SUBMISSION No. 49

Joint Select Committee on Cyber Safety
Department of House of Representatives
Parliament House
Canberra ACT 2600
Australia

28 October 2012

RE: Inquiry into Cybersafety for Senior Australians

My name is Dr Cassandra Cross and I have recently been appointed as a lecturer in the School of Justice, Queensland University of Technology. However, for the past five and a half years, I have been a research and policy officer with the Queensland Police Service. Since 2008, I have conducted extensive research focused on the problem of online fraud victimisation, particularly as it relates to seniors. While this research has not yet been formally published, links to publically available articles on these research results can be found in Appendix 1.

The following submission articulates my thoughts and observations regarding the terms of reference for this inquiry from my involvement in two separate projects. The first is my experience as a Churchill Fellow in 2011 and the second is a project entitled *Seniors Online Security*, which was delivered by the Carindale Police Citizen's Youth Club (PCYC). A brief summary of each project is detailed below:

Churchill Fellowship

In 2011, I was awarded the Donald Mackay Churchill Fellowship to study methods for preventing and supporting victims of online fraud. This fellowship was given to me through the Winston Churchill Memorial Trust of Australia. As part of this fellowship, I travelled to the United Kingdom, the United States of America and Canada, to examine other jurisdictional responses to the problem of online fraud. During the eight weeks that I was away, I spoke to over thirty agencies across law enforcement, government, industry, academic and community fields. The wealth of knowledge and expertise that I learnt from this trip was invaluable. It was abundantly clear from this trip that Australia has much to learn from overseas responses surrounding the prevention and support of online fraud victimisation. A link to my report, detailing the trip and my subsequent recommendations, can be found in Appendix 1, with a full copy of this attached.

Seniors Online Security Project

In 2010, the Carindale PCYC was awarded $86,000 from the Australian Government under the *Proceeds of Crime Act* grant scheme. This money was provided to develop a training package targeted specifically at seniors on issues relating to computer and internet security. With the support and advice of a project reference group and key stakeholders in this area, I developed all the training materials for this project. The project was officially launched on 20 August 2012, as part of Senior's Week. The complete package comprises individual workbooks and accompanying PowerPoint presentations across five distinct topics. These are computer security, identity crime, social networking, fraudulent emails and internet banking.

The aim of the training package was to develop a resource for seniors to be able to better educate themselves about online security, either individually or in a group setting. It has also created a resource for police and other agencies to be able to deliver presentations to seniors on these topics as required. The training materials seek to empower seniors through the provision of simple steps that can be taken to reduce the likelihood that they become a victim of online fraud. A link to all available training materials is provided in Appendix 1.

The following submission is broken into the four terms of reference, with evidence from these projects (where relevant) to support the argument presented. It is important to note that the views expressed in this submission are my own and do not necessarily reflect those of the Queensland Police Service, the Winston Churchill Memorial Trust or the Carindale PCYC. Therefore, any errors which appear in the content of this report are the sole responsibility of the author.

Should you wish to discuss further any of the content presented in this submission, please contact me directly on the details below.

Thank you for your consideration.

Dr Cassandra Cross

2011 Churchill Fellow
Lecturer, School of Justice, Faculty of Law
Queensland University of Technology

1) The nature, prevalence and level of cybersafety risks and threats experienced by senior Australians.

The development of technology has had significant changes for society. In particular, the advancement of the internet has opened up lines of communication which were previously not possible. With relative ease and minimal costs, a person can communicate with others from across the globe, through email, social networking sites, chatrooms and web cameras. While the benefits of this technology are many and varied, so too are the threats which arise from the use of the same technology. Consequently, there are several things that seniors need to be aware of when using their computer and the internet.

However, it is important to note up front, that seniors are not the only demographic who are vulnerable to security threats from the internet. All users are vulnerable. Everyone has a weakness, which if targeted in the right way, at the right time, can lead to online victimisation. It is not useful for an individual to think that victimisation only happens to other people and that will never happen to them. This isn't to scare people away from using the internet, rather it to assert that every person needs to acknowledge their own vulnerability in an effort to avoid and recognise possible threats. Despite this, seniors can be attractive targets for criminals for a variety of reasons. Seniors generally have access to the superannuation, life savings and own their own assets. In many cases, seniors are also looking for opportunities to invest their money, and can be easily manipulated into fraudulent transactions.

