Research Director
Communities, Disability Services and Domestic and Family Violence Prevention Committee
Parliament House
George Street
Brisbane Qld 4000

28 May 2015

RE: Inquiry into the adequacy of existing financial protections for Queensland's seniors

My name is Dr Cassandra Cross and I am currently a Lecturer with the School of Justice, Queensland University of Technology. I commenced this job in 2012. Prior to this appointment, I held research and policy positions within the Queensland Police Service for five and a half years. It was in this capacity that I started researching the topic of online fraud victimisation. Since 2008, I have undertaken several research projects and spoken with approximately 150 victims of fraud, with a strong focus being on the victimisation of older persons. A summary of my expertise in this area is below.

In 2008, while I was employed by the Queensland Police Service, I conducted a research project entitled *Seniors and Online Fraud*. As part of this project, I interviewed 85 seniors (aged 50 years or over) throughout Queensland who had received a fraudulent email request for money, personal details or passwords. Many participants in this project were victims of fraud, with some having lost several hundreds of thousands of dollars. This research provided valuable insights into an area which was previously unknown and has formed the basis for my ongoing research.

In 2011, I was awarded the Donald Mackay Churchill Fellowship to examine the prevention and support of online fraud victims. This enabled me spend eight weeks abroad and travel to the United Kingdom, the United States of America and Canada to meet with different agencies on their jurisdictional responses to the problems posed by online fraud. I was able to visit over 30 different agencies, including law enforcement, government, non-government and community organisations all working in the fraud space. This was an invaluable experience in terms of learning how other countries and agencies respond to online fraud and what Australia can learn from their example. I have maintained several relationships with key agencies since my return to Australia.

In 2012, under the auspices of the Carindale PCYC, we launched the *Seniors Online Security* Project. This was the result of an $86,000 federal government grant under the *Proceeds of Crime Act* funding scheme. This project specifically delivered a comprehensive training package for seniors targeting a number of identified needs. The package consists of five distinct modules which I wrote, each with a workbook and accompanying PowerPoint presentation. The five modules encompass general computer security, identity crime, social networking, fraudulent emails and online banking. The premise of the package was to develop resources which seniors could use themselves to teach other seniors about these important issues. They have also been used by many police to deliver presentations to seniors groups. This package was developed in consultation with a range of stakeholders from the seniors community and was piloted be several Neighbourhood Watch groups.

In 2014, this package was launched in Western Australia, under the badge of the West Australian Police and Department of Commerce. This package is currently being revised in Queensland to incorporate recent changes, such as the creation of ACORN, the Australian Cybercrime Online Reporting Network, and the ability of victims to report through this mechanism.

In 2013, myself and two colleagues (Dr Kelly Richards and Dr Russell Smith) were awarded a Criminology Research Grant entitled *Improving the response to online fraud: An examination of reporting and support*. This is the first Australian study to specifically examine the reporting experiences and support needs of online fraud victims. This has enabled Dr Richards and I to conduct 73 interviews across Australia with individuals who have reported fraud losses in excess of $10,000 to the Australian and Competition and Consumer Commission's SCAMWatch website. While not specifically focused on seniors, we have interviewed several older persons who have suffered substantial impacts as a result of online fraud. This project is due for completion in mid-2015.

Lastly, in 2014, I was able to visit the Canadian Anti-Fraud Centre and interview twenty-one volunteers (all seniors themselves) who provide telephone support to older victims of fraud across Canada. The program (known as SeniorBusters) is a unique service which seeks to provide support and advice to older persons who have been victims of fraud or who are considered vulnerable. My interviews with these volunteers provided an important insight into the impacts experienced by older victims of fraud and the many difficulties encountered in seeking to provide assistance to this particular group. The results of this research have been presented to the Canadian Anti-Fraud Centre and are currently being drafted for wider publication.

Overall, based on these projects and my ongoing research in this area, I feel I have considerable knowledge and expertise to offer on the topic of online fraud, how it relates to seniors and particularly how it impacts on their financial security. The following submission is based upon my knowledge and experience across the past eight years and seeks to offer an informative contribution to the current inquiry. The financial protection of seniors is a critical issue which impacts on their overall wellbeing, across physical, emotional and financial realms. Fraud is one of the many ways that this can be compromised and their long term financial security threatened. I acknowledge the committee for taking the time to consider such an important issue and look forward to seeing the topic remain a priority for government into the future.

