australians.

KEY ISSUES

- The government announced on 23 April 2023 that, as part of its Fighting Scams initiative, the ACMA will implement an SMS sender ID registry (with total budget announced of $10.9 million over 4 years, plus $2.2 million per year ongoing). We anticipate that phase one will commence in December of 2023.

- The ACMA is concerned about rising levels of scam activity on digital platforms (where we currently have no powers to address scams). We are working across government on potential solutions and are also directly engaged with major platforms on the issue.

- Telcos have reported blocking over 1.4 billion scam calls and 257 million scam SMS under ACMA registered rules to 30 June 2023. Telcos are due to provide updated stats to the ACMA at the end of October for the July to September 2023 period. The criminal syndicate-driven industrial scale and sophistication of scam activity targeting Australians requires an ongoing, adaptive and multi-faceted approach to disruption by industry and government. Promisingly, more scams are being blocked each quarter as a trend over time.

- The ACMA is actively supporting the work of the Australian Competition and Consumer Commission (ACCC) to implement the National Anti-Scams Centre (NASC).

Sender ID registry

- An SMS sender ID registry will protect the alphanumeric message headers (shortened business names or related tags, such as 'ATO' or 'NAB') of brands and government agencies from impersonation by scammers. It will complement existing protections and make SMS with alphanumeric message headers trustworthy for consumers.

- Impersonating Sender IDs is a key technique used by scammers to gain consumer trust, as the messages appear legitimate because they display in brand message threads on consumer devices.

- The ACMA is implementing the registry in phases, so that initial protections are in place as quickly as possible.

- Phase 1 involves the consolidation and expansion of existing provider-level initiatives to prevent SMS scam impersonation and is scheduled to commence in December 2023, subject to trialling, and telco industry and brand readiness.

- Phase 1 will be voluntary, without legislative underpinning. Telco providers, along with brands most at risk of scam impersonation, will be encouraged to participate to provide consumer and brand protections as soon as possible. During this phase, brands will not be charged to participate.

- It is anticipated that phase 2 will commence in the latter part of 2024, after the introduction of required supporting legislation and subject to trialling and industry and brand readiness. Cost recovery arrangements will commence in phase 2.

- The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (the Department) is currently developing supporting legislation to provide a head of power for the registry to be operated and cost recovered.

2023–24 Budget

- As part of the 'Fighting Scams' budget measure, funding of $10.9 million ($10.5 to ACMA, and $0.4 to the Department) is being provided. $4.3 million has been allocated to the ACMA in the first year to develop the scheme ██

- An excerpt of Budget Paper No. 2 showing the full 'Fighting Scams' measure is at **Attachment A**.

Scams on digital platforms (also covered in **Cross Divisional Executive brief 3.2**)

- The ACCC's Scamwatch data shows that for the 2023 calendar year (as at 31 August 2023), reported losses on social networks have increased by approximately 40% (to $71.4M) and on mobile apps by approximately 16% (to $52.1M) compared to the same period for 2022.

- In 2022, reported losses on social networks increased by approximately 43% (to $80.2M) and on mobile apps by approximately 98% (to $71.6M) compared to 2021. (See **Attachment F** for related Question on Notice (QoN)).

- The ACMA does not have regulatory powers to address scams on digital platforms. We have raised this in submissions to the ACCC's Digital Platform Services Inquiry (the Inquiry), and Treasury's consultation on the ACCC's regulatory reform recommendations from the fifth interim report of the Inquiry.

- Legislative changes would be required to give the ACMA powers to regulate scams on digital platforms and over-the-top apps. These could include powers for rule making or code registration, information gathering, record keeping, and enforcement. (See **Attachment E** for QoN about scams on digital platforms).

- We continue to raise scam matters with Meta, X (formerly Twitter) and Microsoft (Skype) regularly and the ACCC has consulted publicly on these matters through the Inquiry.

Successes to date

- The ACMA has made or registered new enforceable obligations on telcos to prevent scams reaching Australians, make the country a harder target and disrupt the economics of the scammers 'business' model. Key actions are set out in table 1 below:

Table 1: Key scam disruption activities to date

Start date	Action	Impact
30 April 2020	Multi-factor ID rules to prevent mobile porting fraud in the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard	95% reduction in these types of scams
2 Dec 2020	Rules that require telcos to identify, trace and block scam calls in the Reducing scam calls industry code	1.4+ billion calls reported as blocked from 2 December 2020 – 30 June 2023
30 June 2022	Multi-factor ID rules to prevent scammers accessing high-risk interactions between telcos and customers, e.g., SIM swaps and password changes, in the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022	70+% reduction in these types of scams
12 July 2022	Rules that require telcos to identify, trace and block SMS scams in the Reducing scam calls and scam SMS industry code	257+ million SMS reported as blocked from 12 July 2022 – 30 June 2023

- The ACMA has developed and continues to disseminate a comprehensive suite of consumer awareness-raising materials about how consumers can spot and stop phone scams. The material is available in versions for First Nations Australians and in simplified Chinese, traditional Chinese, Arabic, Vietnamese and Italian.

- We anticipate that our educational material will be reviewed and adapted to be consistent with advice from the NASC in due course.

- The ACMA proactively issues scam alerts to consumers, predominantly via online and social media, to raise awareness of emerging or high-risk scams about which we are aware. Key alerts issued in the 2023 calendar year are at **Attachment B**.

Other current anti-scam activities

- The ACMA is actively enforcing rules and working closely with industry, trusted brands, government agencies and international regulatory partners to disrupt scams. Some of this work is public and some occurs behind the scenes.

Compliance and enforcement activities

- As part of the ACMA's current compliance priorities, we have been auditing telcos that send bulk SMS as a potential conduit of SMS scams onto Australian networks. We have found non-compliance with rules that require telcos to confirm that the senders of bulk SMS have a legitimate case to use sender IDs, such as shortened business names.

