Submission to the Parliamentary Joint Committee on Law Enforcement: *Inquiry into and report on vaccine related fraud and security risks*

May 2021

Introduction

The Australian Competition and Consumer Commission (ACCC) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement inquiry into and report on vaccine related fraud and security risks.

The ACCC provides the Scamwatch service, which includes the website www.scamwatch.gov.au, through which consumers can report scams. The ACCC monitors scam reports to understand and raise public awareness about scam trends and to provide intelligence sharing and disruption activities.

This submission will focus on those Terms of Reference that are most relevant to Scamwatch:

(a) Telecommunications and internet fraud relating to COVID vaccinations

(b) Criminal activity around the supply of fake vaccines, black market vaccines and/or fake vaccine certifications and the acquisition of certificates.

COVID-19 vaccine related scams

The ACCC has received reports of scams relating to the outbreak of the COVID-19 pandemic since 27 January 2020. Scammers have taken advantage of Australians' fears about the pandemic through phishing[1], selling false products and other types of scams. The ACCC's role in responding to COVID-19 scams has been to increase our level of monitoring and sharing of scam reports to support awareness raising and disruption activities.

With the earlier rollout of the COVID-19 vaccine, the United Kingdom and the United States of America, have identified a range of vaccine scams, including:

- Selling fake vaccine appointments
- Administering fake vaccines door to door for payment
- Asking for participation in fake vaccine surveys
- Asking for payment to ship vaccines to consumers
- Charging for a pre-test prior to getting a vaccine
- Putting your name on a waiting list to get a vaccine
- Tricking recipients into clicking on links in text messages stating they are eligible to receive the vaccine

Vaccine scams appear to target personal information which can be used to commit fraud at a later time or identity compromise. Based on the overseas experience we were expecting to see similar COVID-19 vaccine related scams in Australia. From 8 January 2021, the ACCC has received 58 reports about COVID-19 vaccination scams. We anticipate that reports to Scamwatch may increase as the vaccine rollout in Australia continues.

The ACCC has responded to COVID-19 vaccination scams by engaging in disruption, awareness raising and intelligence sharing in the following ways:

[1]Phishing is a range of techniques used by scammers to trick people into giving out personal information such as bank account numbers, passwords and credit card numbers.

- Providing advice and information to consumers via the Scamwatch website on COVID-19 vaccinations scams https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams/covid-19-vaccination-scams
- Sharing Scamwatch reports mentioning COVID-19 vaccination scams with key government stakeholders including Australian Cyber Security Centre (ACSC), Australian Federal Police, Services Australia, the Australia Communications and Media Authority, the Australian Criminal Intelligence Commission and the Australian Securities and Investments Commission.
- Daily monitoring for vaccination scam reports and taking action in the form of a warning via social media or other means, or more direct intervention.
    - For example, if a vaccination scam appears in an advertisement or is promoted in a profile on social media, an online marketplace, or fund-raising platform, we will ask that platform to remove it. We notify the ACSC immediately if we identify a standalone website that is hosting a vaccination scam.
- Sharing alleged scammer phone numbers from Scamwatch reports, including COVID-19 vaccination cold calls, with telecommunications providers for further investigation.[2]
- Sharing information on vaccination scam reports received by the ACCC at the regular Inter-Regulator Teleconference on COVID-19 Scams with the Fintel Alliance[3]. This meeting provides an opportunity to ensure key private sector and government entities are informed of the latest developments in vaccination scams.

COVID-19 and Scamwatch reports generally

The ACCC reports annually on the impact of scams in Australia.[4] Due to the well-known under-reporting of scams, the financial losses reported by Scamwatch are a fraction of the total losses suffered by Australians. While Scamwatch is the primary government website used by Australians to report scams, not all victims make a report to Scamwatch and instead make reports to other government agencies and banks. In 2020, Scamwatch received over 216 000 reports with $175.7 million in reported losses. Of these, 5622 reports mentioned COVID-19 with reported losses of $7.4 million. We have continued to see a substantial volume of COVID-19 themes in scams so far in 2021, but a very limited number relate to vaccinations.

- Between 1 January 2021 and 9 April 2021, Scamwatch received 793 reports mentioning COVID-19 with $2.4 million in reported losses.
- By comparison, only 58 of these 793 reports mentioned COVID-19 vaccines or vaccinations, with no reported financial losses. Of the 58 reports 6 reporters advised that they gave personal information to the scammer. A further 4 reporters advised that they gave personal information however these reports were all legitimate government or medical centre contacts.

