THE DONALD MACKAY CHURCHILL FELLOWSHIP

to study methods for preventing and supporting of victims of online fraud.

I understand that the Churchill Trust may publish this report, either in hard copy or on the internet or both, and consent to such publication.

I indemnify the Churchill Trust against any loss, cost or damages it may suffer arising out of any claim or proceedings made against the Trust in respect of or arising out of the publication of any Report submitted to the Trust and which the Trust places on a website for access over the internet.

I also warrant that my Final Report is original and does not infringe the copyright of any person, or contain anything which is, or the incorporation of which into the Final Report is, actionable for defamation, a breach of any privacy law or obligation, breach of confidence, contempt of court, passing-off or contravention of any other private right or of any law.

Signed: Cassandra Cross

Dated: 17/02/2012
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TABLE OF CONTENTS</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>ACKNOWLEDGEMENTS</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>EXECUTIVE SUMMARY</strong></td>
<td>6</td>
</tr>
<tr>
<td><strong>FELLOWSHIP PROGRAM (13 OCTOBER – 9 DECEMBER 2011)</strong></td>
<td>7</td>
</tr>
<tr>
<td><strong>LONDON, UNITED KINGDOM (17 OCTOBER – 4 NOVEMBER 2011)</strong></td>
<td>7</td>
</tr>
<tr>
<td><strong>PORTSMOUTH, UNITED KINGDOM (7 NOVEMBER – 11 NOVEMBER 2011)</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>WASHINGTON, DISTRICT OF COLUMBIA, UNITED STATES OF AMERICA (14 NOVEMBER – 19 NOVEMBER 2011)</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>NEW YORK CITY, NEW YORK, UNITED STATES OF AMERICA (21 NOVEMBER – 23 NOVEMBER 2011)</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>NORTH BAY, ONTARIO, CANADA (28 NOVEMBER – 30 NOVEMBER 2011)</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>TORONTO, ONTARIO, CANADA (1 DECEMBER – 7 DECEMBER 2011)</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>INTRODUCTION</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>THE PROBLEM OF ONLINE FRAUD</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>PREVIOUS RESEARCH EXAMINING ONLINE FRAUD VICTIMISATION</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>THE CURRENT SITUATION FOR QUEENSLAND VICTIMS OF FRAUD</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>AN OVERVIEW OF THE CURRENT PROJECT</strong></td>
<td>12</td>
</tr>
<tr>
<td><strong>THE FELLOWSHIP JOURNEY</strong></td>
<td>14</td>
</tr>
<tr>
<td><strong>UNITED KINGDOM</strong></td>
<td>14</td>
</tr>
<tr>
<td><strong>UNITED STATES OF AMERICA</strong></td>
<td>15</td>
</tr>
<tr>
<td><strong>CANADA</strong></td>
<td>17</td>
</tr>
<tr>
<td><strong>SUMMARY – THE GLOBAL CONTEXT OF ONLINE FRAUD</strong></td>
<td>19</td>
</tr>
<tr>
<td><strong>MAIN FINDINGS</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>A UNIFIED APPROACH TO FRAUD PREVENTION</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>LESSONS LEARNT ON THE BENEFITS OF HAVING A STRATEGIC DIRECTION</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>MOVING FORWARD ON THE DEVELOPMENT OF A STRATEGY</strong></td>
<td>21</td>
</tr>
<tr>
<td><strong>A CENTRAL REPORTING AGENCY</strong></td>
<td>23</td>
</tr>
<tr>
<td><strong>LESSONS LEARNT ON THE BENEFITS OF ONE PORTAL</strong></td>
<td>23</td>
</tr>
<tr>
<td><strong>MOVING FORWARD TO A SINGLE REPORTING AGENCY</strong></td>
<td>24</td>
</tr>
<tr>
<td><strong>THE IMPORTANCE OF RELATIONSHIPS</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>LESSONS LEARNT ON THE IMPORTANCE OF RELATIONSHIPS</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>MOVING FORWARD WITH RELATIONSHIPS</strong></td>
<td>26</td>
</tr>
<tr>
<td><strong>THE CULTURE OF POLICING FRAUD</strong></td>
<td>27</td>
</tr>
<tr>
<td><strong>LESSONS LEARNT ON THE CURRENT STATUS OF ONLINE FRAUD</strong></td>
<td>28</td>
</tr>
<tr>
<td><strong>MOVING FORWARD TO IMPROVE GENERAL PERCEPTIONS AROUND ONLINE FRAUD</strong></td>
<td>29</td>
</tr>
</tbody>
</table>
Acknowledgements

The ability to travel overseas as a Churchill Fellow is a once in a lifetime opportunity which I am very blessed to have been given. Consequently, there are many people to whom I owe a great deal of gratitude.

Firstly, I want to thank the Winston Churchill Memorial Trust, particularly the Queensland selection panel, who believed in the merit of both my project and my ability to complete it. I am forever grateful for your decision to present with me with this award and I intend to make the most of what I have been given. I also wish to extend my utmost gratitude to the Griffith Rotary Club of New South Wales, who sponsored the Donald Mackay Fellowship for Organised Crime that I received. I hope to visit in the near future and present to you the fruits of your sponsorship.

Secondly, I wish to thank the Queensland Police Service for allowing me to undertake this trip as part of my work. In particular, I would like to thank my colleagues at the Community Safety and Crime Prevention Branch, who have put up with my incessant talk about fraud for some years now. I would also like to thank Detective Superintendent Brian Hay and colleagues at the Fraud and Corporate Crime Group for their continued support and encouragement of my research. It is easy to stay passionate about this area with someone such as Brian leading the way in Australia.

I would like to thank Professor Belinda Carpenter, School of Justice, Queensland University of Technology, and Dr Russell Smith, Principal Criminologist, Australian Institute of Criminology, for their very kind words expressed in my referee reports for the Churchill Trust. I have no doubt that your solid support of my abilities as a researcher greatly influenced my receipt of this award.

I am greatly appreciative to previous Churchill Fellow, Senior Sergeant Michael Mitchell, Queensland Police Service (QPS) for his initial encouragement to apply, and his subsequent assistance at every step of this process. I would not have been able to achieve this fellowship without him. I also would like to thank previous Churchill recipients Paul Friedman (QPS) and Superintendent Donna Sturgess (QPS) for giving me advice and sharing with me their own Churchill experiences.

I express my sincere gratitude to the many victims of fraud who I have spoken to over the past couple of years, particularly the frank manner in which they have opened up to me about their victimisation experiences. Many have gone through unimaginable hardships and struggles and it is their resolve and resilience that inspires me to keep working in this area.
I extend an immense amount of gratitude towards the many people I met throughout my overseas travels (the majority of whom are named in the following section). What became clearly apparent to me is the large number of people who are working tirelessly in this area, across all jurisdictions. I met so many incredible individuals throughout my eight weeks, many of whom are unwaveringly passionate about what they do and how they do it, and many of whom want to see an improvement in the services offered to victims of online fraud, as well as a reduction in the number of fraud victims overall. It is easy to draw inspiration from these people and I am thankful for the way in which everyone shared such great personal and professional insight and expertise with me. I have developed solid relationships with several individuals and look forward to staying in contact and working together in the future.

Lastly, I wish to thank my husband Lachlan, for his love and support of all my endeavours. I am eternally grateful for his love in letting me go.

Please Note
The views expressed in this report are solely those of the author and do not necessarily reflect those of the Queensland Police Service or the Winston Memorial Trust.

Any errors or omissions in content throughout this report are the sole responsibility of the author.
Executive Summary

Dr Cassandra Cross
A/Senior Policy Officer
Community Safety and Crime Prevention Branch
Queensland Police Service
GPO Box 1440, Brisbane QLD 4001
Phone: +61 7 3234 2193
Email: Cross.CassandraA@police.qld.gov.au

Project Description
Every day inboxes are being flooded with invitations to invest money in overseas schemes, notifications of overseas lottery wins and inheritances, as well as emails from banks and other institutions asking for customers to confirm information about their identity and account details. While these requests may seem outrageous, many believe the request to be true and respond, through the sending of money or personal details. This can have devastating consequences, financially, emotionally and physically. While enforcement action is important, greater success is likely to come in the area of prevention, which avoids victim losses in the first place. Considerable victim support is also required by victims who have suffered significant losses, in trying to get their lives back on track. This project examined fraud prevention strategies and support services for victims of online fraud across the United Kingdom, United States of America and Canada. While much work has already been undertaken in Queensland, there is considerable room for improvement and a great deal can be learnt from these overseas jurisdictions. There are several examples of innovative and effective responses, particularly in the area of victim support, that are highlighted throughout this report. It is advocated that Australia can continue to improve its position regarding the prevention and support of online fraud victims, by applying the knowledge and expertise learnt overseas to a local context.

Highlights
→ Meeting with staff at the National Fraud Authority, Serious Organised Crime Agency and the Metropolitan Police, all with considerable expertise around online fraud.
→ Visiting the ActionFraud call centre in Manchester, UK, and listening in on victim calls.
→ Meeting with staff across the many units within the US Department of Justice.
→ Visiting the Canadian Anti Fraud Centre (Analytical Unit, Call Centre and SeniorBusters program).
→ Discussions with D/C Mike Kelly, Toronto Police Service.

Recommendations
This report puts forward 21 recommendations across the following categories:
→ The Creation of a Fraud Strategy
→ The Creation of a Central Reporting Agency
→ The Development of Formal Relationships
→ The Revision and Development of Training Materials and Resources
→ The Identification of Crime Enablers
→ The Revision and Development of Online Fraud Prevention Materials
→ The Monitoring of Fraud Victims’ Wellbeing
→ The Promotion of Support Services Available
→ The Establishment of a Volunteer Support Program
→ The Rebranding of Online Fraud Victims

Dissemination of Findings
This report and its findings will be disseminated via the following methods:
→ Presentation of the findings to the Senior Executive of the Queensland Police Service
→ Distribution of the report to all fraud and crime prevention staff across Queensland
→ Distribution of the report to other law enforcement bodies across Australia
→ Distribution of the report to other government, industry and academic bodies through existing contacts and networks
→ Presentation of findings at upcoming conferences and seminars
Fellowship Program (13 October – 9 December 2011)

London, United Kingdom (17 October – 4 November 2011)
National Fraud Authority/ActionFraud
→ Mike Haley
→ Jamey Johnson
→ Collin Belcher
→ Sophia Agamemnonous
→ Steve Proffitt
London School of Economics
→ Professor Jennifer Brown
Victim Support, Birmingham
→ Amanda Redfern
Metropolitan Police (Operation Sterling)
→ Detective Sergeant Mark Ham
→ Detective Constable Soraya Hosking
→ Detective Constable Mike Hurst
Metropolitan Police (Police Central E-Crime Unit)
→ Detective Sergeant Frank Tutty
Serious Organised Crime Agency
→ Colin Woodcock
→ Alexander Hudson
→ Terry Griffiths
Serious Fraud Office
→ Nick Stroud
→ Tim Stillman
Victim Support, London
→ Lisa Collins
City of London Police
→ Detective Chief Superintendent Steve Head
→ Detective Inspector Peter Ratcliffe
→ Detective Inspector Steve Strickland
National Fraud Intelligence Bureau
→ Detective Superintendent Tony Crampton
→ Detective Chief Inspector Richard Waight
Office of Fair Trading
→ Simon Gunning
Women’s Fraud Network
→ Toni Sless
Brunel University
→ Professor Mary Gilhooly
Financial Services Authority
→ Steven Mayfield
Th!nk Jessica
→ Marilyn Baldwin
Portsmouth, United Kingdom (7 November – 11 November 2011)
Centre for Counter Fraud Studies, Institute of Criminal Justice Studies, University of Portsmouth
→ Dr Mark Button
→ Dr Alison Wakefield
→ Dr Aldert Vrij

Washington, District of Columbia, United States of America (14 November – 19 November 2011)
Fraud Section, United States Department of Justice
→ Jonathan Rusch
→ Barbara Corprew
→ Pat Donley
Internet Crime Complaint Centre, Federal Bureau of Investigation
→ Special Supervisory Agent Charles Pavelites
→ Special Supervisory Agent Donna Gregory
→ Special Supervisory Agent Herbert Stapleton
→ Stephanie Provow
→ Special Supervisory Agent William Blevins (Australian Attaché)
Victim Assistance Unit, Federal Bureau of Investigation
→ Kathryn Turman
Office of Victims of Crime, United States Department of Justice
→ Laura Ivkovich
→ Meg Morrow
Bureau of Justice Statistics, United States Department of Justice
→ Lynn Langton
United States Secret Service
→ Special Agent Christopher Riley
→ Jeffery Shelton RAIC, Sydney Resident Office, Australia
Federal Trade Commission
→ Laureen Kapin
→ Steven Toporoff
→ Carol Kando-Pineda
United States Postal Inspection Service
→ Lena Carroll
American Society of Criminology Annual Conference

New York City, New York, United States of America (21 November – 23 November 2011)
New York District Attorney’s Office
→ Assistant District Attorney Ehren Reynolds
**North Bay, Ontario, Canada (28 November – 30 November 2011)**

Canadian Anti Fraud Centre  
→ Staff Sergeant Paul Proulx  
→ Corporal Louis Robertson  
→ Detective Constable John Schultz  
→ Jessica Tough  
→ Daniel Williams

**Toronto, Ontario, Canada (1 December – 7 December 2011)**

Toronto Police  
→ Detective Constable Mike Kelly  
Ontario Provincial Police  
→ Detective Sergeant MaryAnn McInerney  
Royal Bank of Canada  
→ James Arndts  
→ Peter Warrack  
Homeland Security Investigations  
→ John Ward (Assistant Attaché Toronto)  
Ministry of Transport  
→ Laura Barkley-McKeeman  
Victim Services, Toronto Police

Thanks also to the many other people I met at these agencies and who were generous enough to talk with me but who are not listed.
Introduction

The Problem of Online Fraud

Online fraud is a growing and significant problem. Cybersecurity issues pose a risk to individuals, businesses and governments alike. Everybody seems to have their own personal story around online fraud, whether it relates to card skimming, fraudulent activity on a credit card, the accidental download of malware or viruses on a computer, an online purchase which never showed up, or the receipt of fraudulent emails asking for money, personal details or passwords. While there is a growing recognition of the magnitude posed to Australians from online fraud, the equivalent awareness of one’s own vulnerability to online fraud is not apparent. Instead, while the majority of society has heard about online fraud and may have experienced victimisation to a minor degree, the majority of society does not believe that they could become involved in anything more sinister.