The risks experienced by seniors are common to all internet users, and focus predominantly on a loss of their identity and their finances, both of which are more specifically outlined below.

The use of the internet to share and store information has had a profound effect on the security of private data. Individuals are increasingly sharing more of themselves within the virtual world, without recognising the possible security threats which exist. Many seniors do not realise the value of their own personal information. They do not recognise how personal information can be traded as a commodity in a similar fashion to money. Overall, greater emphasis needs to be placed on the need to secure personal data in the same way that money is protected.

Along these lines, there are many misunderstandings that seniors have about the nature and privacy element of the internet. For example, seniors may think that only their friends and family can view information that they have posted on a social networking site. However, without adequate security settings, this information can be seen by anyone. Many seniors do not have an adequate knowledge of security settings on accounts, either about their existence in the first place, or the importance of changing the default setting. They believe that only their contacts can access the information that is being posted. In reality, this is not the case.

Fraudulent emails (namely phishing emails) also pose a threat to the security of personal information. Many seniors will respond to fraudulent emails with personal details for one of two reasons. They will either believe in the legitimacy of the email or they will respond on the basis that they don't perceive the sending of personal information to be problematic. Regardless of the reason, this then renders the individual exposed to potential identity crime or loss of funds through their bank accounts being accessed.

Fraudulent emails also pose serious a serious threat to the overall financial wellbeing of many seniors. While all computer users can successfully discern hundreds, if not thousands, of fraudulent emails across their lifetime, it only takes one response to become a victim. As previously stated, all individuals have a weakness or vulnerability, which if targeted in the right way at the right time, can be successfully exploited. Education and awareness of frauds does not necessarily counteract against victimisation, as many highly educated and otherwise savvy individuals have become victims of online fraud. Fraudulent emails can manifest themselves in an endless number of possible scenarios, and can include (but are certainly not limited to) lottery notifications, inheritance notifications, business investments, job advertisements, and charity schemes. In addition, the use of social networking, particularly online dating websites, has allowed romance and dating fraud to flourish. This is perhaps the most insidious type of fraud, as it compounds the financial damage with the loss of a perceived relationship, romantic or otherwise.

Overall, the risks experienced by seniors using the internet generally mirror those faced by other demographic categories of internet users and revolve around the security of personal details and finances. Both of these can be compromised, leaving seniors vulnerable to online fraud victimisation. The actual extent of victimisation is not well known, with reporting rates on this type of crime unreliable in terms of underestimating the true nature of victimisation. This stems from many factors, which include not knowing who to report it to (banks, police or government agencies), a belief that nothing can be done to rectify the situation, and most significantly, the stigma arising from a sense of shame and embarrassment in having become a victim of online fraud. This may be exacerbated for seniors, who fear that family members will deem them to be incompetent to manage their own financial affairs, their online fraud victimisation be made public.

2) The impact and implications of those risks and threats on access and use of information and communication technologies by senior Australians.

As previously stated, the risks experienced by seniors when using computer and internet technology, are not significantly different to those experienced by members of the general public. However what differentiates seniors is the impact that victimisation can have on their lives. Obviously a monetary loss incurred by a 70 year old will have a far greater impact than a similar loss experienced by a 30 year old, who still has the majority of their working life to recoup the loss and regain financial security.

What can be seen as unique to a significant number of seniors is a knowledge of the internet. Having not grown up with the technology or been exposed to it in the same way as younger generations have experienced, this can impact on their ability to use the internet safely and in some cases may contribute to their victimisation. While many seniors have an in-depth understanding of the internet, there are many more who do not have such knowledge. In many instances, a lack of knowledge creates a fear of the unknown and an awareness of the risks posed by online fraud tends to exaggerate this fear.

The area in which this appears to be most prevalent is the use of internet banking. Even individuals who are confident and proficient in using other aspects of the internet, such as email and social networking, do not have the same attitude towards online banking. While the exercise of caution is a positive attribute, there appears to be an inability or an unwillingness to engage technology in this manner. This can impact on the ability of seniors to access their bank accounts and conduct financial transactions if they continue to rely upon face to face transactions at a branch.

For those who have been victims of online fraud, the impact of their victimisation can be significant and can negatively influence their trust and confidence in using the internet. As a result, this can further isolate the individual, who is likely to already be suffering in silence the burden of their victimisation experience. Ideally, the internet has the ability to engage seniors and address the isolation that many older people experience. However, in some circumstances, it appears to have the opposite effect and in fact excludes those who no longer have confidence to use the internet or place their trust in the happenings of a virtual world.