- In some cases, there is direct evidence the vulnerabilities created by the non-compliance has been used by scammers to send high profile SMS scams to Australians. Key results are:

- o 41 SMS aggregators have been audited. We have finalised 29 assessments, with 12 still in train
- o the audit has resulted in 15 investigations under the Reducing Scam Calls and Scam SMSs Code – 9 are finalised and 6 are in train
- o we have taken enforcement action in 7 of the 9 finalised investigations, including giving 6 directions to comply and issuing 1 formal warning
- o in 4 of the finalised investigations, we found evidence that scammers have exploited non-compliance to send high profile SMS scams to Australians.
- Enforcement outcomes are:
  - o published directions to comply include Sinch Australia Pty Ltd, Known Pty Ltd and Infobip Information Technology Pty Ltd
  - o Phone Card Selector Pty Ltd was formally warned
  - o there are 3 further entities that have been issued with directions to comply, however these are not yet published
  - o penalties of up to $250,000 apply for breaching directions to comply with the obligations.

Collaboration with industry

- We are actively engaged with telcos on a range of scam disruption matters, including:
  - o providing de-identified complaint data to facilitate identification and blocking of scams (see blocked scam figures in Table 1)
  - o monitoring telco efforts to trace the origins of scam traffic (to effect blocking)
  - o sharing information and intelligence about current and emerging scam threats, including via regular intelligence reports and the ACMA's Scam Telco Action Taskforce, which last met in September 2023
  - o assisting well-known brands and government agencies to engage with telcos to protect their numbers and Sender ID from impersonation
  - o telco capability uplift, including the introduction by key telcos of AI or machine learning to automate and enhance the identification and disruption of scams.
- An example of a new industry initiative to combat scams involves Telstra preventing the misuse of its customers numbers on its network. For all calls presenting these Numbers that do not originate on Telstra's network, Telstra intervenes at the network layer before the caller can be connected. ███████████████████████████████████
- Another example is the Australian Financial Crimes Exchange (AFCX) and Optus running a joint initiative to block calls to phone numbers identified as being used by scammers. The initiative targets scam texts that impersonate banks by requesting call-backs on a phone number contained in the message.

- The ACMA has established formal mechanisms to obtain data from the AFCX to monitor for scam activity and inform compliance actions where warranted. The AFCX holds scam and fraud data from the financial sector.

Work across government

- The ACCC-led NASC launched on 1 July 2023 and will build its information sharing capabilities over the next 3 years. It has been set up to coordinate government, law enforcement and the private sector to combat scams, building on the work of the ACCC's Scamwatch service.

- The NASC will deliver better protection for Australian consumers and businesses by improving cooperation between government and industry to respond to increasingly sophisticated scam activity. It will facilitate partnerships between government and the private sector including telcos, digital platforms, and payment system participants (See **Attachments C** and **D** for previous QoNs about the NASC).

- The NASC will run scams disruption Fusion Cells, which the ACCC defines as time-limited taskforces designed to bring together expertise from government and the private sector to take timely action to address specific, urgent problems. The NASC will coordinate a series of fusion cells with different participants to target particular scam types.

- The ACMA is supporting the ACCC's implementation of the NASC, including through being a member of the NASC's:

  o Regulator Steering Group, which ensures key regulators (ACCC, ACMA and the Australian Securities and Investments Commission [ASIC]) have the opportunity to collaborate with and contribute to the NASC program

  o The Regulator Operational Coordination Group (ACCC, ACMA, ASIC, Australian Tax Office [ATO], AUSTRAC and Attorney-General's Department [AGD]), which provides support to the Regulator Steering Group.

- The ACMA has also been an observer in NASC meetings on the Fusion Cell for disruption of investment scams and the Advisory Board consisting of industry and consumer representatives.

- Aside from the ACCC, the ACMA has strong working relationships with other departments and agencies with roles in scam reduction, including ASIC, the ATO, and Treasury and the Australian Cyber Security Centre (ACSC). We have formal Memoranda of Understanding (MOU) with the ACCC, ASIC, and the ACSC to facilitate collaboration and intelligence sharing.

International collaboration

- The ACMA is an Executive member of the Unsolicited Communications Enforcement Network (UCENet) (a global network of agencies engaged in combating unsolicited communications) and is a signatory to the UCENet MOU, which provides for engagement and information-sharing with agencies from the Republic of Korea, Canada, the United States of America, the Netherlands, the United Kingdom and New Zealand.

- The ACMA also has individual MOUs with the following agencies to formalise sharing of intelligence and best practice:

  o Federal Communications Commission, USA (May 2021)

  o Canadian Radio-Television and Telecommunications Commission (Dec 2021)

- o Department of Internal Affairs, New Zealand (June 2022)
- o Singapore Infocomm Media Development Authority (July 2022)
- o Information Commissioner's Office, UK (March 2023).

ATTACHMENTS

Attachment A	Excerpt of Budget Paper No. 2
Attachment B	ACMA scam alerts issued in 2023
Attachment C	QoN – 14 February 2023 - Timetable for National Anti-Scam Centre
Attachment D	QoN – 24 May 2023 – Correspondence between ACMA and the ACCC
Attachment E	QoN – 24 May 2023 – Submissions or documentation provided to the Minister and her office in relation to stopping scammers
Attachment F	QoN – 24 May 2023 – Change over the last five years in scams

<table>
<tr>
<td>

Contact Officer
Jeremy Fenton
Acting General Manager
Consumer Division
Ph (03) 9963 6909
████████████

</td>
<td>

Contact Officer
Tanya Farrell
Acting EM, Unsolicited Communications and
Scams Branch
Ph (02) 6219 5194
████████████

</td>
</tr>
</table>

Date 3/10/2023

Excerpt of Budget Paper No. 2 – 'Fighting Scams' measure

Treasury | **Budget** 2023–24

Fighting Scams

Payments ($m)

	2022-23	2023-24	2024-25	2025-26	2026-27
Australian Competition and Consumer Commission	-	18.5	23.6	15.9	-
Australian Securities and Investments Commission	-	4.8	4.2	4.2	4.4
Australian Communications and Media Authority	-	4.3	2.0	2.1	2.1
Department of Infrastructure, Transport, Regional Development, Communications and the Arts	-	0.2	0.1	0.1	0.1
Total – Payments	-	27.8	29.9	22.3	6.6
Related receipts ($m)					
Australian Securities and Investments Commission	-	-	4.8	4.2	4.2

The Government will provide $86.5 million over 4 years from 2023–24 to combat scams and online fraud. Funding includes:

- $58.0 million over 3 years from 2023–24 to establish the National Anti-Scam Centre within the Australian Competition and Consumer Commission to improve scam data sharing across government and the private sector and to establish public-private sector Fusion Cells to target specific scam issues

- $17.6 million over 4 years from 2023–24 (and $4.4 million per year ongoing) for the Australian Securities and Investments Commission (ASIC) to identify and take down phishing websites and other websites which promote investment scams, to be cost recovered through levies under ASIC's industry funding model

- $10.9 million over 4 years from 2023–24 (and $2.2 million per year ongoing) to the Australian Communications and Media Authority and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts to establish and enforce an SMS sender ID registry to impede scammers seeking to spoof industry and government brand names in message headers.