The volume of reporting may vary with future announcements in relation to Australia's COVID-19 vaccination plans.

---

[2]Since 2020 telecommunications providers must comply with obligations under the new C661:2020 Reducing Scam Calls Code https://www.commsalliance.com.au/Documents/all/codes/c661

[3]Fintel Alliance is a range of organisations involved in the fight against money laundering, terrorism financing and other serious crime. Alliance partners include major banks, remittance service providers and gambling operators, as well as law enforcement and security agencies from Australia and overseas.

[4] https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity

Common examples of COVID-19 vaccination scams include:

- text, social media posts and emails with misinformation about the coronavirus
- investment scams claiming coronavirus has created new opportunities to make money or to invest in COVID-19 vaccinations
- survey and research scams offering a reward for participation in research or survey about the vaccine.

Vaccination phishing phone calls and text messages are used by scammers to trick people into giving out personal and financial information. Some typical examples include asking the victim to register for a COVID-19 vaccine, registering for an appointment to receive COVID-19 vaccine, or misinformation about receiving a rebate against COVID-19 vaccination costs.

Phishing is used by scammers to trick people into giving out personal information such as bank account numbers, passwords and credit card numbers.

Vaccination investment scams typically relate to opportunities to invest in a particular branded COVID-19 vaccination. Victims are contacted via email or cold-calls. The purpose of these is to obtain money and personal information.

Vaccination survey and research scams typically involve offering a reward for participation in research (by entering a trial group for the vaccine) or survey about the vaccine. These scams are after personal or financial information.

Example cases that illustrate Scamwatch reports on some common COVID-19 vaccination scams are in **Annexure 1**.

Consistent government messaging required

Of the 58 Scamwatch reports relating to COVID-19 vaccination received by 9 April 2021, 11 (18.9%) related to legitimate contacts from government agencies or private organisations such as medical centres. The true figure is likely to be higher, but several reports categorised as ‘Phishing’ contain insufficient detail to be certain.

One of the high risk issues in the COVID-19 crisis was the impersonation of legitimate government websites and communications. The roll out of government funding programs, additional support measures and vaccination information combined with increased levels of communication about COVID-19 from governments and business provides opportunities for scammers to impersonate these organisations – this results in a higher than usual level of phishing activity which in the COVID-19 crisis is more sophisticated and professional.

Consumers and businesses are unable to easily differentiate between legitimate government communications, trusted organisations and fake communications, making them more susceptible to scammers. Many communications utilise sophisticated technology such as ‘phone spoofing’ making it almost impossible to detect.

We have received many reports from people who thought that a legitimate government message was an approach from a scammer. The government’s need to put information out quickly and have citizens act on it has resulted in some actions – such as including links in text messages – that complicate the ACCC and other organisations’ attempts to simplify messaging about how to avoid scams. For example, in early 2020 during COVID-19 the government sent text messages to millions of Australians including a link to the website Aus.gov.au. Scamwatch and other agencies regularly warn consumers not to click on links in text messages and emails. This is an important message that protects people from phishing scams and malware. This inconsistency raises two issues:

- consumers will become desensitised to clicking on links and will be easier targets for scammers using this technique
- Australians will ignore legitimate messages from governments and businesses.

The ACCC recommends that government communications do not include links in text messages and continues to work on this with other agencies.

Significant steps to ameliorate this issue were taken in 2020. Government agencies worked together through the Criminal Justice and Law Enforcement Forum (CJLEF)[5] to develop more consistent approaches to government communications. In addition, Telstra (in conjunction with the Australian Cyber Security Centre and Services Australia) through the *Cleaner Pipes Initiative* developed a solution to restrict the sending of messages from 'myGov', 'Centrelink' and other specified SenderIDs to a limited number of approved sources. This resulted in a marked drop in reporting of these scams. However, more can be done to prevent impersonation of government and other organisations by SMS, including expanding such initiatives to a wider range of agencies.

We continue to receive reports of scam messages claiming to be from government organisations including myGov, coming from spoofed international numbers, spoofed local landlines, and spoofed Australian domestic mobile numbers rather than trying to claim 'myGov' as the sender. These scams continue to successfully trick people into believing the correspondence is legitimately from the government.