The following submission addresses each of the terms of reference outlined by the inquiry. Should you wish to discuss further any of the content presented in this submission or require any references to support my statements, please contact me directly on the details below.

Regards,

Dr Cassandra Cross

Lecturer, School of Justice, Faculty of Law
Queensland University of Technology
[redacted]
[redacted]
Twitter: @DrCassCross
Publications: http://eprints.qut.edu.au/view/person/Cross,_Cassandra.html

1) The current levels of financial literacy of seniors and how that can be improved, for example by education programs

Financial literacy is important for all individuals. In a paper I wrote with a colleague (Drew and Cross 2013), we examined the issue of financial literacy as it applies to investment fraud. Within the paper we outlined the research which suggests that financial literacy is not always a protective factor against fraud victimisation. Rather, there have been various studies which have found that instead, levels of financial literacy are associated with higher victimisation. While this seems counterintuitive, several explanations have been put forward to account for this, which include the over confidence of a financially literate person to determine if an investment pitch is fraudulent or legitimate. Those without knowledge are more likely to dismiss fraudulent approaches, but those with experience and knowledge may rely heavily on this and not realise they have become involved in fraud. In this regard, increasing the financial literacy of individuals, especially seniors, is important but is not the only means by which to improve financial outcomes for seniors.

Further in this article, we highlighted the techniques of social engineering and persuasion that are used by highly skilled and tech savvy offenders. No amount of financial literacy can guard against a smooth talking offender who knows all the psychological tools in which to manipulate and exploit potential victims. Therefore, we argued that any education package targeting financial literacy must also include information on social engineering and the methods by which offenders will aim to gain compliance from unsuspecting victims.

I have seen firsthand the application of this in real life. Numerous victims I have spoken with have expressed previous knowledge of fraud generally, and in many cases of the specific fraud that they become involved in. However, despite this knowledge, there was an inability on their part to apply any warning signs and known characteristics of fraud to their situation. Instead, many were deceived through complex and sophisticated operations, which did not raise any of the red flags they were looking out for.

This point speaks to the current content of prevention messages across fraud. In a previous submission to a federal government inquiry into the cybersafety of seniors, I argued that current fraud prevention messages are too complex and characterised by what I term “white noise”. By this, I mean that current prevention messages incorporate too much detail about the different ways that potential victims can be approached and focus on the specific details of each fraud which appears. By providing individuals with large amounts of detail, the overall message is lost. For example, for many years prevention messages have focused on warning people to not send money to West African countries, via remittance agencies such as Western Union or MoneyGram. This has been somewhat successful with many victims I have interviewed in my recent Australian study indicating this would have been a warning sign for them. However, in their cases they were asked to send money via a bank transfer to an Australian bank account. While this was also fraud (and likely to be transferred into a money mule account which would be onforwarded to West Africa), it demonstrates the counterproductive outcomes that arise from framing prevention messages at a micro level. The ways in which offenders can target potential offenders is limitless in its possibilities. Each one of 150 victims I have interviewed have had a unique story, with each bearing some similarities to others, but always with at least one aspect or element which is different. However,

what is consistent across all the victims is the request from the offender to send money, personal details or passwords at some point during their communication. Therefore, I would argue that our prevention messages need to focus on this higher level concept, rather than get caught up in the details and specificities of the possible circumstances that one can be approached, the method of being asked to send money and the country in which to send it to. These can all be modified by an offender and are therefore somewhat redundant. Instead, fraud prevention messages need to be premised on the sole characteristic which is consistent across every victim experience: the request to send money, personal details or passwords. We should be educating people that if a request such as this comes through, regardless of who it is from and regardless of the circumstances that it originates, the answer should be no. This would help to overcome the many victims who clearly have an understanding of fraud, but were not able to identify their particular situation as fraudulent and apply this knowledge to their own circumstances.