Partial funding for this measure will be held in the Contingency Reserve pending further development of ICT system requirements for the National Anti-Scam Centre.

This measure builds on the 2022-23 October Budget measure titled *Fighting Online Scams*.

ACMA scam alerts issued in 2023

Date of issue	Type of scam and brief description
13 Jan 2023	myGov impersonation scams – email and text messages impersonating myGov and associated government services that try to trick the recipient into clicking on a malicious link in order to claim a fake refund.
19 Jan 2023	'Hi Mum' SMS scams – a convincing variation of the lost phone/new number scams, which label the sender of the scam message as 'Mum' or another family member on your phone. This makes these scams difficult to distinguish from legitimate messages and they can slip into legitimate message streams.
25 Jan 2023	Optus impersonation scams (update) – new scam emails requesting consumers to click on a link to update their contact details for security reasons, or to pay an outstanding bill.
15 Mar 2023	Telstra impersonation emails – new scam emails requesting consumers to complete a form to avoid disruption or cancellation of their service
14 Apr 2023 25 May 2023 18 Aug 2023	ACMA impersonation scam calls – targeted at Mandarin speakers where callers impersonate the ACMA and other government agencies, claiming the consumer's phone number has been used to perpetuate a scam and will be disconnected.
4 May 2023	Remote access requests - callers pretending to be from well-known companies or government agencies, claiming there's a problem with an account or device and wanting remote access to fix it.
8 Jun 2023	Government impersonation scams - calls, emails or SMS asking recipients to urgently update personal information, claim a refund or make a payment.
3 Jul 2023	Tax scams – emails, SMS and calls claiming to be from the Australian Taxation Office requiring urgent payment of a tax debt, or requesting personal information in order to process a tax refund.
25 Aug 2023	Parcel delivery scams – SMS or emails asking recipients to update delivery details or requesting a fee for delivery.
7 Sept 2023	Fake invoice and bills scams – convincing emails impersonating well known businesses attempting to steal your financial information by getting you to pay a fake bill or subscription renewal.

Environment and Communications
QUESTION ON NOTICE
Budget Estimates 2022 – 2023
Infrastructure, Transport, Regional Development, Communications and the Arts

Departmental Question Number: SQ23-003198
Division/Agency Name: Australian Communications and Media Authority
Hansard Reference: Spoken, Page No. 63 (14 February 2023)
Topic: ACMA - Timetable for National Anti-scam Centre

Senator Ross Cadell asked:

Senator CADELL: It's a new one for me. I went to sell something on Facebook Marketplace the other day—it's a Mavic 2 Drone, if anyone's looking for one!—and suddenly got a message saying: 'Is this still available? I can't pay. Can I use PayID?' And there's another scam going over Messenger as well. And we have no ability to deal with that via ACMA or any other body?

Ms Rainsford: What we've been outlining here is that the role we play is effectively about disruption. Our goal in the telco space has been to take steps to prevent calls and SMS from hitting consumers. There is regulation in the ACCC around misleading and deceptive conduct. Of course, that is very difficult in a world where you've got, largely, overseas criminals who are sending those scams. Likewise, sometimes law enforcement is properly engaged in looking at scam activity there. Sorry, I've just lost my train of thought.

Ms O'Loughlin: I think that's also, Senator, why the government has announced a national antiscam centre— so we can pull together the elements of government, including us, who are not only looking at scams through different points of view but also getting industry into that discussion as well so we can share information and address scams more quickly.

Senator CADELL: What's the timetable for that centre to be finalised?

Ms O'Loughlin: It's being established by the ACCC, so I don't believe I have a date in my briefing pack. I'm happy to take that on notice.

Answer:

In the October 2022-23 Budget, the Government provided $9.9 million over 4 years from 2022–23 to the Australian Competition and Consumer Commission (ACCC) for initial work on the establishment of a National Anti-Scam Centre. The timetable for the Centre to be finalised is a matter for Government and the ACCC.

Environment and Communications
QUESTION ON NOTICE
Budget Estimates 2023 - 2024
Infrastructure, Transport, Regional Development, Communications and the Arts

Departmental Question Number: SQ23-003825
Division/Agency Name: Agency - Australian Communications Media Authority
Hansard Reference: Spoken, Page No. 98 (24 May 2023)
Topic: ACMA - Correspondence between ACMA and the ACCC

Senator Sarah Henderson asked:

Senator HENDERSON: Pulling in resources from other departments based in the offices of the ACCC—and I'm sure the ACCC does need more resources, because it's very much under strain—is not a centre. That is not an anti-scam centre as an ordinary Australian would interpret 'centre' to mean.

Ms O'Loughlin: I think it has a contemporary meaning which people would understand. We don't necessarily establish separate agencies to deliver on things, particularly when there is shared responsibility across the Commonwealth. We have different responsibilities with regard to scams. This will have us working together with industry and with other government agencies to deliver on it.

Senator HENDERSON: Would you be able to provide all correspondence in relation to the establishment of the so-called centre to the committee?

Ms O'Loughlin: I don't believe I have any correspondence. I think we've been talking to the ACCC. There have been budget announcements.

Senator HENDERSON: There must be correspondence between you and the ACCC about how this would be established.

Ms O'Loughlin: It's a process. It has been worked through by an IDC. I can certainly check for you, and I'll take it on notice.

Senator HENDERSON: Thank you. I would appreciate that.

