The use of financial intelligence as a prevention tool to target online fraud victimisation

Dr Cassandra Cross
School of Justice
Queensland University of Technology
@DrCassCross
Acknowledgements
Acknowledgements


• All views presented in this presentation are my own and do not necessarily reflect those of other agencies.
Today’s presentation

• Provides background and context to the problem of online fraud
• Documents previous research in this area
• Details the emergence of using financial intelligence to target online fraud victims
• Locates this within a crime prevention framework
  – Tertiary, victim-oriented prevention
• Concludes with overall benefits of this approach
Definition of online fraud

• “The experience of an individual who has responded through the use of the internet to a dishonest invitation, request, notification or offer by providing personal information or money that has led to a financial or non-financial loss of some kind” (Cross, Smith and Richards, 2014)
Types of online fraud

• There are an infinite number of approaches that offenders can take to defraud a potential victim (Cross and Kelly, 2016)

• Two most relevant types for this project
  – Advanced fee fraud: a person is asked to send a small amount of money in promise of a larger return (Ross and Smith, 2011)
  – Romance fraud: A person is defrauded under the guise of a legitimate relationship (Rege, 2009)
What we know...

• Fraud has a low reporting rate, online fraud even lower (Button et al. 2014; Copes et al. 2001; Smith 2007; 2008; van Wyk and Mason 2001)

• Victims have great difficulty in seeking to access the “fraud justice network” (Button et al. 2014)

• Large degree of shame and stigma associated with victimisation – strong attitude of victim blaming (Cross, 2015)

• The impact of fraud is far greater than pure financial losses and extends to physical health, emotional wellbeing, relationships, unemployment, homelessness and suicide (Button et al. 2009; Cross et al. 2014)

• Fraud is not generally a priority of policing agencies (Button, 2012; Doig, Johnson and Levi, 2001; Frimpong and Baker, 2007; Gannon and Doig, 2010)
Crime prevention

• Defined as “any action designed to reduce the actual level of crime and/or perceived fear of crime” (Lab, 2013: 27)

• Brantingham and Faust (1976) proposed the primary/secondary/tertiary model

• Further refined by van Dijk and de Waard (1991) to focus on offenders, victims or situations
Crime prevention

- Tertiary prevention centres on individuals who have already offended or been victimised and aims to prevent revictimisation.

<table>
<thead>
<tr>
<th></th>
<th>Offenders</th>
<th>Victims</th>
<th>Situations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tertiary</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Emergence of proactive approaches

• Within Australia, there has been a growing recognition on the value of financial intelligence and how it can be used to target fraud victims (Cross and Blackshaw, 2015)

• It overcomes two main barriers:
  – Victims not recognising that they are involved in fraudulent activity
  – The social stigma in reporting fraud to authorities
Case studies

• The following presents results from three Australian examples to illustrate the benefits of this approach:
  – WA: Project Sunbird (Partnership between West Australian Police and Department of Commerce)
  – SA: Operation Disrepair (South Australian Police)
  – Australian Competition and Consumer Commission: Scam Disruption Project (NSW/ACT)
Project Sunbird

- Coordinated approach between West Australian Police (WAPOL) and West Australian Department of Commerce (Commerce)
- Targets individuals sending money to Nigeria, Ghana, Togo, Benin and Sierra Leone
- Five stages which are clearly divided between the two agencies
  - Identification (WAPOL)
  - Intervention (Commerce)
  - Interruption (Commerce)
  - Intelligence (WAPOL and Commerce)
  - Investigation (WAPOL)
Five stages of Project Sunbird

1. Identification
   – Using financial intelligence to identify victims

2. Intervention
   – Sending a letter to potential victims (1\text{st} and 2\text{nd} letters)

3. Interruption
   – Liaising with banks/remittance agencies to shut accounts

4. Intelligence
   – Using information for investigations

5. Investigation
   – Arrest and prosecution where possible
Operation Disrepair

- Exclusively led by South Australian Police
- Based on the Project Sunbird model
- Focuses on transactions to Nigeria and Ghana
- Sends out letters to potential victims (1st and 2nd letters)
  - May also initiate personal visits
Scam Disruption Project

• Exclusively led by ACCC
• Based on the Project Sunbird model
• Focuses on transactions to Nigeria and Ghana
• Sends out letters to potential victims (1st and 2nd letters)
  – 1st letter is standard, 2nd letter is personal
  – No face to face intervention
• Liaises with local police where necessary
Preventing revictimisation

Sending activity of individuals after receiving a first letter
(Project Sunbird, unpublished date file)
Preventing revictimisation

Sending activity of individuals after receiving a second letter

(Project Sunbird, unpublished date file)
### Summary of average amount sent per individual

(March 2013 - July 2015)

<table>
<thead>
<tr>
<th>Action after letter</th>
<th>1\textsuperscript{st} letter</th>
<th>2\textsuperscript{nd} letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ceased transactions</td>
<td>$2,554.35</td>
<td>$5,991.62</td>
</tr>
<tr>
<td>Decreased amount sent</td>
<td>$10,052.87</td>
<td>$18,439.53</td>
</tr>
<tr>
<td>Increased amount sent</td>
<td>$15,531.25</td>
<td>$22,055.79</td>
</tr>
<tr>
<td>All persons</td>
<td>$5,331.57</td>
<td>$12,787.08</td>
</tr>
</tbody>
</table>

Average amount of money sent by Project Sunbird letter recipients, 2013-2015 (Project Sunbird, unpublished data file)
Early intervention

Number of recurring months that individuals have remitted funds (Operation Disrepair, unpublished data file)
Limitations of this approach

• At the moment, this proactive approach is restricted to a narrow list of West African countries
  – Anecdotally victims are sending money across the globe (Asia, UK and other European countries)
  – Victims may continue to send money to other countries and this would be unknown
  – Is there a displacement effect?
  – Timeframes of victim follow up are varied and quite short

• It is clearly more effective as an early intervention approach and not appropriate for chronic or long term victims
In conclusion...

• Online fraud continues to pose unique challenges for prevention efforts

• A targeted, victim oriented approach appears to be having a positive impact
  – Reduction in victimisation timeframes as well as amount being sent
  – Appears to be more effective as an early intervention tool

• Need for further research to determine a more accurate assessment of effectiveness
Contact

Dr Cassandra Cross
Email: ca.cross@qut.edu.au

@DrCassCross