



Australian Government  
Australian Institute of Criminology



# Serious and Organised Investment Fraud in Australia



**INVESTIGATE**  
before investing

**Correspondence should be addressed to:**

Chief Executive Officer  
Australian Crime Commission  
PO Box 1936 Canberra City  
ACT 2601

**Telephone:**

02 6243 6666 (from within Australia)  
61 2 6243 6666 (international)

**Facsimile:**

02 6243 6687 (from within Australia)  
61 2 6243 6687 (international)

**Published July 2012**

The information contained in this report is produced by the Australian Crime Commission (ACC) and the Australian Institute of Criminology (AIC).

© Commonwealth of Australia 2012.

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without written permission from the Chief Executive Officer, Australian Crime Commission.



## KEY JUDGEMENTS

- Serious and Organised Investment Fraud refers to the solicitation of investment in non-existent or essentially worthless shares and other securities.
- Financial analysis of Serious and Organised Investment Fraud activity in Australia between January 2007 and April 2012 estimates losses to be in excess of A\$113million, with this figure likely to be conservative.
- Serious and Organised Investment Fraud is not an opportunistic crime, but a calculated, sophisticated, organised criminal event that can attract experienced investors, with many individuals being re- victimised.
- As a prevention measure, law enforcement and regulatory agencies both nationally and internationally highlight that checking a number of sources before investing is essential to ensure the legitimacy of the investment.
- Always seek independent financial advice before making an investment.
- Check that any company you are discussing investments with has a valid Australian Financial Services Licence at [www.moneysmart.gov.au](http://www.moneysmart.gov.au).
- It is also recommended that the following is undertaken if you believe you have come across an investment fraud:
  - Visit [www.moneysmart.gov.au](http://www.moneysmart.gov.au) or call 1300 300 630 for further information.
  - Alert your family and friends to the fraud, especially anyone who may have savings to invest.
  - Report suspected fraud to the Australian Securities and Investments Commission, via [www.moneysmart.gov.au](http://www.moneysmart.gov.au) or 1300 300 630, or your local police. Any information that can be provided such as the company name, location and contact details will assist with subsequent investigations and enquiries.
  - Hang up on unsolicited telephone calls offering overseas investments.

# CONTENTS

KEY JUDGEMENTS	1
ACRONYMS	3
AIM	4
OVERVIEW	5
 <b>INTRODUCTION</b>	 <b>6</b>
Overview of Task Force Galilee	6
 <b>SECTION 1: CHARACTERISTICS OF SERIOUS AND ORGANISED INVESTMENT FRAUD</b>	 <b>8</b>
What is it?	8
Conjunction of criminal opportunities - factors exploited by Serious and Organised Investment Fraud operations	12
The complex and evolving nature of Serious and Organised Investment Fraud operations	14
 <b>SECTION 2: WHO IS TARGETED BY SERIOUS AND ORGANISED INVESTMENT FRAUD?</b>	 <b>18</b>
Victim selection: demographics and characteristics	18
Method of access to potential victims	25
 <b>SECTION 3: CURRENT RESPONSES TO SERIOUS AND ORGANISED INVESTMENT FRAUD IN AUSTRALIA</b>	 <b>28</b>
Australia’s legal framework for addressing Serious and Organised Investment Fraud	28
Task Force Galilee	29
Australian agencies that contribute to the prevention and detection of Serious and Organised Investment Fraud	32
International response	36
Summary	37
 <b>REFERENCES</b>	 <b>39</b>
<b>FURTHER INFORMATION</b>	<b>40</b>