Answer:

The Australian Communications and Media Authority (ACMA)'s engagement with the ACCC about the National Anti-Scam Centre has been through meetings, workshops and discussions. This includes participation in a Regulator Steering Committee that has been established, and is chaired, by the ACCC. There is no written correspondence between the Chair and the ACCC in relation to the establishment of the National Anti-Scam Centre.

Environment and Communications
QUESTION ON NOTICE
Budget Estimates 2023 - 2024
Infrastructure, Transport, Regional Development, Communications and the Arts

Departmental Question Number: SQ23-003826
Division/Agency Name: Agency - Australian Communications Media Authority
Hansard Reference: Spoken, Page No. 99 (24 May 2023)
Topic: ACMA - Submissions or documentation provided to the minister and her office in relation stopping these scammers

Senator Sarah Henderson asked:

Senator HENDERSON: Assistant Minister, that's not accurate. The proliferation of scams has really accelerated on the digital platforms only in recent times. I understand you are the representing minister; you are not the responsible minister. But I say to you, Assistant Minister, it is shocking that ACMA has been asking for these powers—desperately asking—and the ACCC chair has been desperately flying the red flag, saying, 'We need more powers.' They cannot rein in the digital platforms, the likes of Meta and Twitter and Google, without the powers. Assistant Minister, could I ask you—if you need to take it on notice, that's fine—to come back to the committee and urgently update the committee on what the government is doing? Back to you, Chair, could you please provide the submissions or documentation that you have provided to the minister and her office or the department in relation to the powers that you need to bring in and rein in the digital platforms when it comes to stopping these scammers?
Ms O'Loughlin: I'll take that on notice, Senator.

Answer:

The Australian Communications and Media Authority (ACMA) has not made written submissions to the Minister for Communications or her office or the department in relation to the powers to regulate scams on digital platforms. However, the ACMA has made several public submissions about this issue, at Attachments A to C of this response.

Attachments

A: Submission to the inquiry into the influence of international digital platforms

B: Submission to Treasury on ACCC Fifth Interim Report

C: Submission to ACCC inquiry social media services issues paper

Submission to the inquiry into the influence of international digital platforms

Australian Government | **acma**

Australian
Communications
and Media Authority

Red Building
Benjamin Offices
Chan Street
Belconnen ACT 2617

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555

acma.gov.au

Chair and Agency Head

Committee Secretary
Senate Economics References Committee
PO Box 6100
Parliament House
Canberra ACT 2600
via email: economics.sen@aph.gov.au

ACMA file reference: ACMA2019/1496-29

Dear Secretary,

Inquiry into influence of international digital platforms

The Australian Communications and Media Authority (ACMA) is the independent statutory authority responsible for the regulation of broadcasting, radiocommunications and telecommunications in Australia. The ACMA's remit also includes aspects of regulation of online content delivered by big tech companies. Our submission focuses on these matters: relevantly, the regulation of email spam, phone scams and the oversight the voluntary efforts of the Australian digital platform industry to address harmful mis- and disinformation.

The ACMA welcomes the opportunity to provide the Committee with a submission to this Inquiry. Please note, in addition to this submission, the heads of four independent regulators – the ACMA, the Australian Competition and Consumer Commission (ACCC), the Office of the eSafety Commissioner (OeSC), and the Office of the Australian Information Commissioner (OAIC) – have also provided a letter to this inquiry as part of the Digital Platform Regulators Forum (DP-REG).

Australians' use of digital platforms

The ACMA has a longstanding research program to track and monitor trends in the usage of media and communications services. For well over a decade, this work has included data on digital platforms, providing valuable longitudinal insights into the use and growth of these services in Australia.

More recently, in line with our increased regulatory focus on digital platforms, we have reviewed and expanded the scope of our annual consumer survey to capture more information on which specific services are being used, by whom, and for what purpose. This data is published as part of our annual *'Communications and media in Australia: How we communicate'* interactive report. The latest report shows that almost all Australian adults (95%) used at least one communications or social media service in the 6 months ending 30 June 2022, with Facebook (71%), Facebook Messenger (68%), and YouTube (65%) being the most popular platforms in Australia.

Our June 2022 consumer survey also included new questions on the consumption of news services across various platforms. These results show that more Australians access news from online sources (including social media services, news sites, and search engines) than on TV, radio or print. Further, nearly half of all Australians adults had sourced news from social media and

communications websites or apps in the previous 7 days. Given this, it is critical that digital platforms facilitate access to authoritative and reliable sources of news and information and take measures to reduce user exposure to false or deceptive content that can result in real-world harm to individual users or broader societal institutions.

Additionally, as part of our 2022-23 research work plan, the ACMA – in conjunction with members of the Digital Platform Regulators Forum (DP-REG) – is currently undertaking a standalone project examining Australians' experiences with the reporting and complaints processes of major digital platforms. Results from the first stage of this work – completed in January 2023 – indicate that 48% of Australians have seen or heard some form of harmful content while using these services over the previous 12 months, of which nearly half (48%) then made a report or a complaint with the platform about this content. The second stage of this project will be examining user satisfaction with these processes, and we expect to publish the results of this research in the coming months.

Misinformation and disinformation

The Australian Code of Practice on Disinformation and Misinformation (the code) is a voluntary initiative of the digital platform industry in Australia. This code requires signatories to develop and implement measures that reduce the propagation of, and potential exposure of Australian users to, harmful mis- and disinformation on their services. This code currently has 8 signatories, representing most of the major digital platforms operating in Australia: Adobe, Apple, Facebook, Google, Microsoft, Redbubble, TikTok and Twitter. The ACMA oversaw the development of the code and, as part of that process, published a position paper for industry which set out our expectations for the code and views on best practice approaches to self-regulation.

The code adopts an outcomes-based model rather than establish a series of prescriptive common rules. This provides individual platforms with flexibility on how they will achieve the code's objectives, while also improving levels of transparency and accountability across the digital industry without, for example, needing to regulate the operation of disparate, technically complex and dynamic platform algorithms. Under the code, all signatories are required to publish annual transparency reports that demonstrate how they have achieved the agreed outcomes and objectives of the code. Two sets of transparency reports have been published to date, with the next set due in May 2023.