The increase in self-managed superannuation funds also has a role to play in the fraud victimisation of seniors. Retirees are increasingly able and willing to control their own retirement funds rather than use traditional superannuation funds managers. While I cannot speak to the advantage or disadvantage of this as a whole, in terms of fraud it has significant consequences. It gives offenders a pool of willing retirees who have a large sum of money available to them and who are actively looking for opportunities to invest and provide for their retirement. In many cases, this has ended in disaster for older victims, who have invested all of their superannuation and life savings into fraudulent investment schemes. Varying levels of financial literacy in these circumstances have not been able to act as a protective factor against this type of victimisation. It is also important to note that not all fraudulent investment schemes offer a return which would be considered outrageous. Rather, offenders are savvy to this, and can instead offer modest returns to entice a potential victim. In my recent round of online fraud interviews, one victim who invested in a fraudulent company was actually able to withdraw his money out at one stage, including the profit he had made on it. His ability to do this easily without any question led him to believe in the legitimacy of the company to which he then reinvested this money with extra capital. In the end, he lost approximately $200,000. This highlights the ways in which offenders will draw victims in, with the aim of gaining as much money from them as possible.

Overall, it is important to educate seniors on financial literacy. However, I would argue that one cannot rely on financial literacy in isolation to protect against fraud and protect the financial security of seniors. Rather, it is a more complicated issue which requires careful thought and consideration about prevention messages and the content of any education efforts. It must focus on the higher level concepts (such as the transfer of money) and it must take account for the highly skilled social engineering and persuasion techniques used by offenders to gain compliance from potential victims.

2) What support and advice is available to assist seniors with their independent financial decision-making

From the older victims of fraud I have spoken to, I would argue that there are current gaps in terms of the provision of advice and support offered for financial decision making. Several victims have sought advice from a variety of third parties, including banks and financial advisors. In some cases, the advice was sound, however the victim was convinced of the legitimacy of the request made of them through successful coercion from the offender. However, in other cases, bank managers and others in the finance industry have also been unable to determine the fraudulent nature of the offer or scheme presented to them, or they have been unwilling to advise their clients (in this case seniors) of their suspicions and have instead enabled the fraudulent transactions to occur. For example, there has been more than one occasion where a victim has described how they went to the bank and spoke to staff who have assisted them to open accounts to receive alleged winnings or inheritances that were supposed to be coming. While some bank staff have expressed suspicion at the legitimacy of these situations, they still willingly assisted the victims which consequently keeps the victim involved in the fraudulent scenario (and likely sees them send further amounts of money to their offender/s). While there are challenges from the perspective of the bank in terms of weighing up the protection of their customer versus the independence of the customer's decision making capacity, the creation of bank accounts which create a false sense of hope to victims is not a satisfactory outcome.

In addition, there is a gap on where seniors can access information about potential requests that come through, particularly focused on investment or business opportunities. Several victims in my recent round of interviews detailed the steps they took to research and investigate the company and the offer which was given to them. Several had done what they deemed to be due diligence but were unable to ascertain satisfactory information. Seniors had called various government departments and taken measures they assumed would protect them and their investment. In some cases, the inability to find anything detrimental led them to believe in the legitimacy of the company. Again, this is a complex issue, whereby government departments must be careful in giving out information and advice about companies and potential investments. However, the many barriers that victims experience in trying to access information led them to believe in the lies they were being fed by the offender/s. In other words, the inability of anyone to tell them the offer was fraudulent with 100% certainty, led victims to give the fraudulent company and the offender the benefit of the doubt. Often, victims found out too late about warning issued by government or other agencies about the companies they had invested in.

Another factor relevant to this is identity crime. It is not uncommon for offenders to take on the identities of legitimate businesses or individuals to gain the trust and compliance of potential victims. In these circumstances, no amount of research or advice can necessarily ensure that the person or company that the victim is communicating with is who they say they are. Given the trusting nature of many individuals and their inability to comprehend identity crime as a whole, this poses significant challenges in guarding against fraud.

Overall, these points highlight the challenges that exist for agencies to provide adequate support and advice for seniors on matters relating to their financial security.