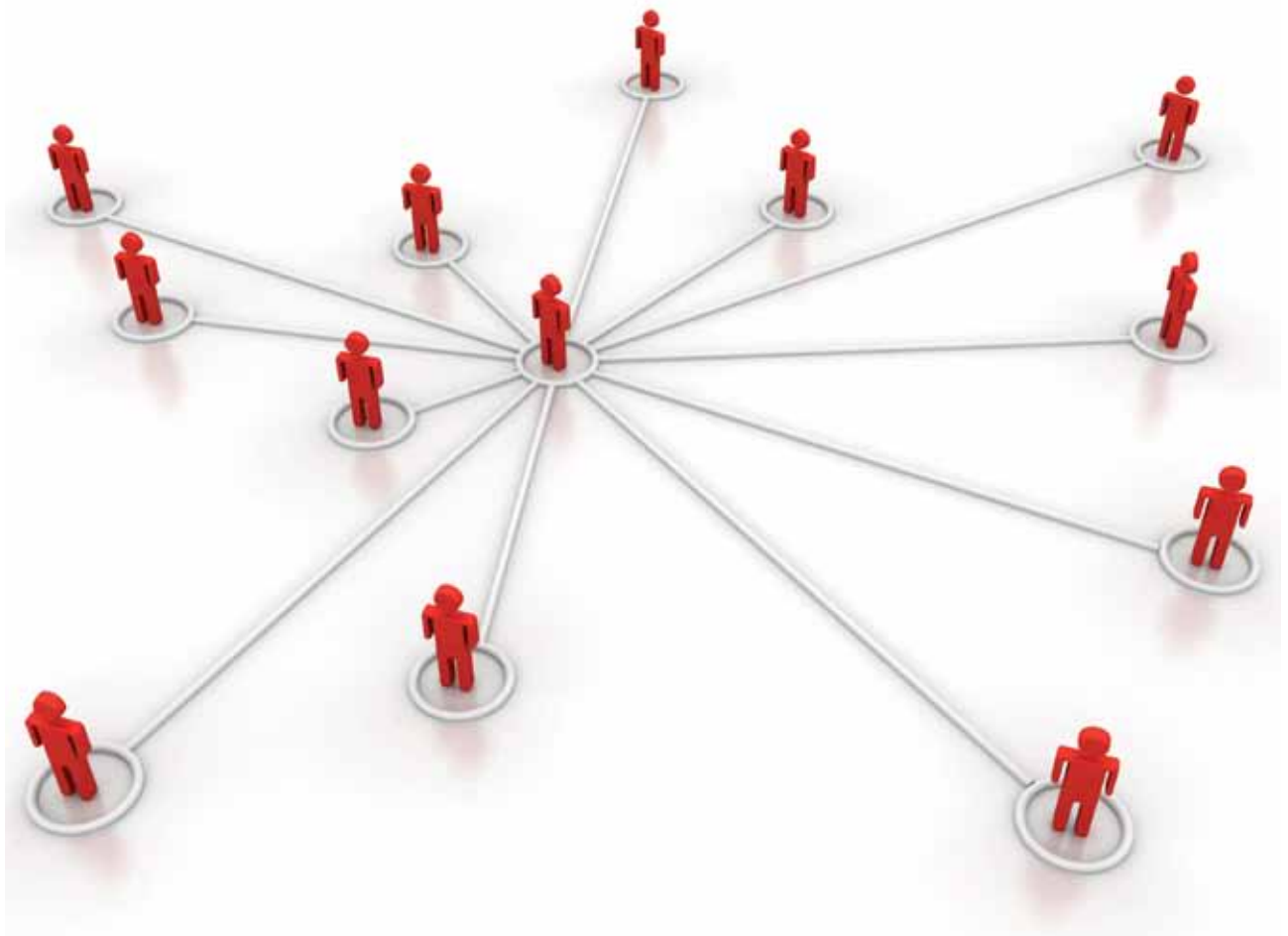


# ACRONYMS

ABS	Australian Bureau of Statistics
ACFT	Australian Consumer Fraud Taskforce
ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
ACCC	Australian Competition and Consumer Commission
ACFT	Australasian Consumer Fraud Taskforce
ACMA	Australian Communications and Media Authority
AFF	Advanced Fee Fraud
AFP	Australian Federal Police
AGD	Attorney-General's Department
AIC	Australian Institute of Criminology
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
AUSTRAC	Australian Transactions Report and Analysis Centre
CCO	Conjunction of Criminal Opportunity
DIAC	Department of Immigration and Citizenship
DBCDE	Department of Broadband, Communications and the Digital Economy
FBI	Federal Bureau of Investigation
FSA	Financials Services Authority (UK)
GFC	Global Financial Crisis
HKP	Hong Kong Police
ICPEN	International Consumer Protection Enforcement Network
IFWG	International Fraud Working Group
POP	Problem Oriented Policing
SAPOL	South Australia Police
SCRT	Serious Crime Research Team
SOCA	Serious Organised Crime Agency (UK)
UK	United Kingdom
VoIP	Voice over Internet Protocol

# AIM

This report provides an insight into Serious and Organised Investment Fraud<sup>1</sup> currently affecting Australia. The insights contained in this report are based on the consolidation of open source information which is informed by intelligence collected under Task Force Galilee. Detail on the role, function and membership of Task Force Galilee can be found in the 'Overview' of this report on page 5.



<sup>1</sup> Serious and Organised Investment Fraud is also colloquially referred to as 'boiler-room' fraud.



# OVERVIEW

In 2011, Task Force Galilee<sup>2</sup> was established to broaden the understanding of Serious and Organised Investment Fraud and to develop a national response. As at April 2012, the Task Force estimated that Australians' losses to this type of fraud since January 2007 were in excess of A\$113 million, with this figure likely to be conservative. During this period more than 2,600 Australians were victims of Serious and Organised Investment Fraud. These figures have largely been established as a result of intelligence analysis, and do not reflect the actual level of reporting by victims, which remains low.

This report has been prepared to provide an insight into the nature and extent of this type of fraud as it currently affects Australia. Since the Task Force's establishment, knowledge and understanding of Serious and Organised Investment Fraud has grown exponentially, and continues to do so. The information in this report is a compilation of the key characteristics identified via available literature and relevant Task Force member findings. The research and assistance of the Australian Institute of Criminology (AIC) is also acknowledged.

This report uses the definition of Serious and Organised Investment Fraud which has been adopted by Task Force Galilee. This Task Force defines it as:

- a) *any unsolicited contact, by telephone or internet, of persons in Australia (potential investors) by persons (callers) usually located overseas, where such callers engage in conduct that is fraudulent, false, misleading or deceptive with the purpose of inducing potential investors to buy, sell, or retain securities or other investments and where such callers do not have the license or authority to engage in a securities business, or investment advice business in Australia; and*
- b) *may include superannuation and investment fraud.*

The report is divided into three sections:

- Section 1: Characteristics of Serious and Organised Investment Fraud
- Section 2: Who is targeted by Serious and Organised Investment Fraud?
- Section 3: Current responses to Serious and Organised Investment Fraud

<sup>2</sup> The Task Force comprises law enforcement, regulatory and service delivery agencies across federal, state and territory government. Task Force members include all ACC Board agencies, as well as the Australian Competition and Consumer Commission, the Department of Broadband, Communications and the Digital Economy, the Department of Immigration and Citizenship, the Department of Human Services and the Australian Transaction Reports and Analysis Centre. Australian Crime Commission Board (ACC Board) 2011, *Protect your retirement savings—Australian Crime Commission Board warns of investment scams targeting Australians*, Australian Crime Commission Board media release 28 September 2011, <http://www.crimecommission.gov.au/media/protect-your-retirement-savings%E2%80%9494australian-crime-commission-board-warns-investment-scams-tar-0>

# INTRODUCTION

Serious and Organised Investment Fraud involves the solicitation of investment in non-existent or essentially worthless shares and other securities. As found in 2002,<sup>3</sup> Australia continues to be recognised as an attractive location for Serious and Organised Investment Fraud operations. This is attributed to the continuing strength of Australia's economy, the overall level of wealth of individuals and interest in investing<sup>4</sup> as well as the high level of superannuation and retirement savings that Australians can access for investing.<sup>5</sup>

## OVERVIEW OF TASK FORCE GALILEE

Task Force Galilee is a multi-agency Task Force, established in April 2011. The Task Force is focused on combating and preventing Serious and Organised Investment Fraud targeting the Australian community. The Task Force is comprised of 19 agencies from across the Commonwealth, states and territories, working together with industry groups, including financial institutions.

The primary objectives of the Task Force are to:

- develop and implement immediate crime prevention and disruption strategies
- identify opportunities to enhance community resilience to, and create a hostile environment for, the operation of Serious and Organised Investment Fraud
- develop a model for enhanced co-ordination between law enforcement, regulatory agencies and private industry for ongoing disruption and prevention of Serious and Organised Investment Fraud.

3 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC.

4 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC.

5 Australian Crime Commission Board (ACC Board) 2011, *Protect your retirement savings—Australian Crime Commission Board warns of investment scams targeting Australians*. Australian Crime Commission Board media release 28 September 2011, <http://www.crimecommission.gov.au/media/protect-your-retirement-savings%E2%80%94australian-crime-commission-board-warns-investment-scams-tar-0>





The Task Force is co-ordinated by the Australian Crime Commission (ACC) and operates in partnership with the:

- Australian Securities and Investments Commission (ASIC)
- Australian Competition and Consumer Commission (ACCC)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Communications and Media Authority (ACMA)
- Australian Security Intelligence Organisation (ASIO)
- Attorney-General's Department (AGD)
- Department of Immigration and Citizenship (DIAC)
- Australian Taxation Office (ATO)
- Australian Customs and Border Protection Service (ACBPS)
- Department of Human Services (DHS), Centrelink
- Department of Broadband, Communications and the Digital Economy (DBCDE)
- Federal, state and territory police agencies.

Task Force Galilee has also consulted with the superannuation and financial sectors as a move towards strategic collaboration in the long term development of national prevention strategies focusing on Serious and Organised Investment Fraud.

This focus is being made in an environment where there is limited information, both nationally and internationally, identifying proven good practice strategies in the prevention and disruption of Serious and Organised Investment Fraud. This is a challenging environment within which law enforcement and regulatory agencies are working to identify and implement proven and successful interventions to address this crime.



# SECTION 1

## CHARACTERISTICS OF SERIOUS AND ORGANISED INVESTMENT FRAUD

### WHAT IS IT?

Serious and Organised Investment Fraud (or ‘boiler room frauds’ as they are referred to in some jurisdictions) use sophisticated techniques to solicit investment in non-existent or essentially worthless shares and other securities. The frauds are well organised and convincing,<sup>6</sup> with constantly evolving modus operandi.<sup>7</sup> They generally operate from an overseas location; however recent investigations have identified operations based in Australia.<sup>8</sup> Combined, these factors contribute to their ability to evade detection. These characteristics also reflect those of frauds in general,<sup>9</sup> and can be attributed to offenders adapting their methods once the investment is recognised as a fraud and/or is not generating the same return as it has in the past.