The code administrator, Digital Industry Group Inc (DIGI), commenced a code review in mid-2022, and launched a revised version of the code in December 2022. Key changes include the broadening the definition of harm, new transparency commitments around the use of recommender systems, and the ability for greater participation by a wider range of industry participants – including companies offering digital advertising services or technology solutions to address mis- and disinformation.

In June 2021, the ACMA provided a report to government on our preliminary findings. This included an examination into the state and impact of online mis- and disinformation in Australia, with our research finding high levels of exposure to false and harmful narratives among users of digital platforms. As part of our targeted assessment into the development and likely effectiveness of the code, we noted concerns about the strength of the underlying governance arrangements and its general enforceability. As a result of these issues, we subsequently recommended that the ACMA should have a more formal role in

overseeing the operation of the industry code, supported by new information-gathering powers, and reserve code registration and standards-making powers should the voluntary code fail or provide inadequate.

Australian
Communications
and Media Authority

www.acma.gov.au

On 20 January 2023, Minister for Communications announced the government's intent to consult on draft legislation in the first half of 2023 to provide the ACMA with these new regulatory powers. If passed, this legislation will enable the ACMA to better assess the effectiveness of platform moderation activities, while incentivising greater participation and performance by industry under the existing code.

Importantly, the government has stressed that the focus of these powers will not be on policing or determining the truth of individual pieces of online content, but rather on the ACMA holding digital platforms to account based on the individual rules and policies of each platform. Digital platforms will continue to be responsible for the content they host and promote to users. This approach is designed to balance the need for stronger regulatory oversight of industry against the right to freedom of expression that is considered fundamental to a democratic society.

Relevant international developments

As part of its European Democracy Action Plan, the European Commission (EC) has developed an EU-wide strategy to combat disinformation and ensure the protection of European values and democratic systems. A key component of this work is the voluntary industry Code of Practice on Disinformation, which was updated and strengthened in June 2022.

In addition to the voluntary EU code, online mis- and disinformation in Europe is also regulated through the recently approved Digital Services Act (DSA). The DSA updates and harmonises the legal framework for regulating illegal content on digital intermediaries across the EU. It requires all online platforms with more than 45 million European users (known as Very Large Online Platforms, or VLOPs) to have measures in place to mitigate risks from the spread of illegal content. As a way to fulfil these mandatory DSA obligations, VLOPs can chose to sign up to the voluntary code and use this as a mitigation measure. The DSA is being overseen by a new European Board of Digital Services and the European Commission, which will have direct enforcement powers and be able to impose fines of up to 6% of a service's global turnover for breaches.

Outside of Europe, the UK Parliament is currently debating the Online Safety Bill (OSB). The bill is designed to protect children and adults online by making social media companies more responsible for their users' safety on their platforms. The latest version of the bill has removed earlier draft provisions that sought to shield adult users from material that is considered 'legal but harmful' (including misinformation) but will require platforms to take action against all illegal content. The OSB will also require the UK communications regulator, Ofcom, to establish an advisory committee to examine issues relating to mis- and disinformation.

The UK Parliament is also debating the National Security Bill (NSB), which will overhaul the UK's previous espionage laws. The NSB includes a new range of 'foreign interference' offences and updated investigative powers and capabilities to enable law enforcement and intelligence agencies to deter, detect and disrupt state threats. The NSB also proposes to add 'foreign interference' to the list of priority offences under the *Online Safety Act 2023*. This means that all platforms will have a legal duty to undertake risk assessments and take proactive,

Australian
Communications
and Media Authority

www.acma.gov.au

preventative action to identify and minimise people's exposure to state-sponsored or state-linked disinformation aimed at interfering with the UK.

Online scams and spam

Scams being perpetrated across digital platforms is a growing area of concern for the ACMA, and the broader community. Digital platforms are not captured by current regulations and evidence suggests scammers are pivoting from phone calls and texts to social media and applications. The ACCC's Scamwatch data shows that reported losses to scams in 2022 on social networks increased by approximately 42% and on mobile apps by approximately 98%. The ACCC's 2021 Targeting Scams Report found financial loss to scams over social networking and online forums increased almost 107% in 2021 to $56 million.

The ACMA has been taking steps to combat phone scams in Australia, including making rules requiring telecommunications providers to identify, trace and block scam calls and text messages.

Since the requirement to block scam calls came into effect in December 2020 until 31 December 2022, telecommunications providers have identified and blocked over 955 million scam calls. Consumer complaints about scam calls dropped dramatically in 2022 compared to 2021, with a 56% reduction in complaints to Scamwatch and a 62% reduction in complaints to the ACMA.

The new rules requiring telecommunications providers to identify, trace and block SMS scams came into effect in July 2022. Almost 90 million scam SMS were blocked in the first 6 months of operation.

However, these protections do not apply, and cannot be extended under current laws, to digital platforms. As it becomes harder for scammers to perpetrate fraud using calls and SMS, they are looking to exploit other channels. Digital platforms and messaging applications that are not required to prevent scams on their service will become an increasingly attractive target for scammers.

Consumers should be provided with appropriate safeguards to protect them from scammers across all channels. The ACMA would support the introduction of new laws that require digital platforms and messaging applications to identify and block scam activities, as is required for telecommunications providers.

Our regulatory collaboration efforts

The challenge of protecting Australians from online harms, particularly on global 'big tech' platforms, is complex and multi-faceted. The topic touches on a range of interconnecting issues and regulatory frameworks including user privacy, data protection, defamation, consumer protection, online safety, and the broader online information environment.

To facilitate better coordination across government on digital platform regulation, the ACMA – along with the ACCC, OeSC, and OAIC – formed the Digital Platform Regulators Forum (DP-REG) in early 2022.

DP-REG brings together considerable expertise on regulation of social media companies and provides a forum to help share information and work together jointly on cross-cutting regulatory issues. DP-REG's strategic priorities for 2022/23 include a focus on the impact of algorithms, efforts to improve transparency of digital platforms' activities, and increased collaboration and capacity building. The heads of the DP-REG regulators have also jointly

Page 4 of 5

provided a standalone submission to this inquiry, providing committee members with more information about this initiative.