More generally, the prevalence of risks encountered when using the internet can ostracise older people, in terms of reducing their confidence to use the computer in a safe manner. This needs to be overcome, so that older people are empowered to use the internet consistent with the majority of society as a whole.

3) The adequacy and effectiveness of current government and industry initiatives to respond to those threats, including education initiatives aimed at senior Australians.

There are many lessons that can be learnt and adopted in Australia from overseas jurisdictions in terms of responding to the threats posed by the cyberspace. It is my opinion that there are several deficiencies which exist relating to current efforts to prevent online fraud victimisation and subsequently support individuals who become victims of online fraud.

The first area relates specifically to education initiatives targeted at seniors. Education and awareness campaigns are an important aspect of addressing threats posed to seniors by the internet. However, it is my belief that the way these are currently approached is problematic for a number of reasons. Prior to my Churchill Fellowship trip, I wrote a discussion paper which I distributed to all the agencies that I was visiting. As part of this discussion paper, I posed a series of questions, seeking to determine how each jurisdiction targeted their prevention messages and the perceived effectiveness of these prevention messages. The reason for this line of questioning was premised on the challenges that I believed existed in targeting a fraud prevention message that was wide enough in scope to encompass the various types of online fraud, but specific enough to target individual situations.

My Churchill Fellowship trip has significantly changed my perspective on how we educate people (including seniors) and how to structure these prevention messages. In particular, my ongoing discussions with Detective Constable Michael Kelly, Financial Crimes Unit, Toronto Police, have strongly influenced the following arguments (particularly the coining of the phrase “white noise”). Currently, our prevention messages around fraud and online security in general, focus on the many ways in which fraud can occur. Whether it be through a lottery notification, or an investment invitation or a relationship request, our messages are primarily concerned with the large variety of ways in which a person can be approached. The problem with this method is that there are an infinite number of ways in which a potential victim can be targeted. Prevention messages and awareness campaigns will struggle to remain current and relevant, as criminals modify and refine their approach methods on a daily basis. Educating people to be aware of a single or group of characteristics relating to a particular fraud approach, can blind them to other methods used in different, albeit similarly fraudulent, approaches.

In looking at online fraud, what is central to every situation is the transfer of money or the sending of personal information. Without this there is no offence and no victim. How a victim got to that point is irrelevant, rather what they do in that moment, when asked to send money or personal details, is crucial. The effectiveness of all prevention messages and awareness campaigns culminate in that moment. Therefore, it is the transfer of money or the sending of personal details that should form that focus of all future prevention messages around the particular threat posed by online fraud. In the same way that society has generally been conditioned to read through a contract prior to signing, individuals need to become accustomed to thinking through the potential consequences of sending money (particularly overseas) or sending personal information. Everything else can be seen as “white noise”. To give a simple analogy, take any capital city. There are likely to be hundreds of different roads that a driver can take to get into the city. Each individual driver can take a different route, however all end up at the same destination. The specific roads they travelled become irrelevant to their arrival at the final destination. In the same way, the transferral of money or the sending of personal information by a victim is the final destination. How the person arrived at that point, the way they were approached and the reasons or excuses that they were given to justify sending money or details are irrelevant. Future prevention messages concerning this particular cybersafety threat should be focused more on the essential element of all fraud offences, being the transferral of money or the sending of personal details, rather than how the situation eventuated. In essence, I believe that current prevention messages focus too much on the “white noise” of fraud, and fail to adequately recognise how the offence actually unfolds.

An example of this approach is evidenced in the *Seniors Online Security Project* undertaken by the Carindale Police Citizens Youth Club (PCYC). The PCYC received $86,000 to develop a training package targeted specifically at seniors about online security issues. Five separate modules have been developed, on the topics of computer security, identity crime, social networking, fraudulent emails and internet banking. Having commenced writing these training materials after my Churchill Fellowship trip, I was fortunate enough to be able to integrate the lessons I had learnt overseas into the key prevention messages promoted in the training package. Each topic is structured in the same manner, with short introduction to the topic (generally outlining the benefits of current technology but acknowledging that problems may occur), an outline of the main threats to be aware of, revision questions to reinforce knowledge about potential threats, the provision of simple steps to reduce the likelihood of victimisation, suggestions on what to do if victimisation occurs and a revision scenario to encourage the application of knowledge to a real life situation.