3) Online and internet based vulnerabilities and the prevalence and vulnerability of seniors to scams

There is much debate and discussion in the literature about the victimisation of older persons in relation to fraud. Generally speaking older persons have the lowest levels of any crime victimisation. However, while the total amount of crime victimisation is low, consumer fraud constitutes the highest category of crime experienced by older persons. In terms of fraud, while there are studies which argue that seniors are overrepresented in fraud victimisation statistics, there are stronger studies which assert that older persons are not more likely to be victims of fraud compared to younger persons. This finding is confirmed in the most recent publication from the Australian Competition and Consumer Commission annual report entitled *Targeting Scams*, which documents recorded fraud complaints to the SCAMWatch website from 2014. This indicates an even representation across the age groups 25 years to over 65 years in terms of reported events. While there is a strong argument that seniors are not overrepresented in consumer fraud statistics as a whole, there are types of fraud which particularly target seniors. For example, telemarketing fraud and home repair fraud victims are dominated by older persons.

There is a clear argument though in the literature, on the attractiveness of seniors as potential fraud victims. Many older persons are seen to be vulnerable in three ways. The first is through the ageing process, whereby older persons are understood to have diminished physical and cognitive capacity. This views older persons as easy targets purely as a result of their age. The second vulnerability is social, whereby older persons are seen to be physically isolated from family and friends. The majority of studies which examine the issue of older fraud victims are premised upon the factors of loneliness and isolation as contributing factors to fraud victimisation. The third vulnerability is financial. Many seniors are lucrative targets, as they have access to superannuation, life savings, have strong lines of credit, and generally own assets (such as property). From an offender's perspective, this is an appealing prospect. While there is limited evidence to support the success of these perceived vulnerabilities, there is a strong argument to be made on the fact that seniors are more likely to be targets of fraud.

There is also a compelling argument on the impact that fraud victimisation can have on an older person. By the sheer virtue of their age, the ability of an older person to recover and recoup any financial losses is minimal. Many older victims I have spoken to as part of my research were financially well off and comfortable prior to their victimisation, but in the aftermath of fraud, they become reliant on a government pension and benefits, and struggled to make ends meet. Several older victims have lost their houses and report issues of homelessness, in addition to struggling to pay bills and meet daily living costs. Some have foregone medical care based on the costs and their limited income. There is also an additional impact for older fraud victims, in terms of fraud acting as an indicator for diminished capacity. The majority of older victims will not disclose their fraud victimisation to family or friends, based on a perceived fear of how the family will react. Many feel guilty for having lost their child/rens inheritance. Others are afraid that they will be disowned by family and lose access to grandchildren. There is also the prospect of losing physical and financial independence from well-meaning children seeking to protect their parent/elder from future victimisation. I was made aware of one particular example from Canada, where a victim's son found

out about her fraud victimisation. He consequently took control of her finances and cut off her telephone and internet access, which essentially isolated her from the outside world. This exacerbated the shame and humiliation she was already feeling. It is unknown however, if this is a common occurrence and if the fear expressed by older fraud victims is accurate.

The evolution of technology has increased at a rapid pace and many seniors are embracing the benefits that technology affords in terms of increased communication with family and friends. It also has the ability to decrease isolation through virtual communities, which can overcome some of the physical barriers that some seniors face. However, not all seniors are comfortable or confident in using the internet. Many seniors do not understand the technology and therefore are unable to take simple steps to protect themselves in terms of having virus protection for their computer, maintaining regular updates of their software, and security settings on their social media accounts. There is a level of trust placed in the internet which is not accurate, as well as a misunderstanding that the internet is never truly anonymous or private, particularly when sharing photos and updates. In some circumstances this can lead to a person exposing themselves and their vulnerabilities to potential offenders. There is also a lack of understanding around identity crime. As previously stated, many victims did their own research and what they perceived to be due diligence on the person or company that they were involved with. They were not able to understand that simply because the person or the company may exist, they were not actually communicating with that genuine identity.

