Australian Government
Attorney-General's Department

06 May 2021

Attorney General's Department

Submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into vaccine fraud and security risks

The Attorney-General's Department (AGD) thanks the Parliamentary Joint Committee on Law Enforcement for the opportunity to make a submission to the inquiry into vaccine fraud and security risks.

AGD's submission focuses on fraud risks with the COVID-19 vaccination roll out, in particular it discusses:

- the risk of fraud as it relates to the vaccination roll out
- types of fraud threats identified
- advice on effective ways to counter vaccine fraud threats.

The risk of fraud as it relates to the vaccination roll out

In crisis and emergency response situations, it is important that governments can respond as quickly as possible. Fraud can undermine these efforts if it is not controlled. The complex and time-critical nature of response measures such as the vaccination program gives rise to an inherently higher risk of fraud. Furthermore, as the vaccination program is relevant to all Australians, it exposes members of the public to a higher risk of scams and identity theft.

Australia has not seen significant scam and fraud activity related to the COVID-19 vaccination roll-out. This is a positive trend we would like to see continued to maintain confidence in the vaccination program. In other jurisdictions, including the United States and America (US) and the United Kingdom (UK), there have been notable incidents of fraud during their vaccination roll outs that Australia can learn from.

It is not a failure for some fraud to occur in these circumstances – a certain level of fraud is inevitable and unpreventable due to the time-critical nature of delivery. However, if fraud happens in an uncontrolled manner, it could have significant impacts, such as increasing the cost of the roll out or undermining confidence in the vaccines and Australia's vaccination program.

The Commonwealth Fraud Prevention Centre (the Centre) in AGD, together with the Corporate Assurance Branch in the Department of Health, has engaged with senior officials in that department leading the design and implementation of Australia's COVID-19 vaccination roll out to provide information about fraud threats identified internationally and discuss strategies to assess and mitigate those threats in Australia.

Types of fraud threats identified

AGD, through the Centre, has an excellent working relationship with international counterparts from the UK, US, New Zealand and Canada through the International Public Sector Fraud Forum. Though this forum, partner countries have shared information on fraud threats and incidents during the COVID-19 pandemic response, as well as leading counter fraud approaches.

From the beginning of the COVID-19 pandemic, there have been continued reports about COVID-19 related fraud and scams. As jurisdictions across the world progress with their vaccination roll outs, we have now seen common types of vaccine related fraud. Most frauds have been opportunistic in nature, however there have also been some instances involving serious and organised crime.

The following threats are primarily drawn from the experiences of other nations.

Public scams

In the UK, members of the public and organisations are receiving scam phone calls, text messages and emails about the vaccine, often using fake government branding.[i] These phishing attacks can be sophisticated and based on previous government messages. Fake websites are also being established for the same purposes.[ii] This includes investment scams, which can result in significant financial losses for individuals.[iii]

Phishing messages often contain links asking people to pay money for the vaccine or provide their details in order to access the vaccine. The main purposes of these messages are to solicit money and steal personal and financial details through social engineering or malware. These details may then be used to commit further fraud, including fraud against the individual or third parties, including government programs. The proliferation of personal identifying information online, such as the recent compromise of 500 million Facebook users' data, exposes even more people to these types of phishing messages. Fraudsters are also targeting government and private sector organisations in order to obtain their clients' information to target with scam messages.[iv]

Changes to Australia's vaccination program – such as the changes prompted by the increased risk of rare blood clots following the AstraZeneca vaccine in those under 50 years – can provide additional opportunities for fraudsters to take advantage of public uncertainty and successfully scam individuals and organisations.

If not proactively disrupted, vaccine related scams could undermine the speed and efficacy of Australia's vaccination program. A high prevalence of scams could also reduce the public's confidence in genuine communications from governments and health practitioners, potentially leading them to disregard advice about vaccine availability and appointments.

Counterfeit vaccines

In the UK, fraudsters are creating and offering counterfeit vaccines.[v] Fake vaccines are being sold over the internet, including the dark web.[vi] There have been reports overseas of people going door-to-door seeking to sell counterfeit vaccines. They have then injected vulnerable people with unknown substances. In addition to putting the public at risk, this undermines public trust in the vaccines.[vii]

The risk of counterfeit vaccines, such as fake Pfizer[viii] vaccines, is potentially exacerbated by concerns about the AstraZeneca vaccine.

Supply chain fraud

Vaccines require specific storage, transportation and equipment to administer effectively. There may be a number of processes through the vaccine supply chain that are vulnerable to fraud where individuals may steal or tamper with vaccines. Changes during the rollout could be vulnerable to fraud as fraudsters take advantage of urgent timeframes.