However, each booklet deliberately focuses on the higher level prevention messages rather than the complexity of addressing every possible fraudulent situation. For example, a key message throughout the five topics relates to the sending of personal details. In each instance, the message clearly states that “no one should send you an email asking for personal details” and encourages people to think through the consequences of sending information. The same goes for the sending of money. The key message centres on the fact that “you should be very wary if a person asks you to send money”. It encourages the recipient to think through why they have been asked to send money, who has requested the money and clearly articulates the lack of recourse available if down the track, the transaction is determined to be fraudulent. Rather than focusing on the ways in which a person can be targeted to send personal information or money, these training materials specifically focus attention on the sending of personal data or the transferral of money. In addition to these two examples, each of the booklets promotes a variety of simple steps that seniors can take to reduce their likelihood of victimisation. This includes things such as installing anti-virus protection and a firewall on their computer and regularly updating it, using strong passwords, avoiding links in emails, avoiding public computers for internet banking, using an email filter and above all, using the delete key. It is hoped that these types of prevention messages are simple enough for seniors to be able to remember, and can empower individuals to use their computers in a safe and confident manner. Feedback from seniors groups to date has been overwhelmingly positive about the training materials, specifically in terms of the content and how it is presented to seniors. It is hoped that this will become a valuable resource for this demographic.

From my experience, there is a continually high demand from seniors groups who are thirsty for information to be presented to them on the topics of computer and internet security. This is positive as it indicates that this demographic are willing to engage with the topics, are willing to learn and hopefully improve and modify their behaviour. In this manner, education and awareness campaigns are important, however I believe that there needs to be a shift in the way that these are presented to seniors and the community in general. I also don't believe that education and awareness by themselves, will reduce victimisation of seniors from the threat posed by online fraud. It is too easy to say that education is the only solution and will subsequently eliminate the problem. Realistically this is not the case, for if it were, then other social and health problems would have already been eradicated. Knowledge of a problem doesn't necessarily protect against experiencing or even identifying the problem in a personal capacity.

Along these lines, more work is required on concentrating on the enablers of fraud, rather than simply educating the public against it. The following scenario was quoted to me by Detective Constable Michael Kelly, Toronto Police Service, and is pertinent to the current argument.

If swimmers were repeatedly drowning in a public pool, it is unlikely that patrons would be advised to improve their swimming ability and a few extra warning signs erected. Rather, it is likely that measures would be taken, such as the introduction of life guards or the expansion of existing life guards, with specialised training, to ensure that people were kept safe. There would be an expectation that life guards would supervise swimmers and intervene when a person experienced difficulty, to prevent further deaths from occurring. There is also a likelihood that the pool owners would be mindful of any criminal or civil consequences which could ensue for not taking sufficient precautions in the first place.

In the same vein, greater attention needs to be drawn towards the mechanisms that enable fraud to occur. Online fraud does not simply involve a victim and an offender, rather it involves a wide array of people and services, which include the means of communication between the victim and the offender and the means of transferring the money. This is not to lay blame one any one party, however it is to acknowledge that current responses to fraudulent transactions by banking institutions and money transfer agencies could be examined with a view to improving their services for legitimate purposes and reducing their involvement in fraudulent transactions. Further work on how this might be achieved and what any changes might look like, needs to be prioritised in the future, and needs to be a collaborative effort, involving all relevant parties. It may involve changes to legislation and policy, improved financial practices or different policing tactics and enforcement methods. However, it is clear from the current level of victimisation and monetary losses experienced, that the current response is not adequate and is not protecting victims.

In looking at the current adequacy and effectiveness of responding to threats posed to seniors within an online environment, focus also needs to be given to the relationship between victims of online fraud and the criminal justice system. There is a strong differentiation between victims of violent crime and victims of non-violent crime, which includes victims of online fraud. Within Queensland for example, the *Victims of Crime Assistance Act (2009)* defines a victim as someone who has suffered harm as the result of a crime committed against them (Section 5), which arguably includes both victims of violent and non-violent crimes. However, in order to access any financial assistance to cope with the consequences of the crime, the definition of victims is restricted to victims of violent crime (Section 21). The legislation does include a set of fundamental principles for the fair and dignified treatment of all victims, which adheres to the initial broad definition of victims, however the majority of these do not apply to online fraud victims.