However, what is most common from the seniors I have interviewed is simply the success of highly skilled offenders who use social engineering and persuasion techniques to gain the trust of victims. This is highly evident in the dominance of dating and relationship fraud (known commonly as romance fraud). This particular type of approach is the most devastating, as victims grieve the loss of the relationship as well as any financial impact. Romance fraud preys upon the desire of a victim to establish a relationship (romantic or otherwise) and uses the trust and rapport developed between the victim and the offender to elicit compliance. Many of these schemes are sophisticated and mirror grooming techniques employed by child sexual offenders. In some cases, victims can be groomed for months or even years before the initial request for money is sent. In some circumstances, the intimate nature of these relationships also provides a means to blackmail and extort the victim for money with the threat of explicit images or footage being exposed. Romance fraud is also the hardest type of fraud to prevent, given its nature. Everyone wants to believe that there is someone out there and it can be difficult to challenge people about the legitimacy of their perceived relationship. The techniques used by offenders are also complex, and will move seamlessly between email, online chat forums, text message, telephone, and in some cases, face to face. This barrage of communication and affection can overwhelm the senses of a victim and distort their ability to see the requests for money objectively.

As previously stated, may victims have prior knowledge about fraud in general, and in some cases, about the particular type of fraud that they were involved with. However, in each circumstance, the victim was unable (or sometimes unwilling) to see their situation for what it was and to apply their knowledge to what was presented to them.

In addition, from my recent round of interviews with fraud victims, it also became evident that for some seniors, there is an assumption that there are laws which will protect them and refund their money if the situation is found to be fraudulent down the track. There is a belief in the existence of a

regulatory framework and accompanying legislation, that if they are defrauded, that there will be a legal response to that. Many seniors framed this around an expectation of a criminal justice response to their situation. This was particularly evident for those who sent money to offenders via bank to bank transfers. There was a common assumption that if the money was transferred through the bank, they would be able to get this back. However, this was not the case.

Overall, everyone has a weakness and vulnerability, which if targeted in the right way, at the right time, can be exploited. Seniors are no exception. However, there are particular aspects to the victimisation of older persons which need further consideration as to how prevention can be more effective as well as work needed to reduce the severity of the impact that fraud victimisation can have on the individual. There are many gaps here for future work.

4) Agencies and organisations that provide advice and support to seniors requiring financial protection

From my experience in talking to older victims of fraud, from their perspective there is a severe lack of agencies which can assist with advice and support. While some victims did seek advice from banks or financial advisors, this has mixed success in terms of the quality of advice provided. In some cases, these individuals or agencies supported the victim in their fraud victimisation or enabled them to continue their involvement despite providing warnings. It is acknowledge that this is a difficult balance to strike at times, between the need of the agency to protect their client/customer and the independence of the individual to make their own decisions. However, there are instances from my interviews where this has clearly failed.

Bank staff, financial advisors, solicitors and medical staff are all in a position to exert influence on older persons and are seen by many seniors as trustworthy. This provides an opportunity to increase the knowledge of these professionals to the reality of fraud, and provide information on the complex and dynamic nature of fraud victimisation and how to best communicate any potential concerns with the victim. Fraud victimisation also does not necessarily imply that the victim has lost their capacity to manage their own affairs. In the majority of interviews I have undertaken, victims are and have been highly successful in all other aspects of their lives, apart from this one decision. One fraud victim stated that when she told her daughter, she reassured her by telling her not to let the fraud victimisation define who she is. It seems that in many cases, this one situation has come to define the otherwise successful lives of older victims, as somewhat of a failure.

In saying this, there are instances where the mental health or cognitive ability of an older person may contribute to their victimisation and steps may need to be taken by third parties to prevent further harm or loss. This does need to be recognised, but also needs to be treated in a different manner to other fraud victims.

Fraud is unique in that there are a number of agencies that victims can report to, including law enforcement, consumer protection, government, non-government and civil organisations which could potentially take a complaint. This can be very difficult for victims to navigate and is not helped by agencies who are unwilling to take a complaint from a victim, instead referring them to another agency. This is termed the “merry-go-round” effect and is an immense source of anger and frustration for victims in trying to make a complaint. In many instances, they are not successful at reporting in person and consequently may turn to online portals, such as SCMAWatch, as there is no human interface to screen them. However, the expectations are still there in terms of their report initiating action and an investigation, and when this does not occur, there is even greater disillusionment with what has happened. Victims report feeling retraumatised by the system in addition to the fraud victimisation in of itself.

