Committee Secretary

Parliamentary Joint Committee on Law Enforcement

PO Box 6100

Parliament House, Canberra, 2600

30 April 2021

RE: Call for submissions to the Vaccine related fraud and security risks inquiry

My name is Dr Cassandra Cross and I am an Associate Professor in the School of Justice, Faculty of Creative Industries, Education and Social Justice, at Queensland University of Technology. My area of expertise targets (online) fraud, but also encompasses related areas such as identity crime, data breaches, cybercrime, and cybersecurity more broadly. I first started researching fraud in 2008, while working as a civilian with the Queensland Police Service. In 2011, I was awarded a Churchill Fellowship to explore the prevention and support of online fraud victims. This enabled me to travel across the UK, US, and Canada to engage with over 30 agencies working in this space. It was an invaluable experience which was the catalyst to my academic transition.

My appointment to QUT in September 2012 has enabled me to pursue a research agenda focused solely on fraud. I have developed an extensive and authoritative track record in this area, across both national and international fronts. I have published over 65 outputs predominantly relating to fraud and cybercrime. I have been successful in bidding for, and attracting research funding, having led eight research projects, all in collaboration with government or industry partners, totalling over $1.3 million.

My fraud research has focused on all aspects of fraud victimisation, across policing, prevention, and the support of victims. I have focused largely on gaining direct narratives from those who have experienced fraud, as well as professionals who are tasked with responding to fraud across a wide range of stakeholder contexts (police, consumer protection, government, industry, and community organisations). Fraud is a global issue, and my work has highlighted the complexities, nuances and ongoing challenges posed by fraud to individuals, governments, corporates, and society as a whole.

The potential for fraud victimisation has become even more apparent in the context of the COVID-19 global pandemic declared in March 2020. The associated lockdowns, restrictions and physical distancing measures implemented globally to combat the virus, have significantly altered the lives of citizens worldwide. The large-scale forced shift to online technologies and communication platforms of individuals and organisations alike, has created a new range of possibilities and approaches for fraud offenders. Sadly, these have been embraced and exploited by offenders mercilessly in the past twelve months, affecting millions of citizens in Australia and beyond. COVID-19 provides fertile ground for offenders to employ both non-specific and targeted fraudulent approaches.

I thank the Joint Parliamentary Committee on Law Enforcement for their interest in this topic and the ability to contribute to this inquiry.

Dr Cassandra Cross
School of Justice, Faculty of Creative Industries, Education and Social Justice, Queensland University of Technology

This submission puts forward observations and findings from my collective research into fraud (and related cybercrime) victimisation. It draws on my knowledge and communications with scholars, law enforcement and industry bodies spanning Australia and overseas. Further, it draws specifically on the arguments I have made in the following articles:

- **Cross, C**. (2020) Theorising the impact of COVID-19 on the fraud victimisation of older persons. *Journal of Adult Protection*. Online first DOI: 10.1108/JAP-08-2020-0035.
- **Cross, C.** (2020) Fake COVID-19 testing kits and lockdown puppy scams: how to protect yourself from fraud in a pandemic. *The Conversation* August (19).

The submission will collectively focus on these specific terms of reference:

> 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;
>
> c) Risks to Australia regarding fraud and integrity of COVID vaccines in South Pacific nations and support for these nations to address issues relating to fraud and integrity risks;
>
> f) Any related matters.

However, prior to discussing the issue of fraud as it relates to COVID-19 vaccines as listed above, it is important to look at the broader context of fraud and how it has manifested itself during the pandemic to date.

An overview of fraud

Fraud is premised around the use of deception to gain a financial advantage. In most cases, this focuses on the ability of an offender to gain direct money transfers, but it can also target personal information and identity credentials as a means to establish new credit cards, loans and other means of finances. Offenders are unscrupulous and will use any means possible to gain a monetary reward.

Fraud costs victims billions of dollars globally each year. For example, in 2019, the Internet Crime Complaint Centre (IC3) in the USA, reported losses from fraud victims of over USD$3.5 billion. Similarly, in Australia, the Australian Competition and Consumer Commission (ACCC) reported Australian losses of over AUD$634 million in 2019. This figure has continued to increase annually and will undoubtedly rise again with official 2020 statistics. Given that fraud has one of the lowest levels of known reporting across all crime types, any of these figures are likely to under-represent actual losses. Further, these figures do not encompass the non-financial harms resulting from fraud victimisation, which can include a deterioration of physical and emotional health; varying levels of depression; relationship breakdown; unemployment; homelessness; and in severe cases, suicide. In this way, any figures will be arbitrary measures that underestimate the true cost and extent of fraud across society.