Previous Research Examining Online Fraud Victimisation

The proliferation of internet usage has seen an increasing amount of people spend an increasing amount of time online. Almost all aspects of one’s life can be conducted online. While the ease and convenience of this is undeniable, the risk of fraudulent activity associated with this is also undeniable, but not fully understood. For the past three years, I have researched one aspect of online fraud, being seniors’ responses to fraudulent requests for money, personal details or passwords. In doing this, I interviewed 85 seniors across Queensland who had received fraudulent email requests. While many of these seniors recognised the fraudulent nature of the email, many did not and went on to respond and send money, personal details or passwords.

There are several key findings to arise from that research. The first concerns the characteristics of fraudulent emails. While most people assume that all fraudulent emails are easy to identify, in reality, their level of sophistication has increased to a point where they can appear to be both legitimate and plausible. The successful fraudulent emails also target a specific vulnerability of the victim at the time of receipt. Under normal circumstances, the victim is unlikely to respond, but for a variety of reasons, circumstances converge to a point where the email can appear to be genuine. The second significant finding of the research is the development of a relationship between the victim and the offender. It does not have to be a romantic relationship, however once trust and rapport is established between the victim and the offender, it is very difficult for third parties such as family, friends and law enforcement, to break that relationship. The research also identified a number of key challenges around the prevention of fraud, which include a refusal to listen to third parties; an underestimation of the value of personal data; a belief that fraud losses are only financial; and negative stereotypes which exist about online fraud.

The final report containing an in depth analysis of these research findings is forthcoming.
victims. This research was clearly able to identify many of the problems which manifest themselves regarding online fraud victimisation. However, the challenge arising from this research was the ability to put forward suggestions on how to overcome these and other problems resulting from online fraud.

The research was unmistakeable in detailing the very real human cost to online fraud victimisation. It is a cost that extends beyond just the pure financial losses experienced by victims, but also incorporates physical effects through the general deterioration of one’s health; emotional and psychological effects manifested largely through depression; relationship breakdown and isolation from family and friends; and in worst case scenarios, suicide. It is a dangerous myth to believe that victims of fraud only lose money. In many cases, they not only lose money, but they lose their feeling of self worth, they lose confidence in themselves, they lose trust and confidence in others, and they lose the future they had planned. What makes it even harder, is that a large number of victims suffer alone in silence, without the confidence or perceived ability to share their burdens with those around them. There is such a stigma and sense of shame and embarrassment associated with online fraud victimisation, that the thought of coming forward and sharing the experience is too much to conceive.

As an outsider, it is undoubtedly difficult to understand how a person can become involved in online fraud. To an external third party (such as family member, friend or even law enforcement) the fraudulent nature of requests and situations is obvious, however for the individual involved, the situation seems both plausible and legitimate. The skills of the offenders are very often underestimated. Offenders are savvy and highly skilled social engineers who are experts in identifying a person’s vulnerability and targeting approaches to exploit that weakness. Particularly once the offender has established a relationship with the victim, it becomes very difficult for the victim to be objective to what is being presented to them and see the fraudulent nature of the situation until it is too late.

All victims successfully negotiate and discern hundreds if not thousands of fraudulent requests across their lifetime, however it takes just one email which hits on a certain vulnerability in the right way at the right time, for them to become involved. No victim ever intends to become a victim, and can easily identify the fraudulent nature of other attempts and solicitations. Nevertheless, for a variety of reasons they were simply unable to identify the same of their situation. The cost resulting from that one decision, for many, can be life changing with long lasting repercussions.

The Current Situation for Queensland Victims of Fraud

Within Queensland, victims of non-violent crime are not afforded the same opportunities as victims of violent crime, when it comes to accessing support or restitution. Under the Victims of Crime Assistance Act (2009), while a victim is defined as someone who has suffered harm as a result of a crime committed against them (section 5), in order to access any subsequent financial assistance, the
definition narrows to only include victims of violence (section 21). The legislation does set out fundamental principles on fair and dignified treatment of victims (section 8-16), which includes all victims as per the initial definition, however the majority of these will not apply to victims of online fraud, as they deal predominantly with their interaction with the criminal justice system.

By the very nature and characteristics of online fraud, victims cannot access any of the current victim initiatives in place within the criminal justice system. The vast majority of offenders are based overseas and prosecution of these offences is both complex and problematic. Although successful prosecutions of online fraud have been achieved in other jurisdictions, the likelihood of this occurring for every offence is unrealistic. Therefore, most victims of online fraud will not see the offender arrested, will not have the ability to participate in any form of court proceedings, will not have the ability to give evidence, will not have the ability to provide a victim impact statement, and will not have the opportunity to participate in any victim-offender mediation or restorative justice practices (which are all contained within section 8-16 of the legislation). This is a constant source of frustration for online fraud victims, who despite being victimised have no practical recourse available to them. This does nothing to encourage the reporting of online fraud victimisation, or to alleviate any of the helplessness that victims feel once they realise what has occurred.

An overview of the current project

This project focused on two key aspects of online fraud, being its prevention and the support services available to victims. While enforcement action is important and cannot be ignored, the reality is that for the majority of online fraud cases, enforcement action is complex, lengthy and both time and resource intensive for little benefit in the long term. It is advocated that greater benefits will arise from focusing heavily on prevention efforts to avoid the losses incurred by victims in the first place. While Australia, and Queensland more specifically, have put in a great deal of time and effort to prevention efforts in recent times, the aim was to examine what other jurisdictions are doing in this area, and whether there are lessons which can be learnt and adopted here.

In contrast, the area of support services for victims of online fraud is one that has been largely ignored, as a consequence of the spread and pervasiveness of online fraud victimisation not being recognised. It is difficult to assess the needs of online fraud victims who in many circumstances do not know they are victims or online fraud, or who in other situations, do not have the confidence to come forward and report the crimes. Recognising this gap in victim support is a slow process, however small steps are being made. In 2010, the QPS established a victim support group solely for fraud victims and this continues today. The group has served as an important mechanism for victims to meet others in their own situations and to remove the isolation that may have been felt prior to the group being formed. In addition, it has taken away the stigma and shame associated with this type of victimisation for those that attend and has allowed many in the group to talk about
their experiences, support each other, and collectively raise awareness of online fraud victimisation. However, while this is an important and significant step, there are still many gaps and opportunities around the provision of support to victims of online fraud. As with the prevention aspect, the aim was to determine what other jurisdictions were doing to support victims of online fraud, and how that knowledge and practice could be translated into an Australian and Queensland context.

Prior to going overseas, I wrote a discussion paper to guide my visits with individuals and agencies. The paper outlined twenty topics broadly grouped into the following categories: online fraud victims; preventing online fraud; reporting online fraud; victim support; enforcement; and information sources regarding online fraud (see appendix 1). This paper was designed as a mechanism to generate discussion, as well as provide those I was meeting with a basis of my understanding and current knowledge in the area. While I was not expecting any one individual or agency to be able to answer questions under the twenty topics, I am indebted to the many individuals who did do this, and spoke to the entirety of my discussion paper. I am very grateful for the time and effort that many people put into preparing for my meeting with them, and this certainly had a very positive effect on the quality of discussions held.

In preparing to visit each of the agencies I contacted, I was generally aware of the great work that many were doing. However, despite knowing this, I did underestimate both the quality and the overall content of what I would learn from overseas jurisdictions. I have been somewhat overwhelmed with information that is both valuable in its contribution to the field, as well as innovative in its response to the problem investigated. Even now, I don’t feel that I have been able to fully process everything that I learnt over the eight week period. This report presents the most pertinent of the key lessons learnt regarding the prevention and support of online fraud victims.

Lastly, it is important to note that this report will only focus on the prevention and support of online fraud victims. While many individuals shared great expertise across the area of enforcement, my knowledge on fraud investigations is limited. Therefore, this report will stick to both prevention and victim support aspects, where I believe I can make the most effective contribution.
The Fellowship Journey

As part of the fellowship, I visited agencies in London, Washington DC, New York, North Bay and Toronto. These agencies encompass three jurisdictions which shared both similarities and differences in their approaches to online fraud prevention and victims support. Prior to detailing the main findings of the trip, the following section provides a brief summary of the agencies I visited across the United Kingdom, United States of America and Canada to give an overall context of these agencies regarding their work on fraud.

United Kingdom

Within the UK, there are a large number of agencies whose work relates to fraud. This includes a number of law enforcement agencies, but there are a number of other government bodies with either regulatory or legislative powers regarding fraud. Within the UK, I was able to gain insight into many of these organisations.

The National Fraud Authority (NFA) is one of the main agencies in the UK for fraud. It seeks to coordinate existing counter fraud work across public, private and voluntary sectors. In addition, it leads the implementation of the UK’s strategic plan Fighting Fraud Together, which sets out three objectives, encompassing awareness, prevention and enforcement. During my time in London, it shifted from being located within the Attorney General’s Department to the Home Office. The NFA is also responsible for ActionFraud, which is the UK’s national reporting centre for fraud. ActionFraud is equipped to be able to take reports from all types of fraud victims on behalf of the police, and issues crime reference numbers. The ActionFraud call centre is located in Manchester and is increasing the number of staff to keep up with demand for service. ActionFraud is also a point of referral to support services for victims who require it.

There are a number of law enforcement agencies with an interest in fraud. The City of London Police (COLP) is designated as the national lead force for fraud. While the City of London covers only one square mile in the centre of London, it is the world’s leading business and financial centre, with over 450 international banks, as well as insurance companies and other multi-national company headquarters. Given the fact that this is one of the major financial hubs in the world, the COLP have developed specialist skills in economic crime and are charged with investigating complex fraud cases. The COLP also hosts the National Fraud Intelligence Bureau (NFIB) which is the national repository for all fraud reports and intelligence across the UK. The NFIB collate data received from ActionFraud and other departments, in an attempt to put together an overall picture of fraud offending in the UK. While many individual fraud offences will not make the threshold for investigation by police, the NFIB have the ability to pull together larger volumes of related offences, which can increase the likelihood of a case being investigated by local police. They attempt to piece together the bigger picture of fraud, which individual agencies and victims are not able to achieve in isolation.
The Metropolitan Police established Operation Sterling in 2005, to focus exclusively on economic crime. They focus heavily on both disruption and prevention of offences, with a large part of their current work centred on fraudulent letters received in the mail. Their work aims to complement that of COLP, and works in conjunction with the strategic goals outlined by the NFA. The Serious Organised Crime Agency (SOCA) is another important enforcement agency, with their focus on serious organised crime within the UK. This includes drugs, people smuggling, human trafficking, gun crime as well as fraud, computer crime and money laundering. With a large focus on mass marketing fraud, during my visit to London, officers were involved in assisting African authorities to prosecute a case of romance fraud which involved UK victims.

As well as law enforcement agencies, there are a number of other agencies such as the Serious Fraud Office, Financial Services Authority, Office of Fair Trading, Trading Standards and CIFAS who have capacity to deal with various aspects of fraud. In addition, there are several non-government bodies working in the area of prevention, with the establishment of a Women’s Fraud Network providing valuable opportunities for women working in this area. Th!nk Jessica is another organisation which was established to raise awareness of fraud, and is passionately driven by the tireless work of Marilyn Baldwin, who’s deceased mother Jessica, was a chronic victim of fraudulent mail. In conjunction with enforcement agencies such as the Metropolitan Police, Th!nk Jessica seeks to play an advocacy role in promoting the reality of fraud victimisation and the devastating consequences it can have on victims and their families.

There are also agencies in the UK which provide support to victims of fraud. Victim Support is a national charitable organisation which provides support to victims across all crime categories. Of particular interest, is the relationship developed between Victim Support and ActionFraud. All victims who call ActionFraud are asked about the impact of their crime, and if they desire further assistance or support, a referral is made to Victim Support for follow up. Victim Support’s call centre is located in Birmingham and all consenting fraud victims receive a phone call from trained staff at this centre to determine their needs. If further support is required, then victims are referred out to one of the many Victim Support offices across the country.

Overall, the UK displays many positive attributes around the prevention and support of online fraud victimisation. As will become apparent throughout the main body of this report, there are many lessons which can be learnt from UK counterparts which could be applied Australian context.

**United States of America**

The United States is in a similar position to the UK in terms of the number of agencies who contribute to the prevention of fraud. While there are a plethora of
police jurisdictions across the country who are likely to deal with fraud in any number of circumstances, there are a number of federal agencies who deal with fraud on a higher level in terms of enforcement, prevention, victim support and overall strategic direction. To further highlight the national focus on fraud, in 2009, President Barack Obama established the Financial Fraud Enforcement Task Force. This task force is a coalition of 20 federal agencies, 94 US Attorney’s Offices and state and local partners charged with targeting financial fraud in the US, which includes various types of online fraud. Along a similar vein, identity theft is the fastest growing type of crime type in the US, and in addition, is now the most prevalent type of crime committed. In combination, these two facts seek to highlight the prominence that fraud currently has within America.

The United States Department of Justice (USDOJ) has a number of key areas which interact with fraud. In particular, there is the Criminal Division which houses the Fraud Division, who plays a lead role in the investigation and prosecution of economic crime as well as provide policy advice and a leadership role around legislation, crime prevention and public education matters. This office deals with a variety of fraud including identity related offences and mass marketing fraud offences. In particular, they have strong experience in dealing with complex fraud cases, comprising large volumes of victims.