Selling/using damaged vaccines

Suppliers may seek to sell or administer vaccines that have not been stored properly. There is also a risk of vaccines being deliberately tampered with before being administered.[ix] These vaccines would no longer be effective, and therefore, would put the public at risk and undermine public confidence in the vaccine.

Procurement for vaccine related materials

Many governments across the world have had to engage new suppliers, some with limited backgrounds, in order to obtain and roll out COVID-19 related medical equipment. Several governments have had fraudulent companies attempt to sell non-existent or faulty medical equipment.[x] There is also a risk of cartel conduct and suppliers price gouging actual equipment.[xi]

Effective ways to counter vaccine fraud threats

AGD, through the Centre, has provided strategic support and advice to a number of Commonwealth entities during the COVID-19 pandemic response, including advice on fraud risks and counter fraud strategies, providing tools and guidance, and running counter fraud forums and workshops.

The Centre is working closely with the Australian Federal Police and the Department of Health to identify, assess and monitor fraud threats related to the vaccination roll out. This includes supporting the Corporate Assurance Branch in the Department of Health to assess and mitigate specific threats to the vaccination program. The Department of Health is undertaking measures to deal with vaccine fraud risks, including working closely with the Australian Cyber Security Centre on potential cyber issues, including with its delivery partners, and working to mitigate the risks of incorrect information in the public domain through its 'Is it true' website.[xii] The Therapeutic Goods Administration has also been working on measures to mitigate the risk of counterfeit vaccines.

There are risks inherent in any large scale activity – particularly one as complex as delivering a national vaccination program as quickly as possible. The best way to prevent risks from being realised is to identify them early and determine appropriate treatments, where possible.

The following advice aligns with international leading practice for fraud control in emergency management and recovery situations.[xiii]

Understanding and acknowledging risks

A key first step to countering fraud is undertaking fraud risk assessments. A detailed, fraud-focused assessment provides relevant public officials with a better understanding of fraud risks and highlights any limitations in existing countermeasures. A fraud risk assessment also helps officials make decisions about how to mitigate fraud risks and where to focus post-event assurance activities.

AGD, through the Centre, has published leading practice guidance on fraud risk assessments on its website, CounterFraud.gov.au.[xiv] These assessments have evolved significantly over recent years, and can lay the groundwork for additional improvements, such as improved data collection, collaboration, information sharing, data analytics and countermeasures that can be scaled across different measures and programs.

Fraud risk assessments should be complemented by ongoing monitoring of risks to ensure officials stay alert to the changing nature of the fraud threat, and manage the evolving risk accordingly. For example, as international borders reopen, new threats will emerge such as the sale and use of counterfeit vaccine certificates,[xv] which could risk public safety and undermine efforts to restore Australia's tourism sector.

Implement appropriate countermeasures

In any emergency response environment, it is important that fraud countermeasures are low friction, so they do not delay program delivery. Implementing prevention countermeasures can appear harder than measures that respond to fraud, such as investigations. However, even low-friction prevention countermeasures, such as clear public messaging and data sharing and analytics, can have wider benefits for protecting public health and program integrity.

Use existing mechanisms and providers

Using existing processes and delivery models is an effective way of maintaining program integrity when delivering programs in compressed timeframes. This approach allows government entities to model new policies, criteria and systems based on what is already established and tested, and thereby reduce the risk of creating unexpected fraud vulnerabilities.

Working with established suppliers and service providers, where possible, can often be a lower risk option than using new, unestablished and untested providers. However, this may not always be possible, particularly with new programs or emergency responses. Therefore, entities should apply appropriate due diligence checks for new suppliers and service providers.

It should be noted that it is individuals that commit fraud - not organisations. Therefore, it is not possible to completely eliminate the risk of fraud using established and 'trusted' suppliers and service providers.

Tailor public communications

The Centre strongly supports the simple, positive message the Department of Health is using to inform the public about the COVID-19 vaccine ('Safe. Effective. Free') and its 'Is it true' website. Clear and trusted public communication can prevent people and businesses falling victim to scams, in addition to providing confidence in the vaccination program.

Clear public messaging about what to expect from government can make it much harder for scammers to craft a believable alternative narrative e.g. you need to pay for the vaccine.

The Centre has also worked with partners in the Australian Cyber Security Centre, the Australian Competition and Consumer Commission and the Australian Federal Police to provide guidance for Australian Government entities about the importance of a consistent approach to SMS communication (Attachment A).[xvi] The guidance explains that URLs (or links) should only be used as a last resort and if they are to be used, they should link to a central 'aus.gov.au' or '.gov.au' site to minimise confusion. Entities should also include scam awareness on their websites.