Serious and Organised Investment Fraud tactics are considered sophisticated, complex and very effective. They are difficult to identify—even for experienced investors—and are usually initiated by cold-calling potential victims using persuasive techniques that are fraudulent, misleading and deceptive for the purposes of inducing victims to purchase investments.<sup>10</sup> Some Serious and Organised Investment Fraud operators have also been identified operating ‘recovery rooms.’<sup>11</sup> Once investors have realised they have invested in fraudulent or worthless shares a second arm of the operation ‘the recovery room’ makes contact with victims and attempts to convince them that for a ‘fee’ they can assist recovery of some of the investment. Recovery is, of course, futile.

- 6 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf), accessed 12 January 2012.
- 7 Australian Securities and Investments Commission (ASIC) 2002a, *Hook, line & sinker: Who takes the bait in cold calling scams?* Canberra: ASIC [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/HookLineSinker.pdf/\\$file/HookLineSinker.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/HookLineSinker.pdf/$file/HookLineSinker.pdf), accessed 12 January 2012.
- 8 Australian Crime Commission, Australian Securities and Investment Commission and Queensland Police, *Serious and organised investment scam disrupted on Gold Coast*, 13 December 2011 <http://www.crimecommission.gov.au/media/serious-and-organised-investment-scam-disrupted-gold-coast>, accessed 12 January 2012.
- 9 Budd, C & Anderson, J 2011, *Consumer fraud in Australasia: Results of the Australasian Consumer Fraud Taskforce online Australia surveys 2008 and 2009*, Technical and Background Paper no. 43, Canberra: Australian Institute of Criminology <http://www.aic.gov.au/publications/current%20series/tbp/41-60/tbp043.aspx>, accessed 12 January 2012.
- 10 Australian Crime Commission, 2012, *Submission to the Department of Prime Minister and Cabinet, The Cyber White paper: Connecting with Confidence*, p. 17, [http://cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066\\_-\\_australian\\_crime\\_commission\\_acc\\_submission.pdf](http://cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066_-_australian_crime_commission_acc_submission.pdf), accessed 4 April 2012.
- 11 City of London Police, *Boiler Room Fraud* <http://www.cityoflondon.police.uk/CityPolice/Departments/ECD/Fraud/boilerroom.htm>, accessed 12 January 2012.





Changes in social, economic, political or environmental contexts can provide opportunities to conduct investment and Serious and Organised Investment Fraud. For example, financial downturns can offer offenders opportunities to develop new investment fraud types.<sup>12</sup> In August 2011, it was reported that the high price of gold was being used to lure investors to invest in ‘mining companies’ that allegedly have high gold reserves, and thus are a lucrative investment in light of the current market downturn.<sup>13</sup> Fraudsters have also been identified as extending their focus beyond company shares to the following:

- green energy investments
- new technology shares
- loans to fund new investments
- selling and misrepresenting products
- illicit lotteries and sweepstakes
- advanced-fee loan and credit offers
- mortgage or real estate ‘investments’
- ‘high-return’ schemes
- option trading
- foreign currency trading.<sup>14</sup>



Serious and Organised Investment Fraud operators targeting Australians have also been identified as manipulating the market or selling shares in a business that is legitimate, but usually misrepresenting the high risk, illiquid nature of the business.<sup>15</sup> These are often ‘unproven start-up operations seeking venture capital in order to establish themselves.’<sup>16</sup>

12 Levi, M and Smith, R G, 2011, ‘Fraud vulnerabilities and the global financial crisis,’ in *Trends and issues in Crime and Criminal Justice*, No. 422, Australian Institute of Criminology, Canberra.

13 Mining company stock values are often measured in the amount of gold reserves, which are difficult to both estimate and verify (Fitzgerald D 2011, Fools gold: Offenders rush to cash in on metal’s surging price, *The Australian*, 26 August).

14 City of London Police, *Boiler room fraud*, <http://www.cityoflondon.police.uk/CityPolice/Departments/ECD/Fraud/boilerroom.htm>, accessed April 2012 and “Ring-Ring Overseas ‘Boiler Room’ Telemarketing Fraud Calling”, Joel Z 10 July 2009 <http://blogs.findlaw.com/courtside/2009/07/ring-ring-boiler-room-telemarketing-lottery-fraud-calling.html>, accessed April 2012; International Mass-Marketing Fraud Working Group. 2010, *Mass-Marketing Fraud: A Threat Assessment*, International Mass-Marketing Fraud Working Group, <http://www.fbi.gov/stats-services/publications/mass-marketing-fraud-threat-assessment>, accessed 10 April 2012. June 2010, <http://www.ice.gov/doclib/cornerstone/pdf/immfta.pdf>, accessed 3 April 2012; and <http://www.scamwatch.gov.au/content/index.phtml/tag/ColdCalling>, accessed 4 April 2012.

15 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf), accessed 13 January 2012.

16 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf), accessed 13 January 2012, p 26.

## CASE STUDY 1

### VICTIM OF SERIOUS AND ORGANISED INVESTMENT FRAUD

**Christopher Fulton\***

**Age: 48**

**Lives: Northern Territory**

**Occupation: Carpenter**

Christopher Fulton\* had a plan.

The married father of six was going to put his money into the share market, buy an investment property and set his family up for life.

He also had dreams of retiring early and taking his wife on a holiday.

But that all changed two years ago when the family's entire savings were lost to organised crime.

Mr Fulton said it all started when he was contacted by a cold-caller offering him a unique investment opportunity.

"I had been looking around for different opportunities to get ahead and then a man claiming to be from a company called Dachser Global Markets started calling me," he said.

"This went on for a couple of months, and at the start I didn't do anything about it."

Mr Fulton said that around the same time that he had been receiving the phone calls, he had attended a business seminar where he learnt about the share market and other investment opportunities.

He said he researched Dachser Global Markets online, spoke to his wife about the investment and eventually decided to give it a go.

"At first we put in \$5000," Mr Fulton said.

"When I looked on their website I could see my investment trading, it was starting to go up."

Mr Fulton and his wife then went to the bank and took out a \$40,000 line of credit against their house.

"I don't know why I didn't wake up to it then because Dachser Global Markets were saying 'don't worry about this bit of paperwork, we'll take care of it' or 'we'll deal with that part of the process later'."



But Mr Fulton said the company's website and the sound advice he was receiving via email and over the phone meant any concerns were pushed aside.

"I've now come to realise that anybody who rings you up and says they can help you make money can't be trusted," Mr Fulton said.

"Everyone used to say that to me, but at the time I thought they were legitimate, their communication lines were professional they must be legitimate.

"I guess I just got blinded by the thought of the money we were going to make and what we could do with it."

Mr Fulton said he started to realise something wasn't right when the company kept pushing him to invest more money.

He said he refused and when he mentioned he was ready to take his money out the company cut all contact.

The fraud was reported to Northern Territory Police and the Australian Securities and Investments Commission.

But for Mr Fulton and his family, the hardship didn't end there.

Twelve months after realising he had lost more than \$40,000, Mr Fulton received another cold-call from a man claiming to be a lawyer in New York.

The man said he was working for a number of investment fraud victims and would be able to help Mr Fulton get his money back for a fee.