Within the USDOJ, there is also the Office of Justice Programs. This section comprises the Bureau of Justice Assistance, Bureau of Justice Statistics and most importantly, the Office for Victims of Crime. Each of these areas contributes in some capacity to the overall prevention and support of fraud victims. Of particular interest at the moment is the initiative called Vision21. This project aims to design a philosophical and strategic framework around responses to crime. Through extensive stakeholder engagement with agencies and individuals in the crime victim field, the final document, due for release in early 2012, will provide an analysis of the current state of affairs, solutions for the future and a blueprint for implementing solutions.

Another important arm of the USDOJ is the Federal Bureau of Investigation (FBI). There are two areas of relevance within the FBI, the first being the Internet Crime Complaint Centre (IC3) (which is a partnership with the National White Collar Crime Centre) (NW3C) and the second being the Office for Victim Assistance. The IC3 acts as the central reporting portal for the US regarding internet crime complaints. As a result, it is able to analyse all internet crime complaints and refer these to enforcement agencies for investigation where relevant as well as identify current trends and disseminate prevention and awareness materials. In contrast, the Office for Victim Assistance focuses on victims of crimes being investigated by the FBI. They are responsible for ensuring that the rights of victims are maintained and that support services are available to victims as needed. The Victim Assistance Office is also responsible for training and information to assist the FBI’s field officers in their interactions with victims.

In addition to the USDOJ, the Federal Trade Commission (FTC) plays a significant role in the education and awareness of consumers on fraud. In particular, the FTC’s
Bureau of Consumer Protection works to prevent fraud, deception and unfair business practices. The work of the bureau focuses the creation of resources and campaigns on topical issues that are affecting consumers. For example, the most in depth campaign recently undertaken was around identity theft, given its prominence across the country.

The United States Secret Service (USSS) is a federal law enforcement agency, which forms part of the US Department of Homeland Security. The USSS are tasked with both protective services of national and visiting foreign leaders as well as criminal investigations. As part of this second mandate, the USSS are responsible for maintaining the integrity of the US financial systems. Consequently, they have a strong focus on counterfeit currency and financial crimes which includes identity crimes, computer fraud, credit card fraud, money laundering and advance fee fraud. While mainly focused on enforcement and disruption activity, the USSS promotes prevention tips and advice to the general public on how best to protect themselves from fraud.

The United States Postal Inspection Service (USPIS) is another enforcement body who plays an important role in the disruption of fraud, through the interception of fraudulent mail and packages. The USPIS is the enforcement arm of the United States Postal Service and seeks to investigate incidents where the postal system is used to commit criminal acts such as fraud. The USPIS work in conjunction with many other agencies both within the US and abroad, in seeking to investigate, prosecute and prevent fraudulent activity.

Overall, the US has a very strong focus on the legislative rights of victims, as detailed in the Victims Rights and Restitution Act and the Crime Victim’s Rights Act. The provisions of these acts in relation to victims were emphasised throughout discussions across the majority of the agencies visited. It is important to note that each of the agencies I was able to visit has federal jurisdiction, and as a result, this report does not encompass the work which is undoubtedly undertaken in relation to fraud at state and county levels. It is assumed that there are many more agencies working to prevent fraud who are based throughout the country as opposed to simply Washington DC, however I was only able to observe efforts at a higher level.

**Canada**

Canada has some of the most innovative responses to fraud observed across my trip. As with both the UK and the US, there are a wide variety of agencies working to combat fraud.

The establishment of the Canadian Anti Fraud Centre (CAFC) has since its establishment in 1993 as “Project Phonebusters” within the Ontario Provincial Police (OPP). Today, the CAFC comprises three agencies, the Royal Canadian Mounted Police (RCMP), the OPP and the Competition Bureau Canada. The CAFC has two primary functions, the first being a call centre for victims of fraud across Canada and the second being Criminal Intelligence and Analytical Unit, which analyses all
complaints received by the call centre. Similar to the NFIB and the IC3, this unit is able to collate data and prepare investigative briefs for investigation where necessary. The unit is also able to document the current trends and issue preventative information, advice and alerts to other law enforcement, industry and the general public.

As evidenced by their involvement with the CAFC, the RCMP are an enforcement body who seek to prevent fraud through disruption and enforcement activities. The RCMP is a federal policing agency, but are unique in that they also provide provincial and municipal policing services. They service Canada as a whole on a federal level, as well as having contracts to serve three territories, eight provinces, over 190 municipalities, 1,984 indigenous communities and three international airports. In addition to the RCMP, the OPP also contributes to the policing of fraud in Ontario, specifically through the work of the Anti Rackets Branch, which focuses on fraud related matters. At a more local level, the Toronto Police Service (TPS) operate across the city of Toronto. In terms of fraud, there is a Financial Crimes Unit which focuses on the various types of fraud, including online victimisation. Despite being a small unit, they have had success in investigating complex, large scale fraud cases.

Throughout Canada, many of the provinces have strategic partnerships or alliances amongst local agencies to combat fraud at a local level. For example, the Toronto Strategic Partnership is a law enforcement partnership that was established in 2000 to target fraud and deceptive practices. Each partnership comprises agencies that are relevant to the situation across the particular province. The Toronto Strategic Partnership includes organisations such as the TPS, Ontario Ministry of Government Services, the Competition Bureau Canada, the USPIS, the US FTC, the OPP, the RCMP and the United Kingdom’s Office of Fair Trading. The partnership allows partner agencies to work more effectively together and to share information more freely than before. The TPS have a central role in this partnership, as well as contributing their own members, staff from other agencies work on assignment out of the TPS. The existence of these formal partnerships amongst key agencies at a local level, highlight both the need and benefits that a collaborative model can achieve.

The Canadian response to victims of fraud is comprehensive. The CAFC runs a program called SeniorBusters, which aims to prevent seniors who have been victims of fraud or are vulnerable to online fraud, from future victimisation. This program uses a peer support model, of seniors working with seniors, to promote a message of prevention as well as support victims where needed. The program is predominantly staffed by over 50 active volunteers, who work out of the CAFC in North Bay, Ontario. In addition, victims of all types of crime and circumstance (including fraud) have access to the support services of Victims Services Toronto. This is the only agency in Toronto who is able to provide immediate support and counselling of victims, either by phone or in person. They are a 24 hour service and use a combination of trained counsellors and volunteers to provide this service to almost 20,000 people each year.

Overall, Canada is in a strong position to deal with the enforcement and prevention of fraud as well as supporting its victims. The agencies and services outlined are only
a few examples of the innovative responses to fraud which has emerged from within Canada.

**Summary – The Global Context of Online Fraud**

As is evident from above, my fellowship enabled me to meet with individuals across a wide variety of agencies in each country. What became evident from the beginning is that the similarities in problems regarding online fraud are universal. While the contexts of many other types of crime may shift significantly across jurisdictions, online fraud appears to remain quite static. For example, discussions held at the University of Portsmouth in the UK, on research they had undertaken on victims of online fraud, mirror the research which I have been conducting here in Queensland. At times in the conversation, I felt as if I was present at one of my own seminars, given that the content being presented to me was identical to what I present to others, despite the fact that the victims are half a world apart. Similarly, after giving a presentation to the CAFC, the observation was made around the experiences of victims and law enforcement in Canada was akin to those I had detailed from Queensland. It is powerful to realise that there is a degree of solidarity across victimisation in the fraud sector, no matter what jurisdiction or time zone it concerns.

The benefits of this observation relate to the core premise of this report, being the prevention and support of online fraud victims. Given that the characteristics and the nature of victimisation experiences are so similar across the four countries, it is easy to see how each country’s response to online fraud can contribute to an improvement in prevention and support services to online fraud victims in Australia and Queensland. Each of the three jurisdictions that I visited has considerable expertise and knowledge in how they currently manage online fraud, albeit in different formats. This trip highlighted the substantial amount of quality work which is being undertaken on a global scale to prevent online fraud and support those who have become victims. While Queensland is currently in a favourable position regarding its efforts in this area, as will become apparent through the remainder of this report, there are considerable improvements which can be done in the ongoing battle against online fraud.
Main Findings

The purpose of my fellowship was to explore other jurisdictional responses around the prevention of online fraud and the provision of support services to victims of online fraud. As is evident in the previous section, there are great examples of work being done across many agencies in several countries.

The following section provides a thematic approach to the research findings. Again, I am grateful to each agency for sharing their knowledge and experiences with me in a very open and frank manner. It would be impossible to detail each of the topics discussed across my fellowship, therefore the remainder of this report presents a selection of the most pertinent topics. Each theme is presented in the following manner: firstly, a summary of the issue is presented, together with evidence from one or more jurisdictions visited; secondly the lesson/s which can be learnt from the example/s are articulated, before the last section puts forward suggested recommendations which would enable Queensland to improve its current situation.

A Unified Approach to Fraud Prevention

It is readily apparent from the number of agencies that I visited overseas, that there are a lot of people and organisations working in the “fraud space”. The UK in particular, has a large number of agencies who all contribute in one way or another, to the prevention of fraud. The ambit of each agency differs, according to their main function and the legislation which governs them, however in their own way, they all contribute to the overall prevention of fraud. One agency within the UK remarked that given the number of agencies, it was difficult for individual organisations to carve out their own niche in the market. While the large number of agencies working in this area can be seen as a positive in terms of recognising fraud as a significant crime problem, it is understandably hard to create or sustain a unified approach. There were several instances where during my visit I had the ability to tell one agency what another agency in their jurisdiction was doing on a specific topic.

Individual organisations each have their own business plans or strategic visions, which guide their work. There are also agencies which have a national focus in their work, and are seen to lead the nation’s activities regarding fraud. For example, the NFA in the UK and the CAFC in Canada, are both agencies which have a national focus on fraud prevention activities. There are strategic plans which guide the actions of these agencies (for example Fighting Fraud Together in the UK) and provide a clear template about what needs to be done in the future, and how this should be best achieved. Within the US, the establishment of the Financial Fraud Enforcement Taskforce provides a clear direction for fraud work in their jurisdiction.

Lessons Learnt on the Benefits of having a Strategic Direction

There is an obvious advantage in having an overarching vision which sets out the vision that all should be striving for, as well as the means in which those involved can
contribute to achieving it. It puts all agencies on the same page and provides clear guidance and direction about what activities should be undertaken and how this should occur. It also should remove some of the ambiguity around the roles and responsibilities of individual agencies and how their actions fit within the big picture. The other main advantage of a strategic approach should be a higher level of consistency with key messages delivered to the public around fraud as well as an integrated approach to services and related programs administered to the public.

While theoretically, a strategic direction appears as a simple means to provide a unified approach to fraud across any jurisdictional level, in practice, it is acknowledged that difficulties exist. As witnessed in the UK, while they have a national lead agency on fraud as well as a strong strategic vision, the sheer number and diversity of agencies working in the area, does lead to a disparity in the approaches and the messages promoted. However, the existence of this in itself is something which should be seen as a positive example in the area.

**Moving Forward on the Development of a Strategy**

Within Queensland (and Australia more broadly) there is no current strategic direction concerning the prevention of fraud, online or otherwise. While the federal government has released the CyberSecurity Strategy, documents such as this one focus more heavily on the technical aspect of fraud. While prevention is clearly apparent as a priority, further details about the how this should be achieved are not evident. Similar to other jurisdictions, Australia also has a number of different agencies working in the fraud space. In addition to state and federal law enforcement bodies, there are other government agencies such as the Australian Competition and Consumer Commission (ACCC), who have fraud prevention within their scope of work.

Within Queensland, given that the QPS has the lead agency status around crime prevention as a whole, it seems appropriate that the development of a fraud prevention strategy could be achieved. Having a strongly articulated fraud prevention plan would allow the setting of clear and realistic benchmarks that contributing organisations would be accountable to. In addition, it would give guidance for future actions in this area and pull together the various stakeholders, (such as law enforcement, government and other bodies) to deliver consistent messages to the public around fraud issues. It would also provide a means which is likely to improve current services and programs available to victims of fraud, online or otherwise.

The impact and consequences of online fraud are unlikely to decrease in the future, therefore it is imperative that proactive steps are taken to ensure the readiness of agencies such as the QPS, to be able to effectively target fraud prevention messages to the public, as well as support victims of this type of crime. The development of a strategic plan (and supporting action plan) is the first step in facilitating this to occur. It also provides an opportunity to assess future developments regarding fraud and what will be required in its prevention, and can attempt to address these at an early
stage. There is a lot which can be drawn from overseas examples to aid in this process.

Recommendation
1) That a fraud prevention 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 in Queensland.
A Central Reporting Agency

One of the biggest problems encountered for victims of online fraud is confusion on who is the appropriate reporting authority. Some will report an incident to their banks, others will try and report to police, while others may report to any number of other agencies such as Office of Fair Trading (or equivalent). For many victims, it appears too difficult and subsequently, no report is ever made. For others, they may experience a merry go round of responses, being referred from one agency to another, and sometimes back again. In essence, the majority of victims of online fraud face negative experiences when trying to report their victimisation and this is a contributing factor to the extremely low rates of reporting for this type of crime.

In order to combat the confusion on who best to report to, the UK, US and Canada have all implemented central reporting agencies for online fraud. In the UK, ActionFraud is the central reporting body for all complaints of fraud, and has the ability to take a fraud report on behalf of the police. In the US, the IC3 serve as a central reporting body for all complaints of computer crime, including fraud. This is similar to the CAFC, who can take reports of fraud victimisation across Canada.

Lessons Learnt on the Benefits of One Portal

There are a number of obvious advantages in having a single point of contact for individuals wishing to report online fraud. First, it gives victims certainty on who they should contact and provides confidence that their report will be taken by someone who understands what they have experienced. This removes the frustration experienced by many people in trying to find the appropriate agency to report their victimisation to. Theoretically, it should also provide a more effective method to make a complaint, through an increased understanding by the reporting agency on the characteristics and circumstances surrounding online fraud, and a more effective reporting process which encapsulates the information required by police or other enforcement agencies.