The ACCC, the Australian Communications and Media Authority, the Australian Cyber Security Centre and the telecommunications industry continue to work together through the Scams Telecommunications Action Taskforce to identify solutions to the use of telecommunications systems to perpetrate scams in Australia.

Government agencies communicating with the public should ensure information is available about the types of communications that consumers can expect from government or legitimate private sector organisations (such as medical centres) involved in the COVID-19 rollout. There is currently no central place a consumer can go to check if a communication they have received is legitimately from the government. Government websites, even when created by contract or in partnership with the private sector, should use the .gov.au domain wherever possible. Registering the .com, .com.au, .org, .org.au and other domain extensions is desirable to prevent misuse, but these should redirect to the .gov.au version of the page.

As an example of good practice, http://covid-19training.com.au/ appropriately redirects to https://covid-19training.gov.au/. This practice enhances the trust in legitimate government sites and decreases the ability of criminals to impersonate government sites. It also means as we can advise consumers to always look for and only trust government sites with the .gov.au domain.

Example cases that illustrate Scamwatch reports about legitimate communications are in **Annexure 2**.

Conclusion

Scamwatch data shows that COVID-19 vaccination scams are currently not a significant problem, with only 58 reports to Scamwatch as of 9 April 2021. This may change with the uptake and further rollout of COVID-19 vaccinations. Governments should ensure that their

[5]The CJLEF is chaired by the Secretary of the department of Home Affairs. Members include the ABF; AFP; ACIC; AUSTRAC; AGD; ATO; ACCC; APRA; CDPP; Treasury; Agriculture; ASD; Services Australia; ASIC. It considers the threat of serious and organised crime and provides strategic oversight and guidance for the development of whole of government strategies, policies and coordinated activities.

own messaging to the public is consistent and provides clear guidance on the types of communications that Australians can expect from legitimate private organisations involved in the COVID-19 vaccine rollout.

The ACCC will continue its efforts in engaging in disruption, awareness raising and intelligence sharing activities. We also continue to work with the ACMA and the telecommunications industry to prevent the use of our telecommunications networks and technology to perpetrate scams.

Annexure 1: Case examples illustrating common COVID-19 vaccination scams

The following case examples are reports to Scamwatch from the public which illustrate the most common COVID-19 vaccination scams. The reports are modified to protect the privacy of the reporters.[6] Each report also includes a wide range of intelligence about scam activity including but not limited to phone numbers; websites; social media platforms; email addresses and profiles that were used to communicate with the victim or perpetrate the scam.

Case Study 1 – Survey scam Scamwatch category: Phishing
Reporter stated that the scammer sent an email asking them "to complete survey in order to receive reward of up to $90. They claim to be vaccine research scientists gathering information on COVID-19 vaccines. Disgusting scam targeting people desperate for money during a pandemic." 
Case study 2 – Survey or research scams – Robocall Scamwatch category: Other scam
Reporter received a robocall (from 02 phone number) asking if they would take the covid-19 vaccine.
Case Study 3 – Vaccination investment scams Scamwatch category: Investment scam
Reporter said they received a call from an 02 number. The scammer was trying to force them to buy a product then "when I said I need time to think he cut the call". Reporter said the website (mentorplus.net) had fake logos on website and fake timeline given. The scammer said they were working for 11 years and a partner of Fizer. Asking for money to make profit on the Covid19

[6]Reports are reproduced largely as reported by the consumer, however small edits are made to improve readability, fix errors, remove personal information or reduce content.