Mr Fulton later found out this man was also involved in serious and organised investment fraud and had been targeting victims in secondary scams with promises to help them recover the money they had lost.

Mr Fulton said this time he refused to give out any of his details over the phone.

"The whole thing caused a lot of stress and a lot of embarrassment," he said.

"It's been two years, but I still get reminded about how much money we owe.

"We now owe more money on the house than we did when we first moved in.

"It's hard to come to terms with losing that much money."

\*Name has been changed to protect the victim's identity

## CONJUNCTION OF CRIMINAL OPPORTUNITIES - FACTORS EXPLOITED BY SERIOUS AND ORGANISED INVESTMENT FRAUD OPERATIONS

Most fraudsters operate across the transnational and cyber environments. As indicated in the ACC's 2012 'Submission to the Department of Prime Minister and Cabinet, The Cyber White Paper: Connecting with Confidence' these sophisticated operators have been identified exploiting technology to develop what appear to be safe websites and environments and develop false websites providing potential victims with a sense that an investment opportunity is legitimate. Such practices suggest a high level of organisation.<sup>17</sup> There are also a host of peripheral individuals who may provide services to the operations indirectly that may be complicit or unwitting. These can include for example web designers to develop the website, accountants, lead list brokers, book keepers and lawyers.

Investment fraud, like most serious and organised crimes, is multifaceted and there are many interacting factors that allow a criminal event like investment fraud to occur. These factors include immediate opportunistic factors such as an available victim, difficulty in identifying the operation as a fraud and the access to potential victims. Table 1 provides an overview of factors that—when combined with one or more factors—can make investment and Serious and Organised Investment Fraud attractive to criminals. The list is not exhaustive and not all factors need to be present in order for the fraud to occur. Identifying these casual factors is important as they can be used to develop interventions to address investment and Serious and Organised Investment Fraud.



<sup>17</sup> Australian Crime Commission, 2012, *Submission to the Department of Prime Minister and Cabinet, The Cyber White paper: Connecting with Confidence*, p. 17, [http://cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066\\_-\\_australian\\_crime\\_commission\\_acc\\_submission.pdf](http://cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066_-_australian_crime_commission_acc_submission.pdf), p. 15, accessed 4 April 2012.





**TABLE 1: CONJUNCTION OF CRIMINAL OPPORTUNITIES THAT CAN MAKE INVESTMENT AND SERIOUS AND ORGANISED INVESTMENT FRAUD ATTRACTIVE TO OFFENDERS<sup>18</sup>**

Causal pathways of criminal events	Factors that can make investment and Serious and Organised Investment fraud easier to occur for each pathway listed* *not mutually exclusive
<b>Promoters (i.e. those who, via their actions, enable crime to occur either wittingly or unwittingly. AKA ‘enablers’)</b>	<ul style="list-style-type: none"> <li>• People willing to participate in the cold calling</li> <li>• Firms willing to be used to pass on funds even though its risk factors may indicate an investment fraud**</li> <li>• Lax business/investing practices</li> </ul>
<b>Preventers (‘capable guardians’) (i.e. those who have the capacity to be a deterrent)</b>	<ul style="list-style-type: none"> <li>• “Victim deserved it” mentality</li> <li>• Lax participation of industry agencies in monitoring frauds/ lack of awareness or information on the fraud</li> <li>• Not verifying investments</li> <li>• Law enforcement, regulatory and other agency lack of understanding of needs and experience of victims (exposing risk of re-victimisation and victim isolation)</li> <li>• Restrictions and limitations for coordination among key agencies <ul style="list-style-type: none"> <li>- National and international</li> <li>- Private and government agencies</li> </ul> </li> <li>• Underreporting of investment fraud by victims</li> <li>• Inability of vulnerable individuals to identify that a crime has been committed</li> </ul>
<b>Wider environment (environmental design, regulation and rules)</b>	<ul style="list-style-type: none"> <li>• Exploitation of the cyber environment: <ul style="list-style-type: none"> <li>- Computer/phone based: no borders</li> <li>- Transactions can happen remotely and immediately</li> <li>- Hard to secure—not a physical access issue such as burglary</li> <li>- Inadequate regulation/legislation</li> </ul> </li> </ul>
<b>Target enclosure (perimeter access and security to funds and victims)</b>	<ul style="list-style-type: none"> <li>• Access to name/phone numbers/other details</li> <li>• Account details/investments freely given by the investors</li> </ul>
<b>Target person or property</b>	<ul style="list-style-type: none"> <li>• Vulnerable citizens (e.g. seniors, retirees, those with money to invest, those desperate for a quick high return investment due to life or other circumstances)</li> </ul>

\*\* Maranzana, P & Finger, L 2011, London accountants in ‘boiler room’ scam, *Accountancy*, vol. 147(1409): 11-11, 1/3p.

<sup>18</sup> Ekblom, P 2010, *Crime Prevention, Security and Community Safety Using the 5Is Framework*, England: Palgrave MacMillan.

Causal pathways of criminal events	Factors that can make investment and Serious and Organised Investment fraud easier to occur for each pathway listed* *not mutually exclusive
<b>Offender presence in situation</b>	<ul style="list-style-type: none"> <li>• Easy access of offenders to telephones/internet</li> <li>• Accessibility of market leads lists (i.e. personal details of potential victims).</li> </ul>
<b>Anticipation of risk, effort, reward, conscience or provocation</b>	<ul style="list-style-type: none"> <li>• Low risk of getting caught</li> <li>• Transnational crime: hard to police</li> <li>• High financial returns for relatively low investment</li> </ul>
<b>Resources to commit crime</b>	<ul style="list-style-type: none"> <li>• Skills in falsifying documents/setting up bogus companies</li> <li>• Exploitation of available technology</li> <li>• Ability to convince investors of fraud</li> <li>• Using legitimate company names to attract investors (e.g. Octopus Investments 2010 in UK: see <a href="http://www.octopusinvestments.com/scamwarning.html">http://www.octopusinvestments.com/scamwarning.html</a>)</li> </ul>
<b>Resources to avoid crime</b>	<ul style="list-style-type: none"> <li>• Inability to identify an investment fraud (victims and unaware phone operators)</li> <li>• Inability to believe that someone is defrauding them</li> </ul>
<b>Readiness to offend (i.e. current life circumstances and other factors that could affect decision to offend)</b>	<ul style="list-style-type: none"> <li>• Well remunerated staff</li> <li>• Quick cash for little effort for staff and organisers</li> <li>• Some call centre operators may not know they are engaging in illegal activity</li> </ul>
<b>Criminality (i.e. predisposition to offend)</b>	<ul style="list-style-type: none"> <li>• Little is known of the factors present from early in a person's life that may influence whether an individual will engage in an investment fraud operation. However, as raised above, it is important to recognise that individuals may not know they are engaging in illegal activity</li> </ul>

## THE COMPLEX AND EVOLVING NATURE OF SERIOUS AND ORGANISED INVESTMENT FRAUD OPERATIONS

The effort and time invested in the planning and conduct of Serious and Organised Investment fraud activities indicate it is principally a well-planned and organised criminal activity. In addition, offenders typically dedicate a great deal of effort to convince an investor of their legitimacy with some strategies in place prior to placing the cold call. This includes:

- producing and using bogus prospectuses (hardcopies, internet-based, etc)<sup>19</sup>
- falsifying company details<sup>20</sup>
- sending paperwork to the investor<sup>21</sup>

19 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC [http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf) accessed 12 January 2012.