The existence of a central reporting agency also improves the ability data and intelligence which can be collected regarding online fraud. In making the process easier for victims, it is anticipated that a greater number of victims will report, when previously they may not have. Fraud is one of the least reported crime categories, so any means to improve the reporting of this offence is positive. In addition, as witnessed in each of the three central reporting agencies mentioned above, there is an increased capacity to analyse the complaint data and identify trends, as well as package reports into a brief which can be tasked for investigation. A central data repository enables a greater degree of information and intelligence to be examined and allows a more complete picture of offending to be constructed. Through the NFIB, IC3 and CAFC, data is able to be collated at a more strategic level than would occur of reports were being received by multiple, disconnected agencies. This has benefits in an overall knowledge of what is occurring in the field as well as an increased ability to be able to conduct meaningful analyses on the intelligence available.
Despite the benefits of having a central reporting agency, it is acknowledged that there are practical difficulties in establishing and operating a single repository for fraud complaints. For example, while ActionFraud in the UK is the central reporting agency for all fraud complaints and can take reports on behalf of the police, victims still report to many of the other agencies and are unaware of the existence of ActionFraud. In addition, some agencies were unaware of ActionFraud and that they were able to take complaints on behalf of the police. Therefore, while theoretically, ActionFraud should serve to improve the reporting of fraud complaints, in practice, it is not that easy. Similar circumstances exist in the US and Canada, in that while they have a central reporting body for fraud complaints, it does not seem to be as simple as having one repository of data. Continued efforts need to be undertaken to promote these bodies as a reporting domain across government and industry as well as the general public.

Moving Forward to a Single Reporting Agency

The establishment of central reporting bodies for fraud across the UK, US and Canada are very positive steps in seeking to increase the reporting of victimisation. This should also increase knowledge and intelligence on the prevalence of online fraud and inform current enforcement and prevention strategies. From this perspective as well, a greater understanding of the problem would allow an improved analysis to be undertaken of the data with a view to producing a better product for other law enforcement, industry and the community.

Currently within Queensland, and Australia more broadly, there is no one reporting body for occurrences of online fraud. Instead, as previously detailed, individuals may report it to banks, police, other government or industry bodies, or in the majority of cases, not report it at all. The establishment of a central reporting agency should have positive effects of victim reporting, as well as improve the availability of data and intelligence for law enforcement and other bodies. The formation of analytical units within these central reporting agencies also enables all reports to be examined for relevant intelligence and for briefs to be put together for possible investigations. While by itself, a single fraud offence may not be able to be investigated, in combination with other offences, an investigation may be more viable. The establishment of a central reporting agency facilitates these types of activities.

Recommendations
2) That a central reporting body is established to act as a single contact point for victims of fraud, and enable a single repository for all complaint data.
3) That all until such time as a central fraud reporting body can be established, greater work is done to educate all possible fraud contact points on the possible reporting of fraud offences.
**The Importance of Relationships**

The value of good working relationships amongst agencies was one of the most prominent observations across each of the jurisdictions. There is a clear recognition that single agencies acting alone are unlikely to be able to effectively address fraud prevention. The ability of agencies to collaborate, both formally and informally, with each other, is one of the core elements that underpins the work that is being done in the area.

Within the UK, there is a formal partnership around mass marketing fraud, which involves a number of different agencies, each with a defined role in the collaboration. For example, SOCA provides knowledge and intelligence on mass marketing fraud; the Metropolitan Police, through Operation Sterling, provide support in the prevention aspect; the Office of Fair Trading focuses on public awareness; COLP conduct enforcement; and the NFA provide an advocacy role around the broader issues. In the United States, the IC3 is a partnership between the Federal Bureau of Investigation and the NW3C to capture national data on internet crime, including fraud. A similar situation is also evident in Canada, where there several examples of strategic partnerships which focus on fraud. Each of the provinces has a strategic partnership which consists of a variety of agencies relevant to the needs of that province. For example, the Toronto Strategic Partnership comprises Canadian, American and British agencies, working together to combat fraud. In addition, the CAFC comprises three agencies (OPP, RCMP and Competition Bureau Canada) who work together to combat fraud.

At a higher level, the existence of the International Mass Marketing Fraud Working Group (IMMFWG), demonstrates how different countries can come together and work towards a unified goal relating to fraud. While the IMMFWG encompasses enforcement, disruption and prevention activities, the importance of working together, and the relationships that have been established, are crucial to any future global initiatives around the prevention of fraud. This group brings together a variety of law enforcement, regulatory and consumer protection agencies from Australia, Belgium, Canada, the Netherlands, Nigeria, the United Kingdom and the United States as well as Europol. Several agencies spoke of their involvement with this group and the benefits they believed arose from having a group of this nature working together across jurisdictions to prevent mass marketing fraud.

**Lessons Learnt on the Importance of Relationships**

No one agency had the ability to singlehandedly deliver all services around the enforcement, prevention or support of victims regarding online fraud. Offenders will explicitly use multiple countries to commit their crimes, knowing that this increases the difficulty of any one enforcement body to investigate and prosecute. Therefore to be successful in gaining success, those working in online fraud are required to build relationships which cross geographical borders and legal jurisdictions. The importance of relationships between individuals and agencies was apparent in each jurisdiction. The strength of some of these relationships was evident in the positive
work and successes that several agencies had experienced. While many of the relationships are largely informal and personality driven between likeminded individuals, the importance of formally established partnerships was equally as important in overall success. By being involved in such strategic partnerships and collaborations, individual agencies are able to achieve more than they would by themselves. The ability to share intelligence, knowledge, staff and other resources has distinct benefits in the quality of outcomes that are able to be produced.

Moving Forward with Relationships

The QPS already has strong relationships established with a large number of agencies, reflected in their membership of the IMMFWG mentioned above and the Australian Consumer Fraud Taskforce, chaired by the Australian Competition and Consumer Commission as examples. Undoubtedly there are other formal and informal partnerships which have been developed between the QPS and a variety of other agencies.

However, the development of a formalised alliance with the QPS and identified stakeholders, specifically in the areas of prevention and victim support services, would be a positive step forward. Much is yet to be achieved in these areas, and there is wide scope for agencies to work together to improve an overall response to the fields of prevention and victim support. Particularly if any new work is to be undertaken, the establishment of partnerships could serve as a catalyst for possibilities to be undertaken which alone, individual agencies would not be able to pursue. There are also benefits to formalising these collaborations, in terms of setting out clear roles and expectations of each contributing party, offering directions on how agencies can contribute to achieving the overall goal of the partnership as well as providing accountability to all those involved.

Recommendation

4) That formalised partnerships are developed with identified key stakeholders to specifically address the prevention and victim support aspects of online fraud.
The Culture of Policing Fraud

It was universally acknowledged that in order to make any future impact in the area of online fraud, a greater political will must be present. If fraud does not rate as a priority on both political and policing agendas, then the resources required to combat the problem are unlikely to be allocated as needed. There were significant differences in perceptions of individuals around the current level of political will towards fraud. In the UK, despite a significant fiscal tightening of all government budgets, ActionFraud was the only department to receive an increased allocation of funding in upcoming years. Also, within the US, given that identity theft is now the most prevalent crime in the country, the establishment of the Fraud Taskforce certainly puts fraud upfront on the political agenda. However, there was still an underlying perception by many, that fraud does not receive the same recognition as other types of crime, particularly in terms of policing resources and budget allocations. Instead, there was a perception that other types of crime (generally violent crime) are still seen to be more important and deserving of police time and resources, and this belief was seen to permeate many enforcement agencies and personnel.

There are several identifiable factors which contribute to this perception, which are evident both overseas and Australia. First, there is a misunderstanding about fraud victimisation. There are strong stereotypes around fraud victimisation which posits victims as greedy, uneducated, lower socioeconomic in status and generally deserving of their victimisation. There is also a belief that victims only lose money, which underestimates the true reality of victimisation which extends to deterioration of health, emotional and psychological problems (such as depression) and relationship breakdown. There is such a strong stigma associated with fraud victimisation, that it is hard for external parties to understand how victims became involved in the first place, and secondly, how they came to lose money. Fraud victims are certainly not viewed as “ideal” victims who have the ability to garner society’s empathy and concern.

Second, it is difficult to deal with a problem which is not reported. Overall, fraud victimisation has one of the lowest reporting rates across all crime categories. Given the shame and embarrassment associated with becoming a victim of online fraud, very few individuals come forward and report their victimisation to police or other agencies. In addition, the majority of online fraud victims do not even know that they are involved in fraudulent transactions, as they believe in the legitimacy of their situation. In these circumstances, victims will hardly come forward to report or to seek assistance if they don’t believe there is a problem in the first place. It is therefore very hard to allocate resources to a problem which is fundamentally hidden from the eyes of society.

Third, there is a lack of understanding from police agencies about the complexities of online fraud. In most cases, if a victim does report this type of offence, it is difficult for the reporting officer to take any action and many do not know how to deal with the complexity of the overall situation. Online fraud victimisation does not fit the
box of what police generally deal with. If a person is robbed on the street, then there a concrete location of where the offence occurred, there may be witnesses, there is likely to be a suspect and police can investigate on this basis. However, with online fraud, the victim is likely to have sent money to more than one overseas jurisdiction through a wire transfer process, there is no physical location where the offence took place, there are likely to be emails from a variety of email addresses which are unlikely to be the true identity of an individual, and the police officer probably does not have the ability to investigate the offence or have the authority to investigate in another jurisdiction. There is also a misunderstanding by many officers that fraud is purely a civil matter, and police may simply refer victims to a lawyer. Unless police officers are specifically trained on the complexities and characteristics of online fraud, then it is difficult for them to provide victims with the assistance and information they require.

In addition, a number of enforcement personnel argued that there is a lack of understanding about the role that fraud plays in the wider sphere of criminal activity. There was a belief that the prevalence and importance of fraud was overlooked for other types of crime (such as drug offences) and this was to the detriment of fraud. These individuals argued that fraud was behind many criminal enterprises and it was sometimes easier to follow the fraud trail than it was to monitor other crimes the offenders may be involved in. From their experience, many offenders were not as stringent in covering up their tracks when it came to fraud, compared to other types of crime. This was seen as a weakness which could be better exploited by enforcement agencies.

Lessons Learnt on the Current Status of Online Fraud

Overall, the factors identified above combine to undermine the importance ascribed to online fraud and hinder the political will needed across several levels, to be able to secure the required resources and funding to combat this crime problem. It also impacts on the priority level given to fraud. If fraud is not seen as a priority at the senior levels of any organisation, it is unlikely that significant progress forward can be made at the lower levels. There are certainly pockets within many organisations who have an in depth understanding of the gravity and nature of online fraud offences and who work tirelessly in this area, however in many instances these units and individuals face many hurdles to be able to continue in this area. Certainly, with an increased acknowledgement of their work and a corresponding increase in allocated resources and budgets, greater progress could be made. The challenge is to package and promote online fraud in a way which highlights the gravity of the current situation and future predictions in terms of fraud losses and their impact, to attract political interest from senior levels across all agencies.

To combat some of the current misunderstandings and misconceptions around online fraud, some agencies have created specific training products to better educate their staff and increase the level of service able to be provided to fraud victims. For example, Victim Support in the UK has developed a specific e-learning program on fraud victim typologies. This training package details the different ways
in which people can become victims of fraud, as well as outlining the gamut of consequences fraud victims may experience and the potential services victims may require access to. This training package was developed specifically to overcome some of the identified gaps in knowledge of staff around fraud victimisation. While it is basic in its content, it still provides a crucial starting point to increase a person’s understanding about various aspects of fraud victimisation. In the Victim Support context, it seeks to give staff a better understanding of the impact of fraud victimisation and to highlight the fact that losses incurred by victims extend far beyond that of just money. Its overall aim is to increase the level of service that Victim Support staff are able to offer to the victims of fraud they come into contact with.

In addition to training, there was discussion around the types of prevention messages that are promoted in terms of their ability to provide insight into the reality of fraud victimisation. There was strong support by many for the use of victim stories as a tool to increase the awareness of society generally towards online fraud. While it is easy to dismiss fraud victims generally contributing to their own circumstances, it is much harder to dismiss a victim if presented with the details of their story, and the emotion behind it. The narratives of victims can be a very powerful method in seeking to change the attitudes of others who have a preconceived idea of how a person becomes involved in online fraud and what that victimisation looks like.

**Moving Forward to Improve General Perceptions around Online Fraud**

Overcoming societal attitudes towards online fraud victims and reducing the stigma associated with victimisation cannot be achieved overnight. In a similar vein, increasing the recognition of fraud to garner political support at senior levels of government and other organisations is a slow process which will also take time as it requires a significant cultural shift in thinking. However, there are small steps which can be taken, which cumulatively work towards promoting a more realistic picture of online fraud and its devastating consequences. These steps can be used in order to gain the resources and finances required to reduce and prevent its occurrence into the future as well as support those who have already become victims.

The development of training materials for police officers would be useful in overcoming some of the misconceptions about online fraud and its victims as well as promoting a more positive message. Similar to the e-learning package developed in the UK, training materials could provide basic information on the characteristics of online fraud cases as well as inform officers on the needs of victims in coming forward. By giving police officers an opportunity to learn more about the reality of online fraud and its victims, it would hopefully promote a better understanding of this type of crime by police and improve the response to victims if and when they seek police assistance.

In addition, it may be valuable to have a dedicated fraud liaison officer across each of the police districts in Queensland. While many existing officers or crime prevention staff may have a solid knowledge of fraud, there are distinct advantages
in having a liaison officer in each district, namely a known and consistent point of contact regarding all fraud queries and concerns. In no way would this seek to diminish the role of the Fraud and Corporate Crime Group who are based in Brisbane, rather it would add to the resources available to officers in the regions when seeking information and advice around online fraud issues. It is likely that to begin with, this position would not be exclusive and would be taken on by officers in addition to their substantive role on a voluntary basis. However, the long term goal could be to provide a dedicated fraud liaison officer in each police district to act as a point of contact and liaison between the QPS, and fraud victims as well as the community in general.