Australian
Communications
and Media Authority

www.acma.gov.au

The ACMA also engages internationally on emerging regulatory issues relating to digital platforms, social media services and scams. The Media and Online Regulation Forum (MORF) brings together content regulators from Australia, Canada, Ireland and the United Kingdom, and meets quarterly. We are also a core member of the Unsolicited Communications Enforcement Network of internal regulators, ands have bilateral agreements in place to share strategic initiatives and collaborate with key internal regulators such as the USA's Federal Communications Commission and the Canadian Radio-television and Telecommunications Commission.

I hope this information may be of assistance as the Committee's inquiry progresses.

Yours sincerely

Nerida O'Loughlin PSM
15 February 2023

Submission to Treasury on ACCC Fifth Interim Report

Australian Government | acma

Australian
Communications
and Media Authority

Red Building
Benjamin Offices
Chan Street
Belconnen ACT 2617

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555

acma.gov.au

Chair and Agency Head

Director, Digital Competition Unit
Market Conduct Division
The Treasury
Langton Crescent
PARKES ACT 2600
Via: digitalcompetition@treasury.gov.au

ACMA file reference: ED23/2435

Dear Director

Digital Platforms: Government consultation on ACCC's regulatory reform recommendations

The Australian Communications and Media Authority (ACMA) welcomes the opportunity to provide a submission to Treasury's consultation on the Australian Competition and Consumer Commission's (ACCC) regulatory reform recommendations from the fifth interim report of the Digital Platform Services Inquiry (the Inquiry).

The ACMA offers the following observations to assist in Treasury's consideration of the Inquiry's recommendations.

Scams

As a sectoral regulator for the telecommunications industry, the ACMA's focus is on stopping scams before they reach Australians. To help achieve this outcome, we have introduced a suite of enforceable obligations on telecommunications providers, including rules that require them to identify, block and trace scam calls and SMS.

The ACMA's experience shows that working closely with the relevant industry and targeting scam activity on multiple fronts can achieve a meaningful and sustained reduction in the number of scams reaching consumers.

The summary of the ACMA's key actions at **Attachment A** demonstrates that the ACMA's actions to date have had a significant and swift impact, including that:

- over 955 million scam calls have been blocked from reaching Australians since December 2020, and almost 90 million scam SMS have been blocked since July 2022.
- consumer complaints about scam calls dropped dramatically in 2022 compared to 2021, with a 56% reduction in complaints to Scamwatch and a 62% reduction in complaints to the ACMA
- a 95% reduction in reports of mobile phone numbers being fraudulently ported to facilitate scams.

The ACMA's actions are currently limited to services regulated under the *Telecommunications Act 1997*. As such, they do not extend to scams perpetrated over other digital channels including through messaging applications operated by digital platforms or via online marketplaces.

The ACMA fully supports the ACCC's recommendation to introduce targeted measures to require digital platforms to take additional steps to prevent and remove scams being perpetrated on their platforms.

The ACMA favours a regime that applies to all digital platforms. An inconsistent application of anti-scam rules would likely create vulnerabilities that scammers could exploit and would undermine the effectiveness of any new rules. Such measures should have sufficient flexibility for regulatory responses to be tailored to the varying services provided by the relevant platforms.

The introduction of new laws which require digital platforms and messaging applications to identify and block scam activities would be of significant benefit to Australians, disrupt the scammers 'business' models and make Australia a harder target for scammers. The ACMA would be ideally positioned to administer such laws.

Complaint Handling

As the ACCC and Treasury have explained, there are considerable consumer harms attributed to digital platforms and across the digital ecosystem more broadly, including inadequate processes for dealing with disputes and complaints (hereafter referred to as complaints).

The ACMA has previously published its views regarding best practice for minimum complaint resolution standards in other contexts[1]. Of particular relevance, it has given its views on the handling of misinformation complaints in advice to government on the adequacy of digital platforms' disinformation and news quality measures[2] as well as the submission to the 2022 review of DIGI's Australian Code of Practice on Misinformation and Disinformation.[3]

The ACMA contends that complaint handling mechanisms should be, at a minimum, transparent, easily accessible and operated in good faith. Entities should have processes in place for internal escalated dispute resolution and identifying and addressing systemic issues that give rise to complaints. These complaint handling principles are applicable to, and should underpin the development of, minimum internal complaints handling obligations to be adopted by digital platforms.

In the first instance, platform users should be able to access an effective internal complaint handling processes to raise concerns arising from a failure on the part of a digital platform to meet their obligations to consumers and businesses. These obligations could derive from a range of sources including from regulation, industry/consumer codes (be they self-regulatory or co-regulatory) or platform's policies and terms of service.

The ACMA also considers that users should be able to access an external complaint handling mechanism for unresolved complaints where a platform user is not satisfied with the outcome of the platform's internal process. This is consistent with the complaints handling mechanisms provided in the telecommunications industry, whereby:

Australian
Communications
and Media Authority

www.acma.gov.au

---

[1] See, for example, page 18 of Part A of the ACMA submission to the DoCA Consumer Safeguards Review and pages 44 and 45 of the ACMA's What Audiences Want position paper.
[2] See ACMA, A report to government on the adequacy of digital platforms' disinformation and news quality measures, in particular pages 61-62.
[3] See ACMA, ACMA submission to the 2022 review of the Australian Code of Practice on Misinformation and Disinformation, in particular pages 25-27.

Australian
Communications
and Media Authority

www.**acma**.gov.au

1. Telcos are required to have internal complaint handling mechanisms which meet a minimum standard, with those standards set out in the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018*
2. There is a Telecommunications Industry Ombudsman which performs an escalated dispute resolution function
3. Telcos which have certain types of customers or business models are required to become members of the TIO Scheme, and
4. There are incentives built into the regulation and the TIO Scheme to encourage telcos to resolve complaints effectively and early.

The ACMA has also recently commissioned consumer research to better understand the experience of Australians when deciding if, and how, they make a report or a complaint about potentially harmful content (including misinformation) on digital platforms. The outcomes of this research are likely to be relevant to the matters raised in the Inquiry and we expect to publish our findings by mid-2023.

I hope this information is of assistance to the policy development process. The coming months will see the ACMA able to provide further assistance, as it learns more about its recently announced expanded powers to combat online misinformation and receives the results of the ACMA research into complaints about harmful content on digital platforms.