20 Australian Securities and Investments Commission (ASIC) 2002a, *Hook, line & sinker: Who takes the bait in cold calling scams?*, Canberra: ASIC [http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/HookLineSinker.pdf/\\$file/HookLineSinker.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/HookLineSinker.pdf/$file/HookLineSinker.pdf), accessed 12 January 2012.

21 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC <[http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf)>, accessed 12 January 2012.



- coordinating with complicit accountants and lawyers to launder the proceeds of the fraud, conceal the nature of the fraud and sometimes promote the fraud<sup>22</sup>
- contacting 'shareholders' to advise against other suspect companies, isolating themselves from any pending investigations and blaming regulators/law enforcement for 'victimising' their company<sup>23</sup>
- having country-specific scripts for cold callers<sup>24</sup>
- paying a dividend to convince the investor of the legitimacy of the organisation, and to often lure the investor to reinvest<sup>25</sup>
- remaining in constant contact with the victim, and trying to build a relationship<sup>26</sup>
- providing links to fraudulent international regulatory sites<sup>27</sup>
- engaging in misleading use of a complex series of websites to promote stocks
- creation of professional looking but false websites
- monitor and manipulate search engine results moving negative feedback down the list of results
- circumvent the prevention messaging and on-line feedback that has previously alerted potential victims that they are being scammed, and
- issuing account statements to reassure investors that their investments are safe.<sup>28</sup>

Serious and Organised Investment Fraud offenders quickly adapt and alter their modus operandi so they can continue operating and evade detection. For example, offenders have also been identified changing the 'script' (i.e. what the cold caller says to convince a potential investor to invest) and organisational details.

22 See for example BBC News 2010, *Lawyer banned for authorising boiler room adverts*, 13 May <http://www.bbc.co.uk/news/10114516>, accessed 5 April 2012.

23 Australian Securities and Investments Commission (ASIC) 2002a, *Hook, line & sinker: Who takes the bait in cold calling scams?*, Canberra: ASIC [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/HookLineSink.pdf/\\$file/HookLineSink.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/HookLineSink.pdf/$file/HookLineSink.pdf), accessed 12 January 2012.

24 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC. [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf), accessed 12 January 2012.

25 See for example O'Malley, N 2009, Warrant issued over \$1.5b alleged fraud, *Sydney Morning Herald* 5 November, <http://www.smh.com.au/national/warrant-issued-over-15b-alleged-fraud-20091105-hybh.html>, accessed 5 April 2012.

26 Financial Services Authority, 'Typical boiler room fraud victims loses 20,000 pounds warns FSA' 6 June 2006, <http://www.fsa.gov.uk/pages/Library/Communication/PR/2006/053.shtml>

27 Australian Securities and Investments Commission (ASIC) 2002a, *Hook, line & sinker: Who takes the bait in cold calling scams?*, ASIC: Canberra <[http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/HookLineSink.pdf/\\$file/HookLineSink.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/HookLineSink.pdf/$file/HookLineSink.pdf)>, accessed 12 January 2012;

Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14, ASIC: Canberra <[http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf)>, accessed 12 January 2012.

28 Australian Crime Commission, 2012, *Submission to the Department of Prime Minister and Cabinet, The Cyber White paper: Connecting with Confidence*, p. 17, [http://cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066\\_-\\_australian\\_crime\\_commission\\_acc\\_submission.pdf](http://cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066_-_australian_crime_commission_acc_submission.pdf), p. 15-17, accessed 4 April 2012.

Serious and organised investment fraud operators also exploit a broad range of technology to communicate with potential victims. The following is a compilation of some of the different methods used by operators to contact potential victims:

- Voice over Internet Protocol (VoIP)
- email
- phone, including mobile phones and SMS
- development of falsified internet sites with log-ins that allow the victims to track fake balances, and
- manipulation of search engines.

Serious and Organised Investment Fraud operations targeting Australians are generally based overseas. Many are Asian-based but are non-Asian run.<sup>29</sup> Reports also suggest that the cold callers generally have accents from English speaking countries such as Australia, England, Scotland, New Zealand and South Africa.<sup>30</sup> It is likely that attractive pay rates could lure English-speaking travelers and backpackers to become a telemarketer for the operation.<sup>31</sup>



The following extract from the ACC's submission to the Cyber White Paper details how some of these methods can be used to exploit and lure victims.

29 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC <[http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf)>, p.15, accessed 12 January 2012.

30 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC <[http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf)>, p.15, accessed 12 January 2012.

31 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC <[http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf)>, p.15, accessed 12 January 2012.





## HOW SERIOUS AND ORGANISED INVESTMENT FRAUD OPERATORS LURE AND MISLEAD VICTIMS

“Some criminal networks involved in Serious and Organised Investment Fraud use a complex series of false websites, providing potential victims with a sense that an investment opportunity is legitimate. By drawing upon professional expertise, the websites are not able to be identified as false by viewing alone. They monitor and manipulate the results of search engines by entering data. This results in moving any negative feedback chronologically down the list of results, with these entries, often located on the second or third page, not viewed by those researching the scam investment. Using Voice over the Internet Protocol (VoIP), they are able to disguise where they are located, with potential victims believing that they are in the country as purported in the fake website. To further perpetuate the deception, they use western tourists with English speaking backgrounds in the call centres that make contact with the victims.

The sophisticated operations circumvent the prevention messaging and on-line feedback that has previously alerted potential victims that they are being scammed. Increasingly victims are educated, computer literate and have undertaken preventative research that provides them with a sense of assurance.

The relatively minimal investment of establishing a credible-looking website allows networks to reinvent themselves or their scams quickly following detection.”\*

\* Australian Crime Commission 2011, *Australian Crime Commission: Submission to the Department of Prime Minister and Cabinet. The Cyber White Paper: Connecting with Confidence*. ACC Cyber crime white paper submission <[http://\\_cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066\\_-\\_australian\\_crime\\_commission\\_acc\\_submission.pdf](http://_cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066_-_australian_crime_commission_acc_submission.pdf)> , accessed 30 March 2012.

SECTION 2

# WHO IS TARGETED BY SERIOUS AND ORGANISED INVESTMENT FRAUD?

## VICTIM SELECTION: DEMOGRAPHICS AND CHARACTERISTICS

The identification of victim characteristics, opportunities for repeat victimisation and the methods used by Serious and Organised Investment Fraud operators to identify victims are areas of focus in the development of comprehensive support services, prevention and education strategies.

The high level of technological exploitation and sophistication of Serious and Organised Investment Fraud operations is considered one of the reasons that victims are often considered atypical (i.e. financially literate, highly educated) compared with other financial fraud victims. This technological ‘grooming’ of the potential investor combined with personal contact over weeks, even months, is used to convince victims of the legitimacy of the investment.

While Serious and Organised Investment Fraud victims share similar characteristics with other victims of fraud such as those presented in Table 2, further analysis of their characteristics suggest there are other emerging traits. However, similarities in victim characteristics across fraud types highlights an opportunity for agencies to work together in efforts to counter the broad range of investment and Serious and Organised Investment frauds.