By the very nature of the crimes committed against online fraud victims, their involvement with the criminal justice system is limited. The global nature of online fraud and the reality that many victims will send money overseas to a variety of countries, excludes them from participating and accessing the victim initiatives that are accessible to other categories of victims. For example, the large majority of online fraud victims will not have the opportunity to see their offender arrested, will not be able to participate in any court proceedings, will not be able to give evidence about their experience, will not be able to provide a victim impact statement, and will not have the ability to participate in any victim-offender mediation or restorative justice proceedings. Victims of online fraud are excluded from all current victim initiatives within the criminal justice system, based solely on the type of offence which has been perpetrated against them. This directly contravenes many of the fundamental principles of justice which are argued to exist for victims of crime in Queensland.

This omission is a constant source of frustration for this category of victims, who despite experiencing the real and devastating effects of victimisation, have no practical recourse available to them. This does nothing to reduce the sense of helplessness felt by victims of online fraud but reinforces the sense of shame and embarrassment felt by many and the isolation of succumbing to this type of offence. It also does not encourage the reporting of this type of crime to police, given that there are significant limitations on what action, if any, police can take. While the complexity of online offences presents substantial challenges to law enforcement and the criminal justice system, action needs to be taken to address this exclusion and to recognise the legitimacy of online fraud victims, in terms of the support and assistance they require as a result of what has occurred.

The consequences of victimisation for online fraud victims and their subsequent exclusion from the criminal justice system can have devastating effects on individuals, particularly seniors. There appears to be a misconception in society that victims of fraud only lose money, however the reality of the situation extends to so much more. In many cases, online fraud victimisation can lead to a deterioration of physical health, a decline in emotional health (manifested most frequently through varying levels of depression), relationship breakdown and in the most extreme cases, suicide. This is in addition to the financial pressures that a victim may experience, such as an inability to purchase food or other essential items, difficulties in paying rent or their mortgage, and the failure to be able to access required health care services. The losses experienced by victims are so much more significant than simply a loss of money. However, given the inability of general society to acknowledge victims of online fraud as victims, recognition of the extent of their losses is not forthcoming. Coupled with the stigma associated with this type of victimisation, the majority of victims suffer in silence and without the help and support they need to be able to move forward in their lives.

Overseas jurisdictions have a far greater understanding of the impact of online fraud victimisation and the need to support the general health and wellbeing of victims. Throughout my Churchill Fellowship, several agencies shared tragic stories of victims who had taken their own lives as a result of their fraud victimisation, with the majority of these victims being seniors. An example of such a victim was a lady in her late seventies who had lost a substantial amount of money as the result of fraud. In addition, she had involved her brother, and he subsequently lost money to the same situation. The woman committed suicide, her brother unsuccessfully attempted suicide, and was left in a vegetative state. A third sibling was then left to pick up the pieces of this family, having had no knowledge of the fraud victimisation that both his brother and sister had experienced. While this is an extreme case, it is likely not to be as isolated as we might believe. Older Australians have greater vulnerabilities after becoming a victim of online fraud, particularly around the impact of their victimisation, and further work needs to be done to prevent tragedies such as the above occurring in any country. The current lack of recognition of online fraud victims as victims and an absence of support services available, in combination with the stigma associated with this offence, does nothing to promote the recovery of online fraud victims, especially those who are seniors.

There are two examples of support services specifically targeting fraud victims, which exist in the UK and Canada, which highlight the difference in support offered overseas compared to Australia. As stated earlier in this submission, ActionFraud act as the central reporting agency for all fraud offences in the United Kingdom. When a victim lodges a complaint with ActionFraud, as part of the call process they are asked about the severity of the impact of their crime. Based on this response, and with the individual’s consent, they are referred to Victim Support, which is a national charity staffed predominantly by volunteers. Once a referral has been made to Victim Support, contact is initiated with the victim through a phone call (or a letter if phone contact cannot be established). Victim Support offers the victim emotional support of practical help as needed. If required, face to face support can be offered through a network of agencies across the UK. The volunteers who work for Victim Support have the ability to meet with victims and provide ongoing support and assistance on a case by case basis.