Detection and response

Some up-front, prevention countermeasures may be difficult to implement in a rapid vaccine roll out. Consideration should be given to what detection countermeasures can be introduced to bring to the surface any fraud that does occur.

Where it is not feasible to implement countermeasures to mitigate known vulnerabilities, actively recording the risks and preparing response plans will enable government entities to swiftly respond

should the risks eventuate. For example, the Centre has suggested the Department of Health develop an incident response plan to prepare for a potential increase in scam activity related to the COVID-19 vaccine. This would proactively provide department officials tools to:

- avoid ad hoc decision-making in response to incidents
- communicate clearly and responsively with the public
- engage effectively with Minister and stakeholders (including the media)
- provide timely notifications to the Australian Cyber Security Centre and other relevant entities.

While this might not reduce the likelihood of scam activity, a well-planned and well-executed response plan can also reduce the consequences of the threat.[xvii]

Undertake post event assurance

It is also important that post-event assurance activity is undertaken in as timely a fashion as possible, to establish whether fraud risks were realised. A detailed fraud risk assessment can assist in targeting post-event assurance work (such as forensic audits) to check for instances of fraud.

It is important that resources are agreed to early and then set aside to deliver this. Post-event assurance can be done on a variety of scales and officials should determine the appropriate level of post-event assurance based on the entity's risk appetite. For example, this could involve targeted audit activity or data matching exercises, such as matching GP or vaccine distribution records.

Conclusion

The Centre's work recognises that preventing fraud is preferable to investigating it after it occurs. Preventing fraud can help strengthen program integrity and reduce the impact of fraud on government programs, Australian businesses and members of public.

Fraudsters adapt to new opportunities and the fraud threat constantly evolves. Australian Government entities demonstrated extraordinary commitment and agility to ensure services and support quickly reached those in need during the COVID-19 pandemic. While the integrity of government programs and systems have been tested during the pandemic, with criminals successfully targeting some government stimulus measures, detected instances of fraud have generally been lower than overseas.

The Centre is leading efforts to strengthen counter fraud arrangements across the Australian Government. This includes providing guidance to support Australia's economic recovery from the impacts of the COVID-19 pandemic (Attachment B)[xviii] as well as future disaster relief and recovery efforts (Attachment C).[xix]

About the Commonwealth Fraud Prevention Centre

The Commonwealth Fraud Prevention Centre was established within AGD to work with Australian Government entities to build counter fraud capability and put a focus on preventing fraud against Commonwealth policies and programs. Since 1 July 2019, the Centre has developed a series of products and guidance materials, including on fraud risk assessment, data sharing and pressure testing countermeasures. The Centre also worked with the AFP's Operation Ashiba to provide fraud prevention support to Australian Government entities during the Black Summer Bushfires and the COVID-19 pandemic.

References

[i] bbc.com/news/uk-england-hampshire-55840397

[ii] justice.gov/usao-md/pr/three-baltimore-area-men-facing-federal-charges-fraud-scheme-purporting-sell-covid-19

[iii] scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams

[iv] au.sports.yahoo.com/celsius-suffers-third-party-data-163132336.html

[v] bbc.com/news/world-africa-56270243

[vi] bbc.com/news/technology-56489574

[vii] bbc.com/news/uk-england-london-55680856

[viii] bbc.com/news/world-56844149

[ix] abc.net.au/news/2021-01-01/wisconsin-hospital-worker-arrested-for-spoiled-vaccine-doses/13025870

[x] abc.net.au/news/2020-04-01/coronavirus-chinese-ppe-border-force-intercepted/12085908

[xi] justice.gov/usao-nj/pr/us-attorney-s-office-prosecutes-covid-19-fraud-and-price-gouging-personal-protective

[xii] health.gov.au/initiatives-and-programs/covid-19-vaccines/is-it-true

[xiii] *'Fraud in Emergency Management and Recovery'.* International Public Sector Fraud Forum, February 2020, assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864310/Fraud_in_Emergency_Management_and_Recovery_10Feb.pdf

[xiv] counterfraud.gov.au/access-tools-and-guidance/conduct-fraud-risk-assessment

[xv] nytimes.com/2021/04/08/technology/vaccine-card-scam.html

[xvi] counterfraud.gov.au/access-tools-and-guidance/how-use-urls-safely-public-sms-communications

[xvii] '*Review of the Events Surrounding the 2016 eCensus'*, Office of the Cyber Security Special Advisor, 13 October 2016, apo.org.au/sites/default/files/resource-files/2016-11/apo-nid70705.pdf

[xviii] counterfraud.gov.au/access-tools-and-guidance/design-economic-recovery-measures-are-more-resistant-fraud

[xix] counterfraud.gov.au/access-tools-and-guidance/better-protect-relief-and-recovery-support-measures