Vaccines – “Sounds a bit fishy. But I am not sure” ACCC note: Website has been blocked by hosting service.
Case Study 4 – Phishing phone calls 1 Scamwatch category: Rebate scams
Received phone call from a private number referring to me by name with the advice that I was entitled to a rebate against Covid vaccination costs. Did not want to prolong the call so stated that the vaccinations were free and my GP would handle my vaccination
Case study 5 – Phishing phone calls 2 Scamwatch category: Health & Medical Products
Reporter received a phone call. “They were wanting my info for Covid vaccine. Saying I was eligible and could get it sooner. They didn't identify themselves and poor quality sound”.
Case study 6 – Impersonation of overseas government organisation Scamwatch category: Other scams
Reporter from Australia received a COVID-19 Vaccination Invitation via Email stating it was from NHS Test and Trace. “This is a public health message from NHS. As part of the Govt's coordinated response to C/V NHS is performing selections for C/V vaccs on the basis of family genetics and medical history. You have been selected to receive a C/V vacc. Use this service to confirm or reject your C/V vac” (2 links follow one for accept one for reject). Further into this email it states "you can only use this service if you have received an email/SMS regarding this invitation. You cannot use this service for anyone other than yourself”. It was not addressed to either one of us in particular. Although we share the same email we do have separate UK Customer Reference Numbers. Neither were we addressed by name by the sender. Also we know from a relative in the UK that vaccinations are offered on an age-bracket basis only. Whereas my husband's age group has been reached mine has not nor is likely to be for some time. I have NOT replied on either of our behalf nor clicked on either link. I am wary of the fact that the sender appears to have multiple address links ending in a final email address in Japan. However it's not unusual to received mail from The Netherlands or Ireland that is from some UK Govt department or other. *I have included the full address it was sent from in the attached doc.

Annexure 2: Scamwatch reports about legitimate communications

The following case examples are reports to Scamwatch from the indicating confusion about COVID-19 vaccine communications. The reports are modified to protect the privacy of the reporters and legitimate private organisations.[7]

Case study 1 – Medical Centre 1
Email purporting to be from [redacted] which is the medical booking system used by [redacted] Medical Centre calling for patients to register details to get on the list for vaccine. Link in email redirects to the [redacted] domain. On completing the survey it appears to redirect to a SurveyMonkey page. I'm not 100% sure it's fake - if it is fooled me because the email included my first name. ACCC note: *The Medical Centre publishes that it uses [redacted medical booking system] on its homepage. The domain redirected to is standard across several electronic newsletter services. Given the absence of other suspicious indicators the correspondence received appeared legitimate.*
Case study 2 – Medical Centre 2
Text says: "Dear [reporter's first name] We are approved for COVID-19 vaccine delivery to eligible patients. If you have any questions please book an appointment to discuss." There is no information on who the message is from apart from the phone number. ACCC note: *The sending phone number is associated with a medical facility proximate to the reporter's location. The facility in question is involved in the rollout. Given the absence of other suspicious indicators the correspondence was almost certainly legitimate.*
Case study 3 – State government message
I received an email for a COVID-19 vaccination invitation. I suspect that this website is a scam but I'm not sure. They have my full name, my phone number, my email address and I filled the form in with my DOB and home address. the website is as below: https://portal.cvms.vic.gov.au/ ACCC note: *The website ends in .gov.au and there is no indication of a misleading hyperlink that goes to another address. The correspondence received was almost certainly legitimate.*
Case study 4 – Medical Centre 3
The message asked me to phone the above number about my Covid vaccination. You missed a call from [redacted] who said "Hello this is [redacted] Medical Centre.

[7]Reports are reproduced largely as reported by the consumer, however small edits are made to improve readability, fix errors, remove personal information, remove names of private companies, or reduce content.

We just calling in regards to your covert(?) vaccine. If you could call us back that would be much pre-." This message was provided by Telstra at no charge to you. ACCC note: *The phone number belongs to the Medical Centre it stated. Correspondence is legitimate.*
Case study 5 – Medical Centre 4
The text I got was Hello [redacted name of Medical Centre] COVID-19 Vaccination clinic urgently requires your: First name Surname Medicare # Medicare ref # Please respond to this text message at your earliest convenience Kind regards ACCC note: *The phone number belongs to the Medical Centre it stated. Correspondence appears legitimate.*
Case study 6 – Australian Government website
The text stated "Appointment booked for 2021-06-22 at 2.45pm. All patients must completed a registration form complete yours here: https://app.respiratoryclinic.com.au/vaccination-register/[redacted]" The Australian government has an identical website except it is .gov.au rather than .com.au i.e: https://app.respiratoryclinic.gov.au/vaccination-register/[redacted]"So this website looks exactly the same. If it is a scam I am very concerned that people will input their information because it looks so convincing. I suspected it was a scam as I am not due to have the vaccine in June and also I live in [redacted] but this website said it was for a [redacted] clinic." ACCC note: *Hyperlinks in text messages cannot be misleadingly anchored to another site. Respiratoryclinic.com.au is registered to a known subcontractor of the Department of Health and identical to Respiratoryclinic.gov.au. The website and text message are both legitimate though it appears the wrong recipient has received the message for unknown reasons.*