The second example is a program called SeniorBusters in Canada. SeniorBusters was originally established as a small project in 1993 to target telemarketing fraud. However, the magnitude of the problem was soon realised, particularly the high volume of seniors who were reporting victimisation of various types of frauds and seeking assistance. In 1997, SeniorBusters was conceived to meet this identified need. This program utilises around 50 volunteers (all seniors themselves) who work a rotating shift roster to provide support to those who need it. Similar to the UK example, referrals are made to this service through reports made to the Canadian Anti-Fraud Centre, and encompass seniors who have reported fraud victimisation or are considered vulnerable to fraud. Eligible callers are asked if they would like a follow up call from SeniorBusters and with their consent, a volunteer will call the individual on a one off or regular basis to offer support and advice as required.

Overall, there are many areas in which the current response to the threats posed by online fraud against seniors can be improved. These focus on current education initiatives, the enablers of fraud, current participation in the criminal justice system, an awareness of the impact of online fraud and the provision of designated support services. While these areas would arguably improve the current situation for all victims of online fraud, they are particularly important and relevant to older victims of online fraud.

4) Best practice safeguards, and any possible changes to Australian law, policy or practice that will strengthen the cybersafety of senior Australians.

I have been in a very privileged position, as a Churchill Fellow, to travel across three separate jurisdictions and to both observe and discuss with key agencies their responses to the threats posed by the online environment. In doing this, I have been able to identify a number areas in which Australia can improve its current response to the prevention and support of online fraud victims. This includes the many seniors who are victims of this type of crime, as well as the general public. The following reiterates the majority of recommendations that stem from my fellowship report, which is included as an attachment to this submission. These recommendations, with a short justification for their inclusion, are listed below.

1) The creation of a fraud strategy

It is recommended that a fraud strategy and subsequent action plan is developed with the involvement of relevant stakeholders, to provide clear goals, direction and accountability on the future of fraud prevention activities.

While it is acknowledged that online fraud is not the only threat posed to seniors and the community by the internet, I would argue that the nature of this threat is significant and warrants the development of a strategy, which includes online fraud as a major component. The creation of a specific fraud strategy has been successful in the United Kingdom (with the National Fraud Authority leading the implementation of *Fighting Fraud Together*), in terms of clearly articulating a strong vision for the reduction of fraud offences, as well as providing a unified direction to all agencies working in the area. Additionally, it provides a means of accountability to all agencies on how their work seeks to contribute to the overall goal. Within Australia while there are currently strategies in existence, such as the Federal Government's *Cyber Security Strategy*, it is my belief that this does not focus enough on the prevention and support aspect of online fraud victimisation, instead focusing the technical aspects of computing. While this is important, an increased strategic focus on prevention and support is also warranted.

2) A central reporting agency

It is recommended that a central reporting body is established to act as a single point of contact for victims of fraud and enable a single repository for all complaint data.

The UK, USA and Canada all have central reporting agencies when it comes to the reporting of online fraud (ActionFraud in the UK, Internet Crime Complain Centre in the USA and the Canadian Anti-Fraud Centre in Canada). There are clear benefits to the establishment of a single agency. Firstly, it reduces the confusion experienced by many people, including seniors, about who to report an incident to. At present, victims may report directly to their financial institution, the police, or the fair trading department in their jurisdiction. However, in a large majority of cases, victims will not report the occurrence of the crime at all. A single point of contact would alleviate the merry-go-round that some victims currently experience in being sent from one agency to another in order to report the occurrence. It would give victims of online fraud certainly in terms of who to report to, and should improve their satisfaction with the response, if the agency dealt specifically with that type of crime. This would hopefully enable an increase in the reporting of these offences and seek to reduce the large discrepancy which currently exists between actual levels of victimisation and reported victimisation. It also has the distinct advantage of being able to act as a mechanism through which victims can access support services, as seen in both the UK and Canadian examples.

3) The enablers of crime

It is recommended that further work is undertaken to better identify the enablers of fraud, to improve current strategies that address these facilitating conditions.

Across each jurisdiction visited, there was a very strong focus on the enablers of crime, or the conditions/mechanisms that facilitate online fraud to occur. As previously stated in this submission, the crime does not simply involve the victim and the offender per se. Rather, there is the involvement of other people and services, such as the means of communication and the method of transferring the money. By gaining a greater understanding of the ways in which online fraud is perpetrated, it allows all possible intervention points to be better targeted throughout the criminal process. There was a shared belief amongst the UK, USA and Canadian agencies that the ultimate form of fraud prevention lies in the disruption of fraud activity, and it is this belief that should drive further work in this area.