**TABLE 2: IDENTIFIED RISK FACTORS OF FRAUD VICTIMISATION<sup>32</sup>**

Previous victimisation	Belonging to organisations	Retiring, or turning 65
Signing up for “free offers” and “prizes”	Buying things over the phone	An engagement, marriage, birth, graduation or death in the family
Entering contests or sweepstakes	Making purchases on the Internet	Moving
Being on catalogue mailing lists or “junk mail” lists	Registering with any sites or groups on the Internet	Purchasing a house, car or major appliance
Having a major medical treatment or operation	Buying stocks or bonds, or making some other investment	Requesting information about an advertisement
Giving to a charity	Buying insurance	

Australian law enforcement and regulatory agencies have similar views on typical characteristics of Serious and Organised Investment Fraud victims. The most likely individuals to be victims are:

- middle aged to older persons (often over 35 years old but usually over 50 years old)
- male
- small business owners
- self funded retirees
- individuals who have previously made investments in other companies and were considered ‘financially literate’
- victims who are on share holder registers
- socially isolated individuals—geographically or otherwise.

In addition, Australian victims have typically been assessed as ‘educated, computer literate and have undertaken preventative research that provides them with a sense of assurance.’<sup>33</sup> The following case study, provides an insight into one victim’s experience, and clearly demonstrates how convincing Serious and Organised Fraud organisers can be.

<sup>32</sup> Titus, RM & Gover, AR 2001, Personal fraud: The victims and scams in repeat victimisation, in Farrell G & Pease K (eds), *Crime prevention studies*, vol 12. Monsey, NY: Willow Tree Press: 138-139.

<sup>33</sup> Australian Crime Commission, 2012, *Submission to the Department of Prime Minister and Cabinet, The Cyber White paper: Connecting with Confidence*, p. 17, [http://cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066\\_-\\_australian\\_crime\\_commission\\_acc\\_submission.pdf](http://cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066_-_australian_crime_commission_acc_submission.pdf), p. 15-17, accessed 4 April 2012.

## CASE STUDY 2

### VICTIM OF SERIOUS AND ORGANISED INVESTMENT FRAUD

**Martin Harris\***

**Age: 44**

**Lives: Western suburbs of Sydney**

**Occupation: Public Servant (former financial advisor)**

After months of searching, Martin Harris\*, 44, thought he had found the perfect investment opportunity.

The company, based in New York, had previously worked with large investment houses and was looking to expand its services to a limited number of long-term investors.

Mr Harris, who was initially contacted by a cold-caller, thought the opportunity was perfect, but before he handed over his savings the former financial advisor wanted to be sure the company was legitimate.

"I used to work in finance so I've got quite a bit of experience in the industry and I didn't want to do business via cold-calling," Mr Harris said.

"I wanted to do my own due-diligence so I went to their website, checked out some articles and checked to see if they were on any hot lists or red lists."

The whole thing looked really good; I found them to be a clean-skinned company."

Mr Harris said he initially invested \$5000 and immediately saw the returns.

"Very rapidly, I started making good money," Mr Harris said.

"I spoke to my stockbroker Rick on the phone and we discussed strategies then I went off and did my due-diligence again."

Mr Harris then poured a further \$20,000 into the company.

"Again, we made a number of financial wins," he said.

"I was watching the stock market, reading the newspapers and watching the political scene and all of a sudden I had made \$160,000."

Then everything came crashing down.





Two of Mr Harris' friends heard about the scheme and decided to pool their savings and join the investment.

However, the credit union one of the men was using had a red alert on the investment company's nominated account.

Mr Harris's friend immediately contacted him and told him to phone the police. It was then that the elaborate scam became clear.

Mr Harris was told the scammers had been moving from state to state, stealing millions of dollars from unknowing victims.

"The police estimated the scammers had stolen millions of dollars from people in Adelaide alone," Mr Harris said.

"After I hung up the phone I tried calling the scammers, but I couldn't get through to them."

Fortunately, Mr Harris was able to recover the money his friends had invested. He was also able to recover \$25,000 which his father had lent him, but his initial \$25,000 was gone.

"For me \$25,000 is a lot of money," Mr Harris said.

"It was my life-savings, it was my deposit for my dream-house and now it's gone."

Mr Harris said if he had one message for potential investors it would be to never trust anyone offering investment advice over the phone.

"Secondly, never give anyone your money until you see their Australian Financial Services Licence and have checked it with the Australian Securities and Investments Commission (ASIC)," he said.

Mr Harris said he had asked to see the company's licence, but kept getting brushed off with promises they would send it to him. They never did.

"These guys were professionals. They had websites set up, email addresses set up and they understood the market."

"They knew exactly what they were talking about."

\*Not his real name.

While it has been suggested investment frauds seem to flourish in boom times and crash with downturns in the market,<sup>34</sup> it has also been highlighted that investors can be vulnerable to investment frauds after suffering major losses. Financial downturns like the two recent Global Financial Crises could facilitate this atypical behaviour. Therefore, monitoring potential shifts in the financial environment or changing social factors that might influence investor behaviour could be a key method when developing proactive disruption strategies.<sup>35</sup>

Internationally, investment fraud victims are often more financially resourced than persons who do not invest in fraudulent schemes.<sup>36</sup> A recent comparative study of fraud victims and non-victims in the US analysed the characteristics of investment fraud victims compared to victims of other fraud types<sup>37</sup> and non-victims. Investment fraud victims were found to be statistically more likely than the general population to be:<sup>38</sup>

- male (victims 87%; general population 47%)
- married (victims 64%; general population 56%)
- have college education or higher (victims 69%; general population= 42%)
- earn >US\$50,000 a year (victims=59%; general population=41%).<sup>39</sup>

US research has also indicated that investment fraud victims were statistically less likely than the general population to become upset about the potential for losing money.<sup>40</sup>

Investment fraud operations target victims across Australia. Most of the victims identified under Task Force Galilee come from New South Wales (n=724), Queensland (n=563), and Victoria (n= 534) (see Table 3). However this only records victims identified under the Task Force, and does not reflect unreported victims across each jurisdiction.

34 Stanford, RA, Cosmo, N & Nadel A 2009, 'Alleged Investment Scams: A Scorecard', *Business Week Online*; 2/18/2009, p9.

35 Levi, M and Smith, R G, 2011, 'Fraud vulnerabilities and the global financial crisis,' in *Trends and issues in Crime and Criminal Justice*, No. 422, Australian Institute of Criminology, Canberra.

36 NASD Investor Education Foundation 2006, *Fraud Study Final Report*, <http://www.sec.gov/news/press/extra/seniors/nasdfraudstudy051206.pdf>, accessed 29 March 2012; AARP Foundation, 2011, *National Fraud Victim Study* <http://www.aarp.org/money/scams-fraud/info-03-2011/fraud-victims-11.html>, accessed 29 March 2012.

37 These included lottery fraud victims, prescription drug/identity fraud victims and advance fee fraud victims. AARP Foundation, 2011, *National Fraud Victim Study* <http://www.aarp.org/money/scams-fraud/info-03-2011/fraud-victims-11.html> accessed 29 March 2012.

38 Total survey respondents n= 2,232; total victim respondents n=723; General population (i.e. non-victims) n=1509; investment fraud victims n=270. Note that victims were not randomly selected but were identified via law enforcement records. This can potentially influence the representativeness of the sample, and therefore the applicability of the findings to the broader population. For more information on the method and study see: AARP Foundation, 2011, *National Fraud Victim Study* <http://www.aarp.org/money/scams-fraud/info-03-2011/fraud-victims-11.html> (accessed 29 March 2012).