The use of victim narratives to increase the awareness and understanding of people more broadly could also be used more frequently. While this is currently undertaken in Queensland and in Australia more broadly through Scamwatch, there is potential to further this in terms of the frequency and scope to increase its impact. However, it is acknowledged that this is fundamentally reliant upon the confidence and strength of victims to come forward and share their stories.

As previously detailed, the development of a fraud prevention strategy would assist in establishing the importance of fraud prevention into the future. A strategy would provide the framework through which collaborative work could be undertaken between agencies, and provides a clear vision for activities in the area. It also helps by placing fraud on people’s agenda. However, any work undertaken in this area needs to be structured in a way whereby it highlights overall benefits as well as benefits each contributing organisation can expect in order to elicit their cooperation and involvement.

**Recommendations**

5) That training materials are developed on the topic of online fraud and online fraud victims, to foster a more accurate understanding of this crime type and its impact on victims.

6) That a trial of Fraud Liaison Officers in each of the police districts across Queensland is established.

7) That victim narratives are increasingly used to promote an awareness of fraud victimisation to the community.
The Enablers of Crime

Across each of the jurisdictions visited, there was a very strong focus on the enablers of crime, or the conditions/mechanisms which facilitate online fraud to occur. There was a united and firm belief that through increased and effective targeting of the enablers of crime, that the prevention of online fraud would be a natural consequence of this action.

In the UK, there was a strong focus on documenting the process of online fraud, from start to finish and identifying all possible intervention points. Having identified these, work is currently being done on the development of a software program which can subsequently model the predicted outcomes from targeting the proposed intervention points. Ultimately, the development of software to successfully model any changes to the fraud process will assist law enforcement in making effective decisions around which particular intervention points to focus on for a more effective outcome. Disruption activities were a prominent focus within the work of many agencies, and while the problem of fraud has obviously not disappeared, there was a belief that success had been achieved and a positive effect was being had.

On a broader scale of fraud, there have been significant efforts undertaken to prevent fraudulent letters from being delivered to potential and repeat victims. By seeking to remove the fraudulent letter from the mail, it is perceived to be a very effective tool in preventing victimisation from mail fraud. While there is still much improvement to be achieved in this area, even the small steps that have been taken to date will arguably have some sort of positive impact on fraud victimisation.

In the US, similar efforts are targeted towards both online and mail fraud. There are also significant efforts being undertaken by the USPIS in a similar vein to the UK, in seeking to remove fraudulent mail from distribution. However, agencies in the US spoke particularly about the problems encountered with fraud cases, where there are multiple victims involved and the difficulties that this poses. For example, the Attorney General’s Department were in the process of mailing out thousands of letters informing victims of the status of a current case, as per their legislative requirements. This was not a unique situation, with staff commenting on various cases where thousands of victims have been involved and required management. In addition, the FBI spoke of a current case where approximately 42 million people have been identified as victims. In order to manage this case, over 30 external service providers have been contracted, given the sheer magnitude of these numbers. One can imagine the impact that an increased and more effective targeting of intervention points (or choke points as they were referred to) could have on potential victims.

Canada shared the same robust approach to disruption activities and a targeted approach to identifying potential intervention points for enforcement activity. The CAFC has a number of projects currently running which seek to shut down bank accounts, credit cards, email addresses and websites which have been linked to fraudulent activity. In addition, the Toronto Police have undertaken a number of
targeted operations and investigations which have led to successful disruption activity.

Overall, there is a universal belief that the ultimate form of fraud prevention lies in the disruption of fraud activity. This is a principle which drives much of the work of several agencies in their day to day actions. Many have had success stories which continue to pursue further performance and focus in this area.

**Lessons Learnt on Enablers of Fraud**

There are distinct benefits in focusing on the whole process and framework through which online fraud is committed. Within criminological literature, this is referred to as a “crime script analysis”. While this approach has been used frequently with other types of crime (such as organised crime, robbery, and car theft), there is perceived benefit in applying this theoretical lens to the area of online fraud, to determine the various ways in which online fraud is perpetrated, and the intervention points which could be targeted for future disruption activity. The ability to articulate how the crime process operates and identify the potential ways in which the process could be interrupted, is likely to reap significant benefits to law enforcement.

**Moving Forward to Improve the Identification of Enablers**

The adoption of a crime script approach to prevention activities may be a useful tool in helping to map out the overall process of online fraud and identify the points at which action can be taken. Given that online fraud is perpetrated through many different methods, it may be beneficial to create a script on the major categories of online fraud as they are likely to have different choke points (for example, phishing frauds operate quite differently to advanced fee fraud, which can be slightly different to romance fraud). The use of results obtained from a crime script approach could aid in the strategic targeting of crime enablers to prevent online fraud.

**Recommendation**

8) That further research using a crime script approach is undertaken to document the various types of online fraud, with a view to improving the current strategies targeting enablers of online fraud.
The Use of Online Fraud Prevention Resources

Given the diversity in online fraud techniques and methodologies used by offenders, it is not surprising that there is an equal diversity in the prevention resources developed by individual agencies to combat these. Organisations have created somewhat of a catalogue of education and awareness materials for distribution to a variety of audiences, including other government and industry bodies, targeted groups across the community and the general public. The types of resources available include fact sheets, pamphlets and booklets about different types of online fraud offences, how they are perpetrated and how to best prevent them from occurring; alerts which provide information to relevant parties about a new type of offence or provide details about recent offending activities; websites which provide the above information in an electronic format; newsletters which provide bite size pieces of information regarding the different types of online fraud, prevention tips and latest trends on a regular basis to subscribers; promotional materials which generally carry a singular message and can be distributed to the public at events; workshops which target specific audiences on a single aspect of fraud; and recovery toolkits, which provide victims of online fraud with information about what they need to do if they have been victimised, provides telephone numbers of useful agencies, provides steps to take in addressing financial issues, as well as including letter proformas to assist their correspondence with agencies. Many agencies also use a variety of mediums to promote their prevention messages, whether traditional avenues of print media, radio and television, or more contemporary modes of communication such as Facebook, Twitter and blogs.

While the content and the way in which the material was presented differed remarkably across agencies and jurisdictions, the underpinning philosophy governing the development of these materials was the same. There is strong recognition that prevention messages generally need to be short, simple, practical and actionable. In addition, they need to be targeted appropriately to the audience they are intended for. In translating this into practice, consideration needs to be given at the beginning of the process to develop resources, which determines the key message, the intended audience and the best way to target that message to that audience. This will determine the medium of the approach as well as influence its finer details.

For example, the NFA (UK) commissioned research to assess the different segments of the general population in relation to fraud. This research determined there were seven sub population groups within the UK, and was able to profile each sub population by age, gender, occupation, income and level of risk taking behaviour. In addition, the research advocated the most successful means of reaching this target group, as well as the types of fraud they were most susceptible to. The research provides strong platform on which to base future fraud prevention activities.

The appropriateness of fraud prevention messages to successfully reach their targets is also dependent on the way in which the information is presented. For example, within the US, the FTC identified that people with low level literacy skills were an underserved population when it came to prevention messages. Therefore, they
developed a project which sought to rectify this situation. Staff underwent linguistic training which focused on how to write effectively for this audience. Consequently, they were able to conduct usability tests on their websites and review materials accordingly. The result of this aims to improve the effectiveness of prevention messages to the wider public, but particularly individuals with lower level literacy skills.

The importance of networks was also highlighted by many agencies, in terms of distributing fraud prevention resources. There is no point creating prevention materials if they cannot be accessed. While a large number have been made available electronically for download off the internet, there is still a strong push towards hard copy materials which can be physically distributed to their target audience. The different means in which materials can be effectively formatted was one of the key findings of the UK’s segmentation research. One agency in the US, operate what they term a “wholesale retail market model”. This sees them push their products out to a network of partners, for onward distribution through their own networks. This appears to be one of many ways that agencies effectively distribute their materials.

**Lessons Learnt on Prevention Resources**

There are a number of creative ways in which fraud prevention messages are captured and distributed across each of the jurisdictions. Almost every agency has some degree of prevention resources available to the general public, in some format (whether hardcopy materials or a website presence). While it is positive to have such a high level of interest in promoting a prevention message regarding online fraud, it does create somewhat of an overloading of resources, and can lead to uncertainty for people. With so much information available on the prevention of online fraud, it can be very confusing and difficult to navigate through so many different resources to get to the one which is relevant to that person at that time. While the use of segmentation research detailed above seeks to overcome this to a degree, there are still a large number of resources available that individuals must sort through themselves. In addition, there are instances where different organisations have competing or contradictory messages or advice, which further confuses the situation.

However, the existence of such a large array of fraud prevention materials is positive, in terms of increasing society’s awareness of online fraud. There is no “right” way to develop prevention materials and resources, although using a basis such as the segmentation research in the UK, aims to increase the relevance and appropriateness of prevention messages. The challenge remains in achieving this through effectively targeting the prevention materials so that they are relevant to their intended audience.

There is also a significant challenge in determining the success of fraud prevention materials and campaigns. There are very few, if any, evaluations which seek to analyse the effectiveness of prevention campaigns and the development of resources. While research has been conducted to determine how to target messages
on specific populations, there has been no follow up to determine the success, if any, of these materials. Many agencies did speak about positive feedback they had received anecdotally from stakeholders or individuals. However, there is no formalised evaluation to determine if the resources or materials have succeeded in changing or modifying a person’s behaviour, or had an effect to reduce the likelihood of victimisation on their intended targets. While an evaluation of this nature could be complex, there is a need to determine if the prevention messages that are being promoted are having any degree of success. Otherwise, valuable time and money is being used to develop prevention materials which are ineffective and could be better allocated to other areas. In addition, if the messages themselves or the ways in which the messages are being promoted are not achieving their overall aims, there is no point continuing with a defective product. The lack of evaluation surrounding fraud prevention materials is an area which needs immediate attention.

Moving Forward to Improve the Resources Available

There is a need to review the current crime prevention resources that the QPS promotes regarding online fraud. In reviewing these resources, consideration needs to be given to the above points such as: content of the resources; the manner in which the key message/s are presented; the means in which they are distributed; whether or not the current materials are appropriate for their intended targets; and whether or not the materials have any effect on reducing the likelihood of fraud victimisation. Upon completion of this review, future actions regarding the revision of existing materials or the creation of new or additional resources could be considered. In order to better target prevention messages in an appropriate manner, it may also be beneficial to replicate the segmentation research undertaken in the UK, to determine its relevance to an Australian context. This would assist in creating more effective prevention messages as well as targeting them in a more appropriate manner.

Regardless of the outcomes of this review, greater focus needs to be given to evaluating the outcomes of prevention materials overall. An evaluation methodology or template could be developed to ensure that all future prevention materials and resources targeting online fraud can be effectively measured as to the degree in which they achieved their aims. Formal evaluation also provides an opportunity to capitalise on aspects of resources which worked well as well as learn valuable lessons from those efforts which perhaps did not work as well.

Recommendations

9) That all of the current resources and materials promoted on the topic of online fraud prevention are subject to review.
10) That segmentation research is undertaken to determine the different target groups within society regarding online fraud.
11) That an evaluation method is developed to determine the effectiveness of fraud prevention materials on achieving their stated goals.
The Impact of Online Fraud Victimisation

Within society there is an overriding perception that victims of online fraud, or even fraud more generally, only lose money as a result of their victimisation. No consideration is given to the scope of consequences beyond the loss of money which are experienced by many victims. There was a strong recognition by the victim support agencies, as well as other enforcement agencies, around the actual impact of fraud victimisation and its potential consequences. As previously indicated, fraud was advocated as being one of many problems a person may be experiencing and therefore a holistic approach to intervention was seen to be the most effective to assist fraud victims in their recovery. While the majority of victims are likely to experience some sort of depression, there appears to be a greater focus on the potential of suicide for fraud victims than is current within Australia.

The suicide of fraud victims is an area which has received relatively little research to date. The majority of knowledge in this area seems to be anecdotal from agencies who have dealt with fraud victims, rather than any sustained inquiry. Within the UK, there was recognition of this from several agencies, and an awareness of its potential occurrence. An example was given of a case many years ago, whereby 16 people took their own life, largely as a result of a large scale fraud case. In the US, the FBI’s Victim Assistance Unit believe there is evidence to suggest the suicide of fraud victims, therefore they currently monitor their victims for suicide. The tragic case of an elderly woman committing suicide and her brother attempting suicide after losing a substantial amount of money to fraud, highlights the gravity and devastating consequences of some cases. There is a belief on the part of the FBI that victims will often give clues or messages to people around them if they are contemplating suicide, including family and case workers, so all of their officers are trained in suicide ideation. Older victims in particular, have increased vulnerabilities after becoming a victim of fraud, so there needs to be an upfront awareness of this possibility.

Lessons Learnt on the Reality of Online Fraud Victimisation

Victims of fraud are seen by many to be resource intensive and requiring specialised programs and counseling to assist in their recovery. As detailed earlier in this report, there is a need to assist victims in a variety of areas to enable them to get back on their feet and move forward after becoming a victim of fraud. While suicide is an extreme outcome for fraud victims, the seriousness and devastation that many victims experience cannot be underestimated or ignored.

The willingness of the FBI to track and monitor all fraud victims in relation to their wellbeing is an important step in being able to assist victims where necessary and intervene should the need arise. The QPS has recently implemented state-wide use of SupportLink, which is a single electronic referral gateway for police to link victims and other vulnerable persons to community organisations. SupportLink is equipped to assist with many problems including suicide, so there is potential to improve current efforts towards victims of fraud with an increased use of this referral system.
The training of field agents on suicide is another area which has merit. By assisting officers to recognise any signs or messages of potential suicidal behavior, this enables the officer to intervene and refer the victim to the appropriate support in a timely manner. While it is relatively unknown about the extent of suicide resulting from fraud victimisation in Australia, one cannot assume from a lack of knowledge that there is no problem. In addition, with a predicted increase in the number of victims to online fraud offences into the future, without immediate action, it is likely that the number of fraud victims and the severity of their victimisation may exacerbate.