Fraud is not new but has existed for centuries. However, the evolution of technology, and particularly the development of the internet, has shaped the ways in which offenders can target potential victims. Online communication platforms have enabled offenders to communicate with and engage an exponentially larger victim pool with greater ease and reduced cost, compared to older methods of communication. In this way, a large proportion of fraud now has an online element to it. However, it is important to recognise that offenders will still use the telephone, fax, and face-

to-face methods. My own research demonstrates the ways in which offenders will move seamlessly across all communications platforms (including email, telephone, text message, social media and face-to-face) to perpetrate their offences.

Fraud and COVID-19

There are an endless number of approaches that offenders will use to target their fraudulent approaches to their victims. Offenders are highly skilled, tech savvy individuals with a strong creative element to many of their pitches. They will combine blanket approaches to large groups of people, as well as targeting detailed schemes to specific groups or individuals. Offenders will often use real world events as the context for their fraudulent schemes and invitations. There is a well-established link between natural disasters and fraud, with offenders using these events in a variety of ways to gain their monetary benefits. In this way, the use of COVID-19 as a justification for many fraudulent approaches in the past twelve months is consistent with previous research.

The success of offenders using COVID-19 as the context for fraudulent solicitations and invitations can be attributed to several factors. Fraud in general targets a person's weakness or vulnerability. Research indicates that there are very few factors which can predict fraud victimisation as a whole. There are limited factors which are evident with certain types of fraud (for example, older persons are more likely to be victims of telemarketing fraud). Instead, all individuals are argued to have a potential vulnerability, which if identified and targeted in the right way at the right time, can make that person susceptible to fraud. It is also argued that vulnerability to fraud is not fixed, but instead should be viewed along a continuum, which can change on a daily, monthly, or yearly basis. Essentially, vulnerability to fraud is contingent upon a variety of individual circumstances, as well as some demographic and contextual factors.

COVID-19 has been a significant disruptor across all society. It has dramatically changed the ways in which we live, communicate, conduct business, and engage in social and leisure activities. The use of lockdowns, physical restrictions on movement and gatherings, and social distancing across the globe have radically altered daily routines. For some, this may have had a limited impact. However, for others it may have had considerable consequences, with many of these having a profoundly negative impact on one's overall health and wellbeing.

It is understandable that anxiety levels across society have been heightened since the beginning of the pandemic. This has been attributed to the direct health risks associated with the virus but has arguably extended to other aspects of one's life, including relationships with family and friends; employment; housing; education and overall financial wellbeing. Offenders have attempted to take advantage of this anxiety, as well as the corresponding factors related to COVID-19 and all government measures put in place since March 2020.

For example, COVID-19 has seen increases in online shopping fraud. In these circumstances, offenders have created fake websites and social media pages to advertise for products that do not exist. In the early stages of the pandemic, there was a short supply of personal protective equipment, and offenders took advantage of the desire to purchase these types of goods. A similar situation has been witnessed with puppies, with many Australians paying for an animal online which never arrives.

Further, phishing emails remain a popular way for offenders to harvest sensitive information and personal credentials from unsuspecting victims. Phishing emails (or text messages) purport to be from an authority and usually require recipients to click on a link or provide specific information. In the context of COVID-19, these were under the guise of health departments, government agencies

(such as the Australian Tax Office) and well-known retail stores (including supermarkets such as Coles and Woolworths). These were particularly effective in a COVID-19 context, as people were searching for information and each approach usually had an air of plausibility behind it. To demonstrate this, the ACCC (on their Scamwatch site) report that almost 6,500 reports have been lodged with them that are attributed to COVID-19 related approaches. Further, over AUD$9.8 million has been lost by individuals to these schemes since the beginning of the pandemic.

Fraud and COVID-19 vaccines

The previous section has summarised the ways in which offenders have used COVID-19 during the past twelve months to perpetrate fraud. The above has not only been evident in Australia, but these approaches and techniques used by offenders have been mirrored globally.