39 Chi square statistics were used. All p=0.000 with the exception of the 'married' variable, where p=.021. See *National Fraud Victim Study* <http://www.aarp.org/money/scams-fraud/info-03-2011/fraud-victims-11.html> for more information.

40 (p=.001). AARP Foundation, 2011, *National Fraud Victim Study* <http://www.aarp.org/money/scams-fraud/info-03-2011/fraud-victims-11.html> accessed 29 March 2012.



**TABLE 3: LOCATION OF VICTIMS OF SERIOUS AND ORGANISED INVESTMENT FRAUD**

Jurisdiction	Victim Numbers
New South Wales	724
Queensland	563
Victoria	534
Western Australia	496
South Australia	179
Tasmania	53
Australian Capital Territory	35
Northern Territory	51
Other (region not able to be identified)	48
<b>TOTAL</b>	<b>2,683</b>

A 2012 Task Force Galilee assessment has found that the average amount transferred by victims of Serious and Organised Investment Fraud was A\$18,174 (with a range in value between A\$9 and A\$1,293,390).<sup>41</sup> In 2002, ASIC found that the median (not average, but middle of the distribution of known fraudulent transfers) amount lost was A\$17,000 (with a range in value between A\$3,900 and A\$500,000).<sup>42</sup> Most of the monies sent to Serious and Organised Investment Fraud operations from the Australian victims surveyed by Task Force Galilee in 2011 were funded by their superannuation (n=20, 37%) and investment funds (n= 34; 63%). Analysis of serious and organised investment fraud in the United Kingdom showed most victims typically lost £20,000 each, with one loss totalling £1.2 million.<sup>43</sup>

During preliminary investigations, Task Force Galilee interviewed 54 (51 males, three females) Serious and Organised Investment Fraud victims from six Australian states and territories concerning their experiences.<sup>44</sup> Two main victim types were identified—trusting investors and entrepreneurial investors:

41 The average amount transferred is from a recent financial analysis undertaken by Taskforce Galilee on 183 bank accounts (linked to 165 company entities). (Task Force Galilee correspondence 7 March 2012).

42 N= 41. Australian Securities and Investments Commission (ASIC) 2002a, Hook, line & sinker: Who takes the bait in cold calling scams? Canberra: ASIC [http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/HookLineSink.pdf/\\$file/HookLineSink.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/HookLineSink.pdf/$file/HookLineSink.pdf) , accessed 12 January 2012, p18.

43 City of London Police, Boiler Room Fraud <http://www.cityoflondon.police.uk/CityPolice/Departments/ECD/Fraud/boilerroom.htm>, accessed 4 April 2012.

44 Note that this assessment is based on a non-random sample of identified boiler room fraud victims across Australia. Therefore, more research is required to determine if this observation is statistically significant in Australia, and whether it varies between the two different victim types.

- **Trusting investors:** '[these investors] are more likely to be influenced by the relationship developed with the caller and once a level of trust is developed and they perceive the caller to be honest, less thought and scrutiny will go into the substance of the message itself. A perceived trusting relationship with the caller would perpetuate ongoing payments and ignore future warnings.'
- **Entrepreneurial investors:** '[these investors] are more interested in the opportunities to make money, the deal. They understand that high returns equate with high risk, but as they have often had to take risks in their own businesses, they are prepared to do this for such high level investment opportunities.'

More research is needed to develop insights into characteristics that contribute to the involvement of investors in these schemes and the evolving modus operandi of Serious and Organised Investment Fraud operations.

Serious and Organised Investment Fraud operators can also target companies. One technique involves Serious and Organised Investment Fraud operations approaching companies with offers to sell shares on behalf of the company for a commission. In reality, shares might be sold at a rate much higher than the agreed price, exorbitant fees can be charged, and the offenders will take the profits and fee and vanish.<sup>45</sup> Another technique identified involves a Serious and Organised Investment Fraud operator approaching a small company which wishes to raise capital, offering to find them investors for a commission of the share price, then selling shares at inflated prices. This fraud may not be discovered until an investigation into the offence has commenced or an investor finds out their shares are not worth what they paid. This can result in reputation damage for unsuspecting businesses and prevent the company conducting business until the matter is resolved.<sup>46</sup> This suggests that fledgling companies or companies in need of investment could also be vulnerable to Serious and Organised Investment Fraud tactics. It also illustrates how offenders can adapt to target new victims and opportunities, as well as evolving their modus operandi.

<sup>45</sup> Jones, R & Walker 2009, Boiling point: targets and tricks of the boiler room fraudsters. 10 June. Available online: <http://www.inhouselawyer.co.uk/index.php/fraud-and-corporate-crime/7354-boiling-point-targets-and-tricks-of-the-boiler-room-fraudsters>, accessed 4 April 2012.

<sup>46</sup> Jones, R & Walker 2009, Boiling point: targets and tricks of the boiler room fraudsters. 10 June. Available online: <http://www.inhouselawyer.co.uk/index.php/fraud-and-corporate-crime/7354-boiling-point-targets-and-tricks-of-the-boiler-room-fraudsters>, accessed 4 April 2012.





Victims have been further exploited and are being used as facilitators to transfer funds on behalf of Serious and Organised Investment Fraud operators in an attempt by offenders to distance themselves from the transactions. This can include activities such as:

- 'collecting' wire transfers
- depositing cheques or shipping counterfeit cheques to other victims
- accepting deliveries of merchandise purchased with stolen credit cards
- forwarding funds and products overseas
- serving as business account agents for foreign companies.<sup>47</sup>

## METHOD OF ACCESS TO POTENTIAL VICTIMS

There are many ways that Serious and Organised Investment Fraud operations gain access to potential victims. In Australia, it is not uncommon for victims to be targeted on multiple occasions.

Repeat victimisation can either occur through the original offenders changing their identity and re-approaching the victim, or through lists of prior victims being shared and distributed among Serious and Organised Investment Fraud operators. Some investors have been targeted by the same Serious and Organised Investment Fraud operator, who changed their identity, and/or have been the victims of 'recovery room' fraud. Other victims have been approached by different Serious and Organised Investment Fraud operations as a result of being on a shared 'leads market list'.

Financial lists are treated as a valuable commodity among those involved in Serious and Organised Investment Fraud activities. Cases have been identified where individual telemarketers (cold callers) have stolen market lead lists from their employers to initiate 'rip and tear' rooms (where the telemarketer/cold caller operates the scam on their own) or to sell to competing fraud operations.

Analysis of the modus operandi of Serious and Organised Investment Fraud operations and the literature has identified a range of techniques used by operators to identify and contact potential victims. These strategies are outlined below, with all but one of these methods (fulfilment/distribution centres) being identified in Australia. These strategies include:

- *Internal company telephone lists*: these can be stolen from employers.<sup>48</sup>
- *Accessing the member lists of financial/credit ratings agencies.*

47 International Mass-Marketing Fraud Working Group 2010, *Mass-Marketing Fraud: A Threat Assessment*, International Mass-Marketing Fraud Working Group June 2010, <http://www.ice.gov/doclib/cornerstone/pdf/immfta.pdf>, p.22, accessed 3 April 2012.