Moving Forward to Improve the Wellbeing of Online Fraud Victims

Within an Australian context, little is known around the prevalence of suicide amongst victims of fraud. While anecdotally it does not seem to currently be a significant problem, this does not detract from an overall need to better monitor victims of fraud, with an eye to intervening if necessary to prevent outcomes such as suicide.

From this, there is a distinct need to develop a better evidence base in which to gain a better understanding of the wellbeing of fraud victims and to be able to document any current or future trends regarding the suicide of victims. It is anticipated that with an improvement of current support services directed to fraud victims, that these extreme outcomes could be avoided, however, if action is not taken to improve the availability of support services to victims who need it, then these worst case scenarios may become more prevalent.

Stemming from this, it would be beneficial for police officers likely to interact with fraud victims, to receive training on suicide. Currently, the QPS has a suicide prevention training which many officers are undertaking, and therefore, the addition of fraud squad officers to this current training schedule, should be easy to facilitate and better prepare officers if they should interact with a victim contemplating suicide.

Recommendations
12) That a system is developed to better monitor fraud victims and their wellbeing, to prevent the likelihood of suicide.
13) That a greater promotion of SupportLink is made, with regards to its possible assistance with suicide.
14) That research is undertaken to better understand the prevalence of suicide amongst fraud victims, with a view to strengthening protective factors which guard against suicide.
15) That those individuals involved with fraud victims undertake suicide prevention training, to enable an improved recognition of any signs a victim may exhibit relating to possible suicide.
A Different approach to Victims

The approach to victims in several of the agencies I visited differed greatly to that I have observed within Australia, in that there is a strong recognition that victims of fraud may be better served through the combination of a crisis intervention approach as well as a case management approach.

To explain what is meant by crisis intervention, there is an acknowledgement that fraud victimisation may not be the only issue an individual is facing. Instead, fraud victimisation may be symptomatic of wider problems within social, welfare and health fields. Fraud victimisation may also extend its impact to create other problems, such as insufficient money for food, homelessness, and debt concerns, which are likely to exacerbate quickly without a timely and appropriate response. There is a general belief that the earlier a victim receives assistance and intervention, the better their ability to cope with what has occurred.

In order to achieve this, a better integration of existing services for fraud victims was advocated. The issues facing individuals as a result of fraud victimisation are unlikely to be solely a policing issue; rather they fit within a broader social agenda. In the UK, the example of the No Secrets Agenda was put forward. This is an initiative of the health department which seeks to develop and implement multi agency policies and procedures to protect vulnerable adults from abuse. A similar approach was suggested regarding fraud victims. This would involve other stakeholders and agencies to assist fraud victims where necessary, as well as recognising the depth and complexity of many fraud victim’s issues.

In terms of case management, the relationship that an agency developed with individual victims of fraud varied remarkably. However, there was agreement that many fraud victims required intensive support and assistance to get their lives back on track. Although some victims required no assistance, or simply requested information, at the other end of the spectrum there were victims who required intensive and ongoing support. This was able to be provided in some cases, through volunteers services in both the UK and Canada. In the US, the FBI’s Victim Assistance Unit has field agents across the country who work with victims across all types of crimes, including fraud. These field agents are highly trained (with the majority holding Masters degrees or higher in psychology or social work) and specialise in victim issues. There were other agencies and individuals who could be seen to practice a case management approach to victims although this was on an informal and ad hoc basis. A lot of this was driven by the personality of the agency worker involved and their compassion towards the victim/s they had interaction with.

In particular, repeat victims are a group targeted by many for a case management approach. Repeat fraud victims pose unique challenges for law enforcement and other agencies when it comes to preventing future victimisation. In many cases, they are unable to see the situations they are involved in as fraudulent, despite the intervention of third parties, such as family, friends and law enforcement or other agencies. Many people I spoke to have invested great amounts of time with repeat
victims, in trying to get the repeat victim to recognise the reality of their situations and the fraudulent opportunities being presented to them. However, often hours of conversation was erased with one further contact from an offender, or the receipt of another letter or email. While the victim states an acknowledgement that the previous letters or emails were fraudulent, the one presented to them on this occasion must be true. Such an incident is understandably frustrating for agency workers involved with repeat victims, who at times struggle to maintain a sense of calm when dealing with repeat victims. In some of these instances, the agency worker involved treats the repeat victims under some sort of case management approach, but this is not formalised and relies heavily on the good will of the agency worker involved. Arguably what is needed in some of these circumstances is a support person to sit with the repeat victim and go through their mail or emails with them on a weekly basis, or maintain regular phone contact with the person to continually remind them of the fraudulent nature of the invitations and offers they are receiving. Such support and assistance is very resource and time intensive and needs to be tailored specifically for the needs of each individual repeat victim.

Lessons Learnt on the Benefits of these Approaches

There are both advantages and disadvantages to approaching victims from within a crisis intervention and case management perspective. In terms of the crisis intervention approach, it is an important step forward to begin to formally recognise that crisis intervention should not be limited only to victims of violence and this was heavily emphasised by one agency. The idea that fraud victimisation may be symptomatic of other problems being experienced by the victim is also important in being able to treat the person holistically. In order to address the problem of fraud victimisation, other issues may need to be addressed to successfully prevent future victimisation. This recognition is already evident and practiced in other fields, so applying it to fraud seems a logical extension of this. It also seems reasonable that the sooner a victim receives assistance and support, the better they will cope with their experiences. Otherwise, both the fraud victimisation and its consequences may spiral out of control, in some cases leading the victim to commit suicide. The prevention of this extreme is highly desirable.

The benefits of a case management approach are also readily apparent. There is a group of victims, including repeat victims, who would benefit from an ongoing one on one approach to prevention. This would allow the unique needs of each victim to be recognised and addressed. While many individuals and agencies are currently using an ad hoc approach and informal approach to case management, the formal recognition of this approach would enable better services to be provided to those victims who require it.

However, while both the crisis intervention and case management approaches have the potential for significant benefits, it is foreseeable that there are several barriers which would prevent this from occurring. Firstly, both of these approaches require a high level of resources, in terms of allocating staff to victims. It is safe to assume that some victims would require a substantial amount of time invested into them for an
undefined period. For some victims, the consequences and impact of years of fraud victimisation are unlikely to be resolved within a short timeframe. Therefore, in order to provide this service, considerable resources would need to be allocated on an ongoing basis.

The second problem relates specifically to law enforcement agencies. It is easily argued that both of these approaches do not fit within the model of policing currently employed by many police services across the globe. Particularly when talking about case management, it is not the responsibility of the police to provide the ongoing support and assistance to individuals as discussed above. Police officers are already heavily burdened with their workloads and do not have the capacity to sit with a victim on a regular basis to talk through the fraudulent emails or letters they may have been receiving. This then presents a challenge given that police and other law enforcement bodies may be the first point of contact for victims or family and friends of victims, seeking action or intervention on fraudulent matters. There is often an expectation on behalf of the victim or other third parties, that police should be able to achieve more than is realistic or possible in this sense.

**Moving Forward to Improve Responses to Online Fraud Victims**

There are a number of options which could be explored that seek to facilitate both crisis intervention and case management approaches to victims of fraud, while still recognising the boundaries that police agencies have when interacting with victims. These will be outlined in the sections below.

The easiest way to address these issues focuses on a more efficient use of an e-referral system by police to connect fraud victims with existing community support services. SupportLink provides an easy mechanism for police officers to refer consenting victims of fraud for the support and assistance they might require. The introduction of SupportLink fills a large void, where prior to SupportLink, any referrals of support were largely dependent on the knowledge and good will of the police officer.

However, while SupportLink theoretically provides a solid outcome for fraud victims in being able to access support, further work must be done to ensure that it meets the needs of fraud victims. This may entail the securing of services, such as financial counselling, which may be more unique to fraud victimisation. For the main part, it is anticipated that the issues faced by fraud victims are largely similar to victims of other crime types, in terms of the physical deterioration of their health, the emotional and psychological problems experienced (namely depression) and the subsequent relationship breakdown which frequently occurs. Assistance with these types of issues could reasonably be managed by any number of community agencies. However, it is important to ensure that all fraud victim needs can be met through SupportLink and steps should be taken to enable this to occur.

Secondly, the introduction of SupportLink is an important step forward for police in facilitating them to refer victims for support and assistance when required, but
police need to know that this mechanism exists for it to be effective. While it is acknowledged that the project is in its infancy, further work needs to be done to promote SupportLink to police officers around the state, including those who work specifically in fraud. The project has great potential to provide opportunities of valuable assistance to victims of fraud, but unless the police officer handling the victim knows about the program, the victim will not receive a referral. In addition, the ability of SupportLink to assist victims of all types of crime, including fraud, needs to be highlighted. This is to combat any misconception that SupportLink (or any type of victim assistance) is only available for victims of violent or physical crime.

Recommendations

16) That further work is done with the SupportLink Project Team to ensure that appropriate referral agencies are available to support the varying needs of fraud victims.

17) That further work is done with the SupportLink Project Team to promote its existence as an effective means in which consenting fraud victims can receive the support assistance they require.

Further suggestions on how to effectively use a case management approach to fraud victims relates to the use of volunteers and will be further detailed in the following section.
**Volunteers**

The use of volunteers to support victims of fraud is used in the United Kingdom and Canada. Within the UK, it is in the form of Volunteers Support while in Canada it is through a program called SeniorBusters as well as Victim Support Services, Toronto. While these programs have been mentioned earlier, further details are provided in this section, particularly on the role that volunteers play within the programs.

**Victim Support, UK**

Within the UK, all victims of crime can access support through an organisation called **Victim Support**. Victim Support is a national charity, largely staffed by volunteers (four volunteers to one paid staff member according to their website). In terms of online fraud victims, as part of the reporting process in ActionFraud, all victims are asked about the severity of the impact of their crime as well as asking whether or not they would like to be referred to Victim Support for further assistance. If an individual consents to this process, the referral is made to Victim Support. Contact by Victim Support is initiated with the victim via a phone call (or letter if phone contact cannot be established), with the offer of either emotional support or practical help. If required, face to face support can be organised through a network of agencies across the UK. The volunteers have the ability to meet with victims and provide ongoing support and assistance on a case by case basis. There are offices located throughout the UK, which increases the accessibility of victims to this service.

**SeniorBusters**

This program commenced in 1993 as a smaller project called Phonebusters, which was initiated by the OPP Anti Rackets Branch. While the initial scope of the project was focused on investigating complaints of telemarketing fraud to individuals on Ontario, the magnitude of the problem soon became apparent and broadened the scope and need of the project. In particular, a large number of calls were being received from seniors who had been victims of various types of fraud and were looking for assistance. In 1997, SeniorBusters was added to fulfil this need. SeniorBusters comprises of around 50 volunteers (who are seniors themselves) who help to increase the awareness of fraud to seniors as well as offering support to those who need it. Located in the CAFC, North Bay, the volunteers work rotating shifts completing a variety of tasks, including the calling of seniors who have been identified as victims of fraud or vulnerable to fraud. The majority of these individuals are identified through their lodging of a complaint to the CAFC. As seen in the UK, eligible callers are asked whether they would like a follow up phone call from the SeniorBusters program. With their consent, a volunteer will call the individual on a one off or regular basis to offer support and advice as required.

**Victim Support Services, Toronto**

Similar to the work of Victim Support in the UK, Victim Support Services, Toronto provide counselling and assistance to all victims of crime and victims of circumstance
across the greater Toronto area. While there are a number of paid counsellors who work, there are also a large number of volunteers who assist in the provision of counselling or other support as required. This can be done in a number of ways including over the phone or in person. Victims can be referred to the service by a police officer but they can also access the service by themselves without a referral. Victim Support Services can offer their own services or are able to refer the client to any number of other community based services in their local area as required.

**Lessons Learnt on the Benefits of Volunteers**

Volunteers provide invaluable services across each of these three organisations. The generosity of volunteers to give their time and expertise to help victims of crime is of great benefit to the organisations, the victims and the community at large. Without the assistance of volunteers, it is unlikely that each of these agencies would be able to provide their current level of service in supporting victims of crime, including fraud. Therefore, volunteers play a critical role in the ability of each of these agencies to deliver support services to victims as they need it.

From a law enforcement perspective, the use of volunteers to provide a case management approach to victims of fraud and other vulnerable persons overcomes some of the issues previously stated, including the policing role, resources and community expectations. Given that police do not have the time or ability to provide regular or high level assistance to victims, the potential ability of volunteers to fill this gap could be explored. Volunteers in each of the programs detailed, receive varying levels of compulsory training and supervision. It is important to note, that the majority of the volunteers engaged in these programs are not qualified counsellors or psychologists and do not profess to offer professional advice. Instead, they offer what one agency terms “emotional support” through active listening. Volunteers are able to spend the time with the victim, to talk over the phone or sit down over a cup of coffee, and to listen to the victim. Volunteers can direct victims to other services which may be beneficial to their situation, as well as being able to act as an advocate on their behalf in their interactions with other agencies. This role helps to fulfil many of the needs experienced by victims, but cannot be provided by law enforcement agencies. This role also enables the victims to receive ongoing support where needed, and should help to reduce the impact of current and previous victimisation as well as prevent further victimisation.

**Moving forward to Utilise Volunteers**

The use of volunteers across the UK and Canada was one of the most impressive aspects I witnessed during my trip. Their contribution to victim services is invaluable to a population who are otherwise underserved and often ignored. The ability of fraud victims to access these services is a strong indication of the recognition afforded to these victims in other jurisdictions. While SeniorBusters focus exclusively on seniors who have been victimised or are vulnerable to fraud, the other two agencies have a wider ambit which includes victims of fraud into their routine work.
Given the success of these jurisdictions to utilise volunteers to provide ongoing support and assistance to victims of fraud, it would be timely to explore the capacity of a similar program being trialled in Queensland. The use of volunteers fits well within the current Queensland Government’s *Towards Q2* Strategic plan, which advocates the increase of volunteering by 50%. In addition, the use of volunteers to provide much needed support services to victims will drastically reduce the financial costs associated with these services. Harnessing the time and expertise of willing volunteers helps to address the need for victim support in a more costly manner than other possible measures.