Yours sincerely

Nerida O'Loughlin PSM
16 February 2023

Attachment A: ACMA Phone Scams Work Program

Australian Government | acma

Australian
Communications
and Media Authority

ATTACHMENT A

ACMA Phone Scams Work Program

Since 2019, the ACMA has been actively using existing powers and resources to help protect consumers from telco scams and to help make Australia a hard target for scammers.

Only by a concerted effort to disrupt the channels used by scammers will we protect Australians by sufficiently impacting their 'business model'. An essential complement to this is the work of law-enforcement and victim-support organisations for those who are scammed.

The following table sets out the ACMA's key actions and impacts to date:

Date	Key action	Impact	Link
Nov 2019	*Combating Scams Action Plan* – 3 key recommendations: (1) Taskforce (2) Enforceable rules (3) Immediate trials	Scam Telco Action Taskforce set up & successful trial of scam reduction activity	Scam Technology Project
April 2020	New rules to prevent mobile porting fraud – requiring multi-factor identification	**95%** reduction in reported scams of this type	Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020
July 2020	Consumer awareness/ scam alerts (ongoing) & establishing mechanisms to obtain data (ACCC, ACSC, AFCX)	Widespread reach on social media, including to culturally and linguistically diverse and senior Australians	Phone scam educational resources Memorandums of understanding
Dec 2020	New rules requiring telcos to identify, trace and block scam calls	Over **955 million** scam calls blocked to December 2022 & **56-62%** reduction in complaints to the ACCC and ACMA in 2022 on last year's reports	New rules to detect, trace and block scam calls
April 2022	New rules to prevent SIM swap fraud – requiring multi-factor identification	Since the new rules came into force on 30 June 2022, the ACMA has seen a continuous downward trend in SIM Swap fraud reports	Telecommunications Service Provider (Customer Identity Authentication) Determination 2022
July 2022	New rules requiring telcos to identify, trace and block scam SMS	Almost **90 million** scam SMS blocked in the first 6 months since the rules came into force on 12 July 2022	C661_2022
Feb 2023	Commenced investigating the implementation of an SMS sender ID register	A registry would stop scammers impersonating the Sender ID of trusted brands such as banks, delivery companies and toll road providers	Announcement of SMS sender ID registry

Submission to ACCC inquiry social media services issues paper

Australian Government | **acma**

Australian
Communications
and Media Authority

Red Building
Benjamin Offices
Chan Street
Belconnen ACT 2617

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555

acma.gov.au

Chair and Agency Head

Secretariat
Digital Platforms Services Inquiry – March 2023 Report
Australian Competition and Consumer Commission (ACCC)
Via digitalmonitoring@accc.gov.au

ACMA file reference: ACMA2019/1496-27

Dear Secretariat,

ACCC Issues Paper – Digital Platform Services Inquiry – March 2023 Report on social media services

The Australian Communications and Media Authority (ACMA) welcomes the opportunity to provide a submission to the Australian Competition and Consumer Commission (ACCC) on its issues paper, and we look forward to continuing our close collaboration on common approaches to addressing online harms on social media services.

Since 2019, we have been involved in the development of the Australian Code of Practice on Disinformation and Misinformation (the code). As part of our ongoing oversight, we have a close working knowledge of the code and continue to monitor the progress of the digital platforms industry, including social media services, in addressing harmful content targeting Australians. This is a key area of focus under our compliance priorities for 2022-23:
https://www.acma.gov.au/compliance-priorities.

Online scams are another growing area of concern given the current lack of regulatory coverage on digital platforms and signs that scammers are pivoting from phone channels to social media and applications. Our existing work to combat phone scams has seen a dramatic drop in consumer complaints about scam calls, including a 50% reduction to the Scamwatch service and a 70% reduction to the ACMA in 2022. However, the protections introduced do not apply to social media platforms.

To inform our work in these areas and better understand the impact of digital platforms on the sectors we regulate, we undertake annual research and provide regular insights into the use of social media services in Australia.

Our social media research

The ACMA has a longstanding research program to track and monitor trends in the usage of media and communications services. For well over a decade, this work has included data on social networking or social media, providing valuable longitudinal insights into the use and growth of these services in Australia.

More recently, in line with our increased regulatory focus on digital platforms, we have reviewed and expanded the scope of our annual consumer survey to capture more information on which specific social media services are being used, by whom, and for what purpose. We welcome the inclusion of 2021 ACMA figures from our '*Communications and media in Australia: How we communicate*' report in the ACCC's issues paper:

Page 1 of 3

https://www.acma.gov.au/publications/2021-12/report/communications-and-media-australia-how-we-communicate.

Australian
Communications
and Media Authority

www.acma.gov.au

We have since completed our 2022 consumer survey, which included new questions on the consumption of news services on various platforms. These results show that more Australians now access news from online sources (including social media services, news sites, and search engines) than on TV, radio or print. Further, nearly half of adults sourced news from social media and communications websites or apps in the previous 7 days. Given this, it is critical that social media services facilitate access to authoritative and reliable sources of news and information, and take measures to reduce user exposure to false or deceptive content that can result in real-world harm to individual users or broader societal institutions.

While we anticipate publishing full results from this research in the coming months, we would be happy to separately brief the ACCC on these findings if it would be of interest or assistance to this inquiry.

Scams

The ACMA has been actively taking steps to combat phone scams in Australia, using powers under the *Telecommunications Act* 1997. This has included making new rules requiring telecommunications providers to identify, trace and block scam calls and text messages.

Since the requirement to block scam calls came into effect, telecommunications providers have blocked over 660 million scam calls, and there has been a significant drop in consumer complaints about scam calls. We are currently monitoring the impact of rules requiring telcos to identify and block scam text messages introduced in July 2022, but very early signs are promising.

Unfortunately, the nature of scam activity means that as it becomes harder for scammers to use calls and texts to perpetrate fraud, they will look to exploit other channels. This will include social media services and over-the-top services which do not have sector-specific regulations to deal with these issues. There is already strong evidence scammers are moving to these channels, with Scamwatch reported losses to scams in 2022 on social networks expected to rise approx. 20% and on mobile apps by approx. 164%.

The ACMA supports work to further explore the relationship between phone and online channels used by scammers and the potential for the introduction of scam disruption measures on social media platforms.