48 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC [http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf), accessed 12 January 2012

- A ‘snowball’ scenario.<sup>49</sup> In this situation a victim refers the fraudulent ‘opportunity’ onto family and friends, or the victim passes on their details to offenders. This scenario results in a pool of investors being generated through word of mouth. It is possibly for this reason that Serious and Organised Investment Fraud offenders frequently pay dividends to victims as a means to both feign legitimacy and encourage investors to share this opportunity with friends and family. This method of accessing potential victims highlights the need for individuals not to rely solely on the advice and recommendations of family and friends but to conduct their own checks of potential investment opportunities through authorised regulatory agencies.
  - ‘Free lunch’ investment seminars<sup>50</sup>
  - *Public lists.* These include names and details extracted from public telephone directories and shareholder lists, trade journals, professional directories and newspapers.<sup>51</sup>
  - *Buying lists from legitimate companies in the leads brokerage industry:* ACC intelligence indicates that Serious and Organised Investment Fraud operators have also utilised the services of legitimate leads brokerage companies. An example of this is illustrated in Case Study 3.
  - *Buying lists from illegitimate leads brokers:* Also known as ‘sucker lists,’ Serious and Organised Investment Fraud operations can purchase leads lists from other illicit operations and criminal leads list brokers.<sup>52</sup> This includes selling victim bank account and credit card information, and contact details (phone number, addresses etc). It has also been observed that Serious and Organised Investment Fraud operators have utilised social networking sites to trade lists of victims as well as recruit accomplices.<sup>53</sup>

49 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf), accessed 12 January 2012.

50 e.g.; Fitzgerald D 2011, Fools gold: Offenders rush to cash in on metal’s surging price. *The Australian*, 26 August.; FINRA 2011, Investment alert: “Gold” Stocks—Some Investments Mine Your Pocketbook <http://www.finra.org/Investors/ProtectYourself/InvestorAlerts/FraudsAndScams/P124119>, accessed 20 March 2012.

51 Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf), accessed 12 January 2012.

52 International Mass-Marketing Fraud Working Group 2010, *Mass-Marketing Fraud: A Threat Assessment*, International Mass-Marketing Fraud Working Group June 2010, <http://www.ice.gov/doclib/cornerstone/pdf/immfta.pdf>, accessed 3 April 2012.

53 Criminal Intelligence Service Canada 2010, *2010 Report on Serious and Organized Crime*, [http://www.cisc.gc.ca/annual\\_reports/annual\\_report\\_2010/feature\\_focus1\\_2010\\_e.html](http://www.cisc.gc.ca/annual_reports/annual_report_2010/feature_focus1_2010_e.html), accessed 4 April 2012.

## CASE STUDY 3

### TRADE OF PERSONAL INFORMATION

The leads market specialises in on-selling personal data that has, or can be, refined to identify individuals who fall within a target group likely to be able, or to want to, purchase specific products. Often the personal data is obtained legitimately with the full consent of the individuals concerned from sources such as surveys or competitions. While the leads market is a legitimate industry in its own right, it is also a harvesting ground for organised criminal networks. Using the same methodology as the legitimate market, organised criminal networks purchase information to identify potential victims. In some cases one network may purchase, refine and on sell the information to another network. In others, they use the information to directly target the victims. Armed with information such as income, superannuation, mortgage and investment details of individuals, organised criminal networks are able to identify those most susceptible to particular schemes, such as Serious and Organised Investment Fraud. Just as legitimate business uses this information to increase sales rates; organised criminal networks are able to increase their illegal profits.\*

\* ACC 2011, Australian Crime Commission: *Submission to the Department of Prime Minister and Cabinet. The Cyber White Paper: Connecting with Confidence*, ACC Cyber crime white paper submission [http://\\_cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066\\_-\\_australian\\_crime\\_commission\\_acc\\_submission.pdf](http://_cyberwhitepaper.dpmc.gov.au/sites/default/files/public-submissions/066_-_australian_crime_commission_acc_submission.pdf) , accessed 30 March 2012.



# SECTION 3

## CURRENT RESPONSES TO SERIOUS AND ORGANISED INVESTMENT FRAUD IN AUSTRALIA

### AUSTRALIA'S LEGAL FRAMEWORK FOR ADDRESSING SERIOUS AND ORGANISED INVESTMENT FRAUD

Law enforcement and regulatory agencies operate under a range of different and indirect legislation to counter investment fraud activity. These provisions vary greatly and include: the *Corporations Act* (VIC), the *Criminal Code* Section 409 (1) (WA), the *Criminal Code* (NT), the *ACT Crime Act* (section 114D on organised crime) and the *ACT Criminal Code* (Part 3.3 on Fraudulent Conduct and Part 3.6 on Forgery and related offences). There are also laws outlawing hawking<sup>54</sup> within the *Corporations Act 2001*, which includes the prohibition of cold call tactics used by boiler-rooms.<sup>55</sup> Mutual assistance is primarily regulated by the *Mutual Assistance in Criminal Matters Act 1987* (Cth). Under the Act, Australia can request assistance from any country and receive a request for assistance from any country. This process is assisted by bilateral mutual assistance treaties and a number of multilateral conventions which contain mutual assistance obligations.

Trustees of superannuation funds have reporting obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF) to refer a suspicious matter to AUSTRAC under suspicious matter reporting obligations and to ASIC if a matter meets the definition of fraud under superannuation legislation. Regular liaison with the ATO also occurs in relation to identifying fraud and illegal early release schemes (primarily involving self-managed super funds). Superannuation agencies noted they would also report any suspicious matter to their state/territory police agency's fraud squad.

State and Territory law enforcement agencies are primarily responsible for responding to investment fraud, although the AFP does assist other law enforcement agencies in investigations of this type.

<sup>54</sup> Hawking prohibitions indicate that a person cannot engage in unsolicited telephone calls or meetings. More information on these provisions are available in the publications produced by ASIC 2002 (revised 2005). *Hawking Provisions*, Regulatory Guide 38

<sup>55</sup> ASIC 2002 (revised 2005). *Hawking Provisions*, Regulatory Guide 38 [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/Hawking\\_Guide.pdf/\\$file/Hawking\\_Guide.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/Hawking_Guide.pdf/$file/Hawking_Guide.pdf)





## TASK FORCE GALILEE

In recognition of the complexity of Serious and Organised Investment Fraud and the need to address this serious and organised crime, the Task Force is collaboratively working towards the establishment of a long-term response to this fraud.

Task Force Galilee is seeking to disrupt Serious and Organised Investment Fraud operations and the organised criminal groups behind them. It is also working to inform the public about Serious and Organised Investment Frauds and the threat they pose. Industry stakeholders play an integral part in raising awareness and communicating the threat of these Serious and Organised Investment Frauds to the Australian community. Also contributing to fraud awareness raising are the Australasian Consumer Fraud Task Force, and the AIC with their Online Fraud Survey.

As a result, Task Force Galilee has been engaging with a range of industry sectors, including banking, superannuation, financial advisory and community organisations, and Internet service providers, to develop strategies to prevent and disrupt Serious and Organised Investment Fraud. By working across law enforcement, regulatory and welfare agencies, the Task Force benefits from a broad range of specialist skills and capabilities and increased data sharing.

In addition to enforcement and regulatory initiatives and investigations, the Task Force has engaged in numerous public awareness strategies to alert the public to the threat posed by Serious