There are many options which could be explored regarding the establishment of a volunteer program to support victims of fraud. The example of SeniorBusters is advocated as an appropriate model in which to base any Queensland based program, given its origins within the OPP and its focus on seniors, who feature prominently in fraud victimisation statistics within Queensland. It may also be beneficial to extend the scope of the program to include seniors and repeat victims regardless of age. These are arguably two of the most vulnerable populations regarding fraud and are likely to benefit greatly from a case management approach. The QPS already has a well established Volunteers in Policing Program which would provide an appropriate framework to trial a new victim support program.

**Recommendation**

18) That a pilot program is established, which utilises volunteers to provide support and assistance to repeat victims of fraud and seniors vulnerable to fraud.
The Branding of Fraud Victims

It is readily apparent within Australia and overseas, that there is a disparity between perceptions of victims of online fraud compared to the truth of online fraud victimisation. As noted earlier in this report, there is a strong stigma and sense of shame and embarrassment associated with online fraud victimisation. Victims are perceived to be greedy, uneducated, of lower socioeconomic status and somewhat deserving of their victimisation. However, the validity of this stereotype is contradictory to the reality of the majority of fraud victims. The consequences of this stereotype in some respects, can be as devastating as the consequences of the fraud victimisation itself. There was a divide between agencies in terms of ascribing to this stereotype, some did not believe it existed or that it had improved in recent times, while others argued there would need to be a significant cultural and societal shift for this to be overcome.

Generally speaking, all agencies who work with fraud victims, are aware of the reality of fraud victimisation and try to educate those around them so as to not perpetuate the false beliefs. However, a number of agencies themselves do not perceive victims of fraud as victims, and this influences their interactions with them. For example, some agencies view victims as witnesses or sources of intelligence, which although important to the work of their agency, does not acknowledge the true extent of what victims have experienced. In addition, fraud victims battle a number of misconceptions which are not relegated to the above stereotype. There is also a misperception that fraud is a victimless crime, or that victims who get their money back (for example victims of phishing emails) are not really victims at all. In combination, these inaccuracies of fraud continue to reinforce the unrecognized nature of fraud victimisation and the impact it can have on individuals.

The way in which victims are dealt with across jurisdictions differs and there are a number of factors which can impact on this, which can include the existence of victim charters, victim legislation and codes of conduct or practice for professionals. Within the UK, there is a Code of Practice for Victims of Crime (2008) which outlines minimum standards of support for victims of all types of crime. Within the US, there are two pieces of legislation, being the Victims Rights and Restitution Act (1990) and the Crime Victim’s Rights Act (2004). Both of these set out the rights and expectations that victims are entitled to throughout their interactions with the criminal justice system. In each of these, all rights and entitlements are universal and do not differ between victims of violent or non-violent crime. In the US in particular, agencies spoke of the ways in which there should not be any discrimination against victims of non-violent crime (such as fraud) when it came to accessing support and assistance. Within Queensland, while legislative definitions of crime encompass victims of non-violent crime, their ability to access support and services is not established. Instead, the Victims of Crime Assistance Act (2009) specifically articulates that victims must have suffered a physical injury to be eligible for any support. While referrals to SupportLink do not have this limitation, there needs to be an increased awareness of police officers to use this system.
Lessons Learnt on the Current Image of Online Fraud Victims

It is evident that there is no consistency when it comes to the support of victims of non-violent crime, such as fraud. While theoretically, the existence of legislation which codifies victims rights, does not always translate as well into practice. However, the existence of a framework through which to work within is a positive step which can be improved upon. In terms of overcoming the stereotype, there was a suggestion by several individuals to place a greater emphasis on the stories of victims, as opposed to just using messages. As previously noted, the personal narratives of victims can be a powerful tool in helping to breakdown some of the misconceptions around online fraud victimisation. The use of personal stories can also help to reinforce the vulnerabilities of everyone to online fraud, in a non-threatening way.

The ways in which victims are conceptualised by agencies is also important. Those who have experienced online fraud can play a number of different roles in the criminal justice system. The way they are perceived by each agency they interact with, will largely determine the way in which they are treated and viewed. Of particular interest was the way in which some agencies stated they approached victims and the use of language in talking to them. For example, staff at the US Department of Justice stated that in all of their dealings with individuals, they never used the word “victim”. Instead, their approach encompassed presenting all of the known facts the individual and letting them reach the conclusion themselves. There was a belief that in presenting all of the available facts to a person in a calm, rational and respectful way, that most people will come to see the reality of the situation they are involved in. While this isn’t always the case, there was a sense that it worked in most situations.

The use of language is also important. While it is recognised that the term “victim” is value laden and can imply negativity, it is difficult to avoid its usage, particularly when legislation enshrines its use. However, by specifically choosing not to use the word when talking to persons who have been defrauded, it is a positive way of interacting with people at a sensitive time. Nobody wants to hear that they have been victimised and with the stigma associated with online fraud victimisation, the use of the victim label can exacerbate it.

Moving Forward to Reduce the Stigmatisation of Online Fraud Victimisation

It is clear that much work has yet to be done on breaking down the stereotype associated with online fraud victims and the discrepancy between perceptions of fraud victims compared to the reality of fraud victims. There is also much to be done to improve the current disparity between victims of violent crime compared to victims of non-violent crime. There was a belief expressed by several individuals that in many cases, the consequences experienced are the same, however the recognition of this differs remarkably.

Essentially, there is a need to “rebrand” online fraud victims in a more positive and empathetic manner, in a bid to shift societal attitudes around online fraud
victimisation. Cultural change has been achieved in addressing other issues, so there is no reason as to why it can’t occur regarding online fraud. However, it will not happen overnight and it is likely that incremental changes will need to occur over a period of time. To assist with this rebranding, the employment of professional marketers would enable the first step to be made in helping to promote a more realistic picture of online fraud victimisation and to overcome some of the stigma and shame currently associated with this crime type.

Recommendations
19) That a campaign is developed to assist with the rebranding of online fraud victims to overcome the negative stereotype and stigma associated with online fraud victimisation.
20) That greater recognition is given to the way that agencies interact with victims of fraud, with reference to language and the ways they are viewed.
21) That consideration is given to including victims of non violent crime within the eligibility of current victim assistance schemes.
Conclusion
The opportunity to travel overseas and observe first hand, other agency and jurisdictional approaches to the prevention and support of online fraud victims has been a great honour. As is evident from this report, the agencies visited were able to impart a considerable amount of knowledge and expertise across these areas. I am grateful for their willingness to share and discuss these topics with me. There is a lot of positive work happening in the fraud space, and many lessons which can be taken from these examples to improve the current situation in Queensland, and Australia.

As noted at the beginning of this report, it was impossible to capture all of the topics and discussions held with individuals across the fellowship period. Therefore this report has sought to present some of the most pertinent discussions, specifically focused on the prevention and support aspects of online fraud victimisation. In doing this, several recommendations have been put forward during the course of this document. However, prior to concluding this report, the following section sets forth an overall musing focused on crime prevention messages as they relate to online fraud.

Reflections on the Prevention of Online Fraud

It is evident throughout this report, that considerable work is being done on a global scale to combat online fraud. There are a vast number of agencies in every country who contribute to overall prevention efforts, yet at the same time the prevalence of online fraud victimisation is increasing and affecting a growing number of people. It is therefore clear that there is still a real and pressing need to further preventions into the future. While significant work has been undertaken, much work is yet to be done.

This report has highlighted a selection of key strategies, resources and programs used by agencies across the UK, US and Canada. As detailed, there are many shining examples of innovative and effective methods to prevent online fraud. Many lessons can be learnt from the work of these jurisdictions. The challenge remains to translate and adapt these examples into tools which will be equally as effective within an Australian and Queensland context. Having had the opportunity to discuss and observe firsthand many of these programs and measures, I have been able to reflect on how prevention activities are undertaken both here in Australia and abroad, and offer the following observations.

Online fraud is complex. Everything about online fraud can be complex and highly sophisticated. Many offenders use multiple (false) identities. Many offenders use multiple accounts and direct transactions through a variety of countries. Many offenders use multiple reasons (or excuses) as to why further money is required on

---

2 I am very grateful to Detective Constable Mike Kelly (Toronto Police Service) for the many discussions and emails we have shared on this topic and can attribute many of these conclusions as a result of his shared knowledge and expertise as well as coining the phrase “white noise”.

48
the part of the victim. Many offenders use multiple stories and approaches to entice the victim into the fraud in the first place. Many offenders use multiple technologies to hide the truth of the situation. At face value, nothing about online fraud appears straightforward, but this is simply not the case.

While the ways and means through which online fraud is perpetrated are complicated, the essence of this crime lies at the transfer of money. There is no crime until there is a transfer of funds from one party to another, from victim to offender. No matter how the victim ended up at that point, the transfer of money to the offender is the critical point at which the success or failure of all previous prevention efforts culminates. How the victim got to that point is irrelevant, instead what matters is what happens at that point in time and the consequences of that action. Details of the approach, the reasons given for needing the money, all other specifics of the situation can best be seen as “white noise”. To some degree, they can be seen as irrelevant to the overall situation. If the best prevention efforts focus on the lead up to the transfer of money, but not on the transfer of money, then they are unlikely to succeed. The focus needs to be on the crux of the offence, the transfer of funds (or the sending of personal details and passwords in some cases).

Prior to my departure, one of the questions posed in my discussion paper centered on how to promote a crime prevention message for online fraud which was general enough to encompass all the different ways that it can be perpetrated but still unique enough that it held true for its target. Too often in current work, victims have disregarded advice or suggestions provided to them on suspected fraud victimisation because their experience differed slightly to what other victims have experienced. Through focusing the prevention message more strongly on the transfer of money, this removes this barrier as all victims find themselves in this situation.

In the same way that online fraud is seen to be a complex type of crime, the prevention efforts surrounding online fraud have also become quite complicated. To a degree, this is evident in the plethora of resources and materials that are available across each jurisdiction, aiming to educate people against online fraud and increase awareness of its occurrence. While it is important to alert people to the various ways in which they can be approached or become involved in online fraud, it is arguably more important to alert people to the dangers of transferring money, particularly to an overseas contact. Attention needs to be made on the lack of recourse available to victims once they have sent money. In the same way that society generally takes the time to read through a contract prior to signing it, efforts needs to be focused on persuading individuals to show the same level of consideration prior to sending money.

Current crime prevention resources and campaigns focus heavily on the “white noise” surrounding online fraud. They provide information to the general public on characteristics of the various types of online fraud as well as the ways in which they are perpetrated. There are countless examples of fact sheets, brochures, pamphlets, alerts, bulletins, newsletters and web pages which describe the various paths to victimisation. There are fewer resources which focus on the money transfer as the
key element of online fraud. It could be argued that the majority of prevention efforts and key messages focus on the journey (how the fraud is perpetrated) rather than the destination (transferring funds and becoming a victim of online fraud). While the journey is important, greater focus needs to be targeted at the end point. This is likely to be more effective in that it removes the confusion over complex prevention messages which try to encompass all possible scenarios of online fraud victimisation. Money (or personal information) is the essence of all fraud offences, therefore it should be the driving force behind the majority of preventative messages.

This does not seek to undermine the work which has been done by existing agencies in this area. It is important to promote an awareness of the different types of online fraud which exist and to which individuals can be targeted. As seen from this report, some of the recommendations focus on a review of resources and materials used to promote online fraud prevention, the revision or development of new materials. Instead, it is advocated that a greater focus is placed on the critical point of the offence, being the sending of money. Prevention efforts which ignore this aspect are likely to not be as effective, given the potential for interference of the “white noise” to obstruct the main point.

Overall, it is important not to let the perceived complexity of online fraud overshadow the reality of online fraud. While the level of sophistication is important and arguably one of the biggest barriers relevant to the investigation of cases, a more simplistic approach can be applied to prevention messages. In terms of prevention, the focus needs to be on the transfer of money from victim to offender, the first time, and if relevant, all subsequent payments. The factors which hinder investigations are not necessarily barriers to the development of an effective prevention message. Instead, it is about a conceptual shift which alters the focus of future resources, campaigns and prevention messages from the “white noise” to the one critical point that all victims of online fraud have in common, the transfer of funds or the sending of personal information.
Recommendations

Throughout this report, many recommendations have been proposed to improve current responses to online fraud prevention and victim support services. Based on my observations and unique learning position, there is a lot of knowledge and expertise that can be drawn upon from these overseas agencies and adapted to an Australian or Queensland context. Therefore, the following recommendations are made with the view to harnessing the best practices and innovative ideas of the various agencies observed and seeking to transform these to a local context.

In terms of implementing the recommendations, as is strongly argued within this report, one agency cannot be held responsible for singlehandedly preventing online fraud or for the delivery of victim support services. Instead, a collaborative approach must be taken if any future work in this area is to be successful. Therefore, it is suggested that partnerships must be developed amongst a variety of agencies to improve current responses to fraud and to deliver leading prevention programs and support services to victims of online fraud in the future.

The recommendations set out in this report cover a wide array of issues relating to both the prevention and support aspects of online fraud prevention. Given that evidence has been presented throughout the report to justify these recommendations, the following restates these recommendations in their entirety.

### The Creation of a Fraud Strategy
1) That a fraud prevention 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 in Queensland.

### The Creation of a Central Reporting Agency
2) That a central reporting body is established to act as a single contact point for victims of fraud, and enable a single repository for all complaint data.
3) That all until such time as a central fraud reporting body can be established, greater work is done to educate all possible fraud contact points on the possible reporting of fraud offences.