Our regulatory collaboration efforts

The ACMA closely collaborates with the ACCC and other government regulators via the Digital Platform Regulators Forum (DP-REG). DP-REG seeks to develop common approaches to dealing with potential harms caused by social media services, across the various regulatory responsibilities of its 4 members – the ACCC, ACMA, Office of the Australian Information Commissioner and Office of the eSafety Commissioner.[1]

---

[1] These responsibilities include competition, consumer protection, privacy, online safety and data issues; *DP-REG joint public statement*, March 2022.

Environment and Communications
QUESTION ON NOTICE
Budget Estimates 2023 - 2024
Infrastructure, Transport, Regional Development, Communications and the Arts

Departmental Question Number: SQ23-003827
Division/Agency Name: Agency - Australian Communications Media Authority
Hansard Reference: Spoken, Page No. 100 (24 May 2023)
Topic: ACMA - Change over the last five years in Scams

Senator Karen Grogan asked:
CHAIR: Your time is up. We're going to rotate the call. I will ask for one point of clarity. My understanding is scams have been increasing for years. Obviously, the more digital we become, the more it becomes more prevalent. What has been the pace of that change over the last five years?
Mr Fenton: I think we'd have to take that on notice for specific figures, but I think your characterisation that they have been increasing is accurate, and they've been fairly dramatically increasing across that period.

Answer:
While the number of reported scams to Scamwatch is falling, the combined losses reported to government agencies in 2022 were at least $3.1 billion, an 80% increase on total losses recorded in 2021 – see table below. Scamwatch data shows that in 2022 reported losses on social networks increased by approximately 43% and on mobile apps by approximately 98% compared to 2021. However, there are promising indications that efforts to reduce the impact of phone and SMS scams are working.
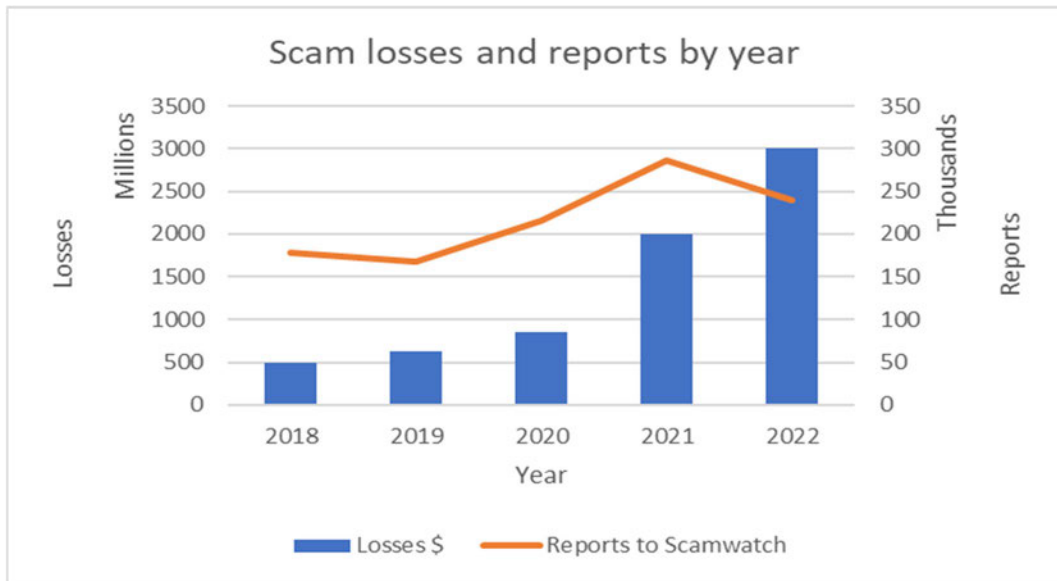
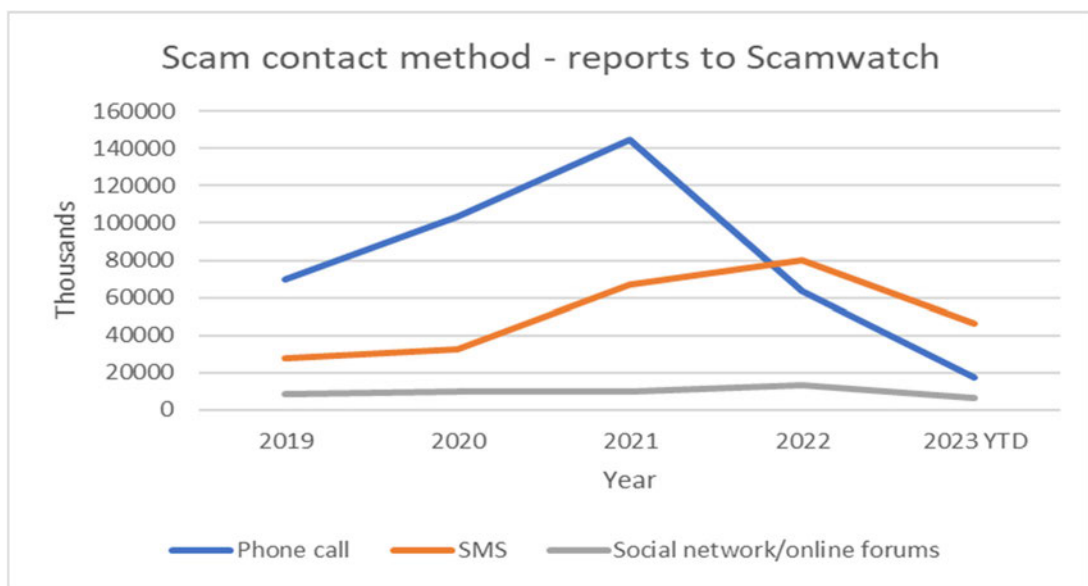Figure 1. Reported losses to scams and number of scam reports - ACCC Targeting Scams Reports 2018-2022.[1]

Figure 2. Scam contact methods reported to ACCC's Scamwatch 2019 to 2023 year to date.[2]

---

[1] Targeting scams: report on scams activity, ACCC, 2018-2022
[2] Scamwatch statistics, ACCC, 2019-2023.