4) Fraud prevention messages

It is recommended that current education and awareness campaigns be reviewed to ensure that the focus is on the essential element of the offence: the transferral of money or the sending of personal information.

These key messages should focus on behaviour modification as opposed to simply detailing the diverse number of ways that a person can be targeted for online fraud. As part of this, it is also suggested that an evaluation method be developed to determine the effectiveness of fraud prevention messages and education materials in achieving their stated goals. There is little value in continuing with prevention messages if they fail to educate seniors and have no marked difference on reducing the number of individuals who become victims of this type of crime.

5) The monitoring of fraud victims wellbeing

It is recommended that a system be developed to better monitor fraud victims and their wellbeing, to enable victims to be able to move forward with recovery after their victimisation.

As stated in this submission, the impact of online fraud goes beyond simply the financial losses incurred through any fraudulent transaction. Rather, victimisation extends to the physical and emotional wellbeing of the individual, as well as impacting on their relationships with those around them. Anecdotally, older victims appear to be more vulnerable than others, and in extreme cases, suicide presents as the only option to victims to end their suffering. As a result, the development of a system or process which enables an improved identification and monitoring of the wellbeing of fraud victims is vital to reduce the impact of their victimisation. There are significant challenges which exist in seeking to improve this area, however that in itself should not be a reason to allow the suffering of online fraud victims to continue.

6) The provision of support services

It is recommended that work is done to identify or develop suitable support services for victims of online fraud and to promote these services.

Further to the previous recommendation, immediate work is required to develop solutions which support victims of online fraud in their recovery. This is likely to be achieved through two means, firstly the identification of current services and infrastructure which can be utilised for this purpose, and secondly, the establishment of specific support programs, similar to those witnessed in the UK and Canada. In terms of current services available, the existence of SupportLink (an e-referral system) in Queensland, Australian Capital Territory and Victoria, can easily cater for victims of online fraud, with some small changes to their interface and the likely addition of services to their existing database of providers. However, the opportunity also exists (particularly in other jurisdictions) to develop a designated support service for fraud victims, which specifically caters for their needs.

Conclusion

The cybersafety of seniors is an important issue. It is vital that this section of the community is able to use their computers and the internet in a confident and safe manner. With society increasingly conducting their everyday lives in an online environment, it is important that seniors are not excluded from this and can enjoy the benefits that this technology has to offer.

However, there are several threats which pose a risk to the security of seniors when engaging in a virtual world. While the threats that they experience do not necessarily differ remarkably from the rest of the population, the impact of any subsequent victimisation does. This submission has focused on the threats posed to seniors through a compromise in their identity or financial security (through online fraud or identity crime). While these are not the only two threats faced by seniors (or internet users as a whole), they are significant in terms of the potential losses they represent to older Australians. Victims of online fraud represent a unique group of victims, compared to other crime categories. Their acceptance as victims and their access to both the criminal justice system and victim support services are severely constrained for reasons beyond their control. This represents an opportunity for considerable improvement to remedy the situation for online fraud victims as a whole, but particularly as it relates to seniors. This submission has highlighted the current issues faced by victims of online fraud as well as put forward recommendations which would seek to improve the current situation faced by many, with the hope that much needed change will occur in the future.

Appendix 1

The following weblinks detail publically available reports of the research that I have conducted with the Queensland Police Service, specifically addressing the topic of seniors and online fraud:

http://www.police.qld.gov.au/Resources/Internet/services/reportsPublications/bulletin/347/documents/internet%20scams.pdf

http://www.news.qut.edu.au/cgi-bin/WebObjects/News.woa/wa/goNewsPage?newsEventID=36941

http://www.ourfrasercoast.com.au/c/document_library/get_file?uuid=30b77676-723e-47d4-b046-03678b78840a&groupId=4362881

A full copy of my Churchill Fellowship report is available at the following:

http://www.churchilltrust.com.au/fellows/detail/3593/cassandra+cross

The complete copy of all training materials which comprise the *Seniors Online Security Project*, are available for electronic download at the following:

http://www.carindalepcyc.org.au/news.php?display_news=true&news_id=60

http://www.police.qld.gov.au/programs/cscp/eCrime/sos.htm

(All links were correct as of 28 October 2012).