### The Development of Formal Relationships
4) That formalised partnerships are developed with identified key stakeholders to specifically address the prevention and victim support aspects of online fraud.
The Revision and Development of Training Materials and Resources
5) That training materials are developed on the topic of online fraud and online fraud victims, to foster a more accurate understanding of this crime type and its impact on victims.
6) That a trial of Fraud Liaison Officers in each of the police districts across Queensland is established.
7) That victim narratives are increasingly used to promote an awareness of fraud victimisation to the community.

The Identification of Crime Enablers
8) That further research using a crime script approach is undertaken to document the various types of online fraud, with a view to improving the current strategies targeting enablers of online fraud.

The Revision and Development of Online Fraud Prevention Materials
9) That all of the current resources and materials promoted on the topic of online fraud prevention are subject to review.
10) That segmentation research is undertaken to determine the different target groups within society regarding online fraud.
11) That an evaluation method is developed to determine the effectiveness of fraud prevention materials on achieving their stated goals.

The Monitoring of Fraud Victims’ Wellbeing
12) That a system is developed to better monitor fraud victims and their wellbeing, to prevent the likelihood of suicide.
13) That a greater promotion of SupportLink is made, with regards to its possible assistance with suicide.
14) That research is undertaken to better understand the prevalence of suicide amongst fraud victims, with a view to strengthening protective factors which guard against suicide.
15) That those individuals involved with fraud victims undertake suicide prevention training, to enable an improved recognition of any signs a victim may exhibit relating to possible suicide.

The Promotion of Support Services Available
16) That further work is done with the SupportLink Project Team to ensure that appropriate referral agencies are available to support the varying needs of fraud victims.
17) That further work is done with the SupportLink Project Team to promote its existence as an effective means in which consenting fraud victims can receive the support assistance they require.

The Establishment of a Volunteer Support Program
18) That a pilot program is established, which utilises volunteers to provide support and assistance to repeat victims of fraud and seniors vulnerable to fraud.
<table>
<thead>
<tr>
<th>The Rebranding of Online Fraud Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>19) That a campaign is developed to assist with the rebranding of online fraud victims to overcome the negative stereotype and stigma associated with online fraud victimisation.</td>
</tr>
<tr>
<td>20) That greater recognition is given to the way that agencies interact with victims of fraud, with reference to language and the ways they are viewed.</td>
</tr>
<tr>
<td>21) That consideration is given to including victims of non-violent crime within the eligibility of current victim assistance schemes.</td>
</tr>
</tbody>
</table>
Appendix One

The Prevention and Support of Online Fraud Victims – Discussion Paper

Dr Cassandra Cross – Churchill Fellow 2011
Queensland Police Service

Introduction
Every day inboxes are being flooded with invitations to invest money in overseas schemes, notifications of overseas lottery wins and inheritances, as well as emails from banks and other institutions asking for customers to confirm information about their identity and account details. While these email requests may seem outrageous to most people, a large number of email recipients believe the request to be legitimate and respond, through the sending of money or personal details. This action can have devastating consequences, financially, emotionally and physically. The Queensland Police Service estimates that over AUD$1M leaves Queensland every month as a result of advance fee fraud victimisation. However, given the complex nature and unique characteristics of online fraud, victims are unlikely to recoup their money and the criminals are unlikely to be arrested and prosecuted. Enforcement action is important, however greater success is likely to come in the area of prevention, which avoids victim losses in the first place. This is acknowledged by the Queensland Police Service, and is evident in the current work being undertaken in the area of online fraud prevention and victim support.

The following paper outlines current knowledge within Queensland regarding online fraud prevention and victim support services. Based on this knowledge and experience, it poses questions around 20 specific topics to gain further insight and expertise into the area, as well as investigating possibilities for future work.

It is not anticipated that every individual and agency will be able to contribute answers to every question. Rather, these questions are designed as a guide to generate discussion on some of the more pressing topics currently under consideration. In addition, these questions are not exhaustive and may elicit other topics of discussion not cited.

*******

Online Fraud Victims

Topic 1
From our own research and experience, there is no one profile for victims of online fraud. Instead, victimisation cuts across all demographics. However, seniors are attractive targets for criminals and this is reflected in victimisation numbers.

- From your own observations, who becomes a victim of online fraud?
- Is there a particular characteristic or demographic which appears to be significant?
- Is there a particular characteristic or demographic which appears overrepresented?
Topic 2
Our own research indicates that there is a strong negative stereotype of online fraud victims, in that they are perceived to be greedy, uneducated, of lower socioeconomic status and deserving of their victimisation.

➢ From your experience, do you believe that this perception is accurate?
➢ From your observations, do you believe that this perception is evident in your jurisdiction?
➢ How do you think we can overcome this perception?

Topic 3
Our own research indicates that there is a strong level of complacency in the community about their own vulnerability to online fraud. There is a pervasive attitude that “it will never happen to me... (or anyone that I know)”.

➢ From your experience, do you think that this attitude exists within your community?
➢ How do you think we can get individuals to acknowledge their own potential vulnerability without scaring them away from computers?
➢ How do you think we can get individuals to recognise that they may have family and friends who have been affected but won’t come forward?

Topic 4
Our own research indicates that victims of online fraud are not considered to be “victims” as they are seen to have contributed to their own circumstances (through compliance in sending money/details to criminals).

➢ From your observations, does this perception exist within your own community?
➢ How do you think we can overcome the attribution of guilt placed on victims of online fraud, who have been deceived into handing over money/details to criminals?

Topic 5
From our research, it is evident that society generally only talks about online fraud in a negative and demeaning way, referring to the greed and stupidity of people who fall victim.

➢ From your observations and experience, in what context do people talk about online fraud?
➢ How can we encourage people to talk about online fraud in a more constructive and positive manner?
➢ How can we more effectively promote an environment whereby victims feel comfortable and confident in talking about their experiences to family/friends and enforcement agencies?
Preventing Online Fraud

Topic 6
From our research, it appears to be difficult to tailor a general crime prevention message around online fraud prevention, when the circumstances are generally complex and somewhat unique.

- What key crime prevention messages have you or your agency promoted around the topic of online fraud prevention?
- How effective do you think these have been?
- What key crime prevention messages have you witnessed from other agencies around online fraud prevention?
- How effective do you think these have been?
- What are the key messages that you think need to be promoted to prevent online fraud victimisation?
- Through what mediums do you think these messages would be most effective?
- Which agency/group do you think is best placed to promote these messages of online fraud prevention?
- How can we improve the crime prevention messages that are promoted through the media regarding online fraud?

Topic 7
Within Queensland, there are a number of prevention activities which are being undertaken to reduce the likelihood of online fraud victimisation and prevent it from occurring in the first place (for example, brochures, seminars, cartoons).

- What types of prevention activities have you/your agency undertaken regarding online fraud?
- How were these targeted?
- How were they implemented?
- What outcomes were achieved?
- Was any formal/informal evaluation conducted on their effectiveness?
- Do you have any future plans for prevention activities?
- What type of prevention activities do you think are most effective?
- How do you think we can more effectively target and implement our prevention activities?
- How do you think we can best measure the impact of any prevention activities undertaken?
- What model of crime prevention do you think would be the most effective in preventing online fraud victimisation?
Topic 8

Given the global nature of online fraud, it is unlikely that any one agency can effectively prevent victimisation from occurring, in any jurisdiction. Instead, collaborative partnerships are essential in working together to prevent online fraud.

- Have you/your agency been involved in a partnership or collaboration with another agency/group?
- How did that work in practice?
- What were the benefits and challenges of being involved with another agency/group?
- What were the outcomes of that collaboration?
- What lessons were learnt for future work?
- How do you think we can work more effectively with others to both prevent online fraud victimisation and support individuals who have already become victims?

Reporting of Online Fraud

Topic 9

Statistics indicate that the reporting of fraud offences overall is extremely low, but the reporting of online fraud victimisation is even lower.

- From your experience, do victims of online fraud report their victimisation to any agency?
- What do you think are the main barriers to victims reporting these crimes?
- How do you think we can try to overcome these barriers?
- What do you think would be the most effective model to implement in terms of reporting online fraud?

Topic 10

The majority of online fraud victims known to the Queensland Police Service have been identified through proactive operations targeting individuals sending money offshore. Of these individuals, many do not realise they are victims of online fraud until they receive a phone call from the police.

- From your experience, how do victims come to your attention?
- How do you think we can improve individuals recognising their involvement in online fraud?
- Given the lack of official statistics in this area, how do you think we can best measure work output of agencies regarding online fraud?
- What key performance indicators do you think would be useful?
**Topic 11**

Frequently, individuals who are experiencing online fraud victimisation deny that they are victims. They refuse to believe family, friends and even the police.

- From your experience, how do victims react when they realise that they have been involved in fraudulent activities?
- Have you had a circumstance where the victim refused to acknowledge the reality of their situation? What did you do?
- What was the outcome?
- How can we encourage third parties to play a more proactive role in situations involving online fraud victimisation?
- How can we increase the credibility of third parties to intervene in situations where victims are being defrauded?

**Topic 12**

From our own research, it is apparent that even when victims do come forward to police to report online fraud victimisation, they can sometimes be met with less than positive responses.

- What type of awareness do you think people working in your agency have regarding the experiences and needs of online fraud victims?
- How do you think we can improve the understanding of our own agencies to interact with online fraud victims?
- How do you think we can more effectively interact with victims of online fraud?
- What are the key messages around online fraud victims that we need to be promoting to members of our own agencies?

**Victim Support**

**Topic 13**

From our own research, there is a belief that online fraud victimisation results only in financial losses. However, many victims experience impacts far beyond the loss of money, such as emotional and psychological distress, deterioration of their physical health, relationship breakdown, and in extreme cases, suicide.

- From your own observations, what impact does the experience of online fraud have on its victims?
- From your observations, how do victims cope with the situations they find themselves in?
From our experience, many victims struggle to come to terms with what has happened to them, and many continue to struggle to get themselves back on track.

- What do you/your agency offer victims in terms of support once they realise they have become a victim of online fraud?
- Are there support services available outside of your agency for victims of online fraud?
- Do you know if victims access these support services?
- If so, do you think they find them beneficial?
- If not, what do you think if preventing them from accessing the services?
- What type of support services do you think would benefit victims of online fraud?
- Who do you think is in the best position to provide these services?
- What model of victim support do you think would be the most effective?
- How would you evaluate the benefits of any support services implemented?

Currently in Queensland, compensation and referrals to victim support services are exclusively for victims of violent crime (under legislative constraints). This means that victims of online fraud are not able to access these services.

- Within your jurisdiction, how are victims defined under legislation?
- Are there constraints against victims of non-violent crimes?
- Do you think that legislation can be used in a constructive way to improve the accessibility of support services to fraud victims?
- If so, what would this look like?
- Do you think that any regulatory mechanisms can/should be used to improve the accessibility of support services to fraud victims?

Enforcement

Enforcement action regarding online fraud is incredibly difficult and complex and generally unsuccessful.

- What enforcement action have you/your agency been involved with?
- What were the challenges/barriers that were faced?
- How were these overcome?
- What was the outcome?
- Any success stories?
- Is there anything that you would do differently in the future?
Topic 17
From our experience, victims of online fraud often have unrealistic expectations surrounding the abilities of police to take enforcement and preventative action regarding online fraud. There appears to be the expectation that police have the same capabilities and resources as criminals and therefore should be able to track them down, arrest and prosecute with ease.

- How do you/your agency manage expectations from online fraud victims about the capabilities of you/your agency to handle their case?
- How do you/your agency explain the challenges and intricacies of online fraud to those who have experienced online fraud victimisation?
- How do you think we can improve a victim’s understanding about the reality of the situation and what realistically can/can’t be achieved?

Information Sources regarding Online Fraud

Topic 18
From our own research, victims and non-victims alike, report a frustration in not having a single point of information regarding online fraud. Rather, information appears to be spread across a number of agencies and sites.

- How does your jurisdiction approach the provision of information?
- Is there a single point of information (or a preferred point of information) in your community regarding online fraud?
- If so, how does this operate? Who maintains it?
- If not, do you think this would be beneficial?
- Who should have overall responsibility?

Topic 19
The same argument exists in terms of contacting someone with questions about online fraud. Victims express frustration and anger at being passed from one agency to another, with no resolution in some cases. Non-victims also report being passed through many people and agencies if they have a query about potential online fraud.

- How do you/your agency respond to victims reporting online fraud?
- How do you/your agency respond to non-victims who have a query about potential online fraud?
- How do you think we can better manage these processes?
- Who do you think would be the best point of contact to deal with victimisation matters?
- Who do you think would be the best point of contact to deal with questions from non-victims?
- How do you think we can resolve the “merry-go-round” that many individuals experience in trying to contact an agency on the topic of online fraud?
- Do you think there is merit in one central reporting agency?
- If so, which agency would that be?
- How would it work with other relevant agencies?
Topic 20
Over the past number of years, the media in Queensland have taken a greater interest in stories relating to online fraud victimisation and generally portray these in a positive and constructive manner.

➢ What are your experiences with the media in relation to online fraud?
➢ Currently, do you think the media help or hinder promoting an increased awareness of online fraud?
➢ Do you have any positive/negative examples of interaction with the media?
➢ How do you think we can better engage the media to contribute to a positive and constructive dialogue around online fraud victimisation?

*******

If there is any other topic you think is relevant or important to consider in this area, please let me know. These topics are not exhaustive and are designed to start discussion on some of the most pressing topics of interest in the area of online fraud prevention and victim support.

*******

Thank you for your participation in discussions surrounding online fraud prevention and victim support. It is envisaged that your expertise and valuable insight into this area will help to improve the capability of the Queensland Police Service to deliver more effective crime prevention messages/activities regarding online fraud, as well as better support those who have become victims.

If you have any further questions or ideas, please do not hesitate to contact me:

Dr Cassandra Cross
Community Safety and Crime Prevention Branch
Queensland Police Service
Cross.CassandraA@police.qld.gov.au (work email)
c.cross@y7mail.com (email while I am overseas 13/10/11 – 09/12/11)