The development and subsequent release of an approved vaccine was an historic moment in the response to COVID-19. Unsurprisingly, this also provided additional opportunities for offenders to embrace the pandemic and virus as a means to extend their fraudulent pitches. Approaches which have been tailored specifically around the vaccine include:

- Requests to pay for vaccinations (the vaccine is being provide free of charge by governments, including Australia);
- Offers to pay a fee to access a vaccination earlier than anticipated; and
- Fraudulent websites created asking individuals to register for a vaccine and harvesting their personal details.

Similar to the those described in the previous section, these approaches seek to target and exploit the same anxieties in existence around the health and wellbeing of individuals in relation to the virus. They also seek to exploit the perceived delay by the community in the Australian vaccination rollout, and a confusion in government messaging over who is eligible for a vaccine at any particular time. Again, these are not restricted to an Australian context, with similar situations observed in countries such as the United Kingdom. Each of these approaches has a potential legitimacy to them, particularly for those in the community who do not have access to, or knowledge of, legitimate sources of information.

Further to those already described, there are still other approaches likely to emerge in a future Australian context. These relate to vaccination certificates and the potential for “vaccine passports” of some form. As more of the population receives their vaccinations, and international borders open for less restricted travel, it is likely that offenders will continue to evolve their approaches accordingly. If vaccination is mandatory in a particular situation (such as travel), this will provide opportunities for offenders to create fake certificates or verification methods. Again, this will be a global issue, and impact countries including Australia.

Summary of fraud as it relates to COVID-19

COVID-19 has provided fertile ground for offenders to target unsuspecting victims globally. Australia has not escaped this, with many citizens having already lost money to offenders through responding to a fraudulent approach, or through having had their personal credentials compromised in some way. Further, the global pandemic has arguably altered on a large scale the level of potential vulnerability for members of the community. The virus itself, as well as associated responses to COVID-19, have radically changed daily lives and routines, and in many cases, increased levels of anxiety and uncertainty on a macro level. Consequently, individuals may be more susceptible to COVID-19 themed fraudulent approaches, compared to other schemes used by offenders. However,

offenders are also harnessing the effectiveness of traditional methods of fraud, such as phishing and are continuing with non-COVID-19 related fraud approaches as well.

Fraud continues to be a problem in Australia, and victims continue to lose millions of dollars annually. COVID-19 is simply the latest event to be used by offenders as a means to increase their success rate. Even without the impacts of COVID-19 on fraud, thousands of Australians are impacted by fraud and struggle to recover from both the financial and non-financial harms that result. In this way, the threat to Australians posed by COVID-19 related fraudulent schemes needs to be considered in the broader context of fraud. Existing resources dedicated to the policing, prevention, and support of those who experience fraud, are not commensurate with the losses incurred by victims and the impacts to their wellbeing and livelihoods. Victims consistently report low levels of satisfaction with responses to fraud victimisation, and instead experience additional levels of trauma as a result of their interactions with the system. Without any changes or intervention, this will undoubtedly continue, and COVID-19 (or the next natural disaster or large event) will persist in providing a means for offenders to deceive, manipulate and exploit those within Australia and overseas for their own financial gain. There is a critical need to explore fraud at its foundations, rather than react to a particular themed approach (such as COVID-19). These same issues and vulnerabilities will occur in the future unless they are targeted and responded to, at a core level.

Recommendations

The following recommendations are put forward for consideration of improving responses to fraud overall, which includes the COVID-19 themed approaches canvassed in this submission:

Recommendation 1

Review of the current prevention messaging that exists targeting fraud prevention. This needs to include a review of specific messaging targeting COVID-19 themed approaches but should also extend to how to best educate and increase effective awareness of fraud prevention across all potential solicitations.

Recommendation 2

Review the current support services available for individuals who have experienced fraud, either through a direct loss of money, or through having identity credentials compromised and/or misused. There are limited support services currently available, and those which operate are overwhelmed by individuals in need. The recovery of victims is currently inhibited by the lack of acknowledgement around what has occurred, the extent of the impact, and adequate support mechanisms available to assist with moving beyond the incident.

Recommendation 3

Invest resources in research which seeks to better understand the ways in which vulnerability operates to increase/reduce levels of fraud victimisation. This would also require an explicit focus on COVID-19, examining both short- and long-term effects on individuals and their susceptibility to fraudulent approaches. These findings should then be used to strengthen resiliency of the Australian community to fraud, both COVID-19 related schemes as well as those already in existence.

Note

A copy of all my publications can be found at the following link:

https://eprints.qut.edu.au/view/person/Cross,_Cassandra.html

I am able to provide full text copies of anything upon request.