It is acknowledged that fraud, particularly in the online context, poses significant challenges for law enforcement. However this is not always directly communicated to victims in an empathetic manner. Much can be done by all agencies within the fraud justice network to improve their interactions with victims, by treating the victim with respect and empathy and by giving a timely and

accurate account of what, if anything, can be done about their case. This would be greatly valued by all fraud victims.

Chronic victims also pose distinct challenges to organisations seeking to better respond to fraud. This is a small group of individuals, seniors included, to which there is currently little known information about and even less action directed towards them. It is easy to dismiss them as refusing to listen to advice and therefore having responsibility for their own actions. However this is not a useful response and there is much work to be done for this particular group. Members of the financial sector are in an important position to identify and assist this particular group of victims.

In terms of support for fraud victims in the aftermath of their victimisation, there is little on offer. Fraud consistently has one of the lowest reporting rates of all crime types and online fraud is even lower. There are many contributing factors, including the inability of victims to recognise their involvement in a fraudulent situation, the shame and stigma associated with this crime type, and a lack of knowledge on where to report. This lack of reporting overall by victims means that many suffer in silence and are unable to disclose their victimisation to anyone, including family, friends or law enforcement. While there are studies which indicate the impact of fraud can be similarly devastating to those who experience violent crime, the victim response is not commensurate. The Queensland Police Service has established a victim support group which is dedicated to fraud victims and has been running since 2010. This provides a vitally important safe environment for victims to share their experiences with those who understand. However, it is limited to a narrow geographic area, whereas fraud victimisation is not.

Current legislation in Queensland also prohibits fraud victims from accessing financial assistance under the *Victims of Crime Assistance Act 2009*. While the definition of victim in this act recognises harm and injury of all kinds, there are specific provisions which limit any support exclusively to victims of violent crime. This means that fraud victims are not able to access financial support for any counselling of financial counselling that they may need to assist in their recovery. In addition, fraud victims are generally excluded through other measures in the criminal justice system designed to promote victim participation. For many fraud victims, given they have sent their money overseas, there is no ability for local law enforcement to initiate an investigation, they are unlikely to have an offender arrested and prosecuted, and therefore unlikely to gain a conviction. As a result, processes such as victim impact statements are irrelevant to these circumstances and most victims will not get any closure or sense of justice. This can add to the overall frustration and anger felt by the majority of victims.

Overall, there are many opportunities to improve the current response to older persons in terms of providing advice and support to them regarding their financial security. In particular, when this is compromised through fraud, there are large gaps which need to be filled in terms of providing support and recovery. At present, it is easy to argue that fraud victims are invisible in the criminal justice system. It is recognised that the sheer nature of fraud, particularly online fraud, places legitimate constraints on agencies such as the police. However there are significant opportunities which exist to improve the response to fraud victims, particularly seniors, to assist in their recovery and seek to restore their overall wellbeing.

5) The role of the financial sector in ensuring adequate safeguards for seniors in relation to financial decision-making

So far, this submission has provided clear gaps which currently exist in relation to protecting the financial security of seniors. The financial sector has a role to play in this, however they will not be able to achieve this in isolation from other agencies and sectors. One of the difficulties in seeking to improve safeguards is the lack of information on which to base any analysis on. Based on my own experience, I can certainly attest to the challenges faced in trying to gain accurate knowledge in this area. However, this does not mean it cannot be achieved. It is important too, to include the voices of seniors in these discussions, as any changes or actions will have a substantial impact on them. Any future actions need to be carefully considered, based on solid research and include strong stakeholder participation from seniors.

In conclusion, this submission has sought to put forward a summary of my own knowledge and experience based on research that I have done on this topic for a number of years. It is premised on existing research as well as that conducted by myself and colleagues, specifically examining how fraud impacts on the financial security of seniors. Fraud poses a significant threat to the overall wellbeing of seniors, including their financial security. Again, I commend the committee for taking the time to examine this important issue and look forward to continuing this discussion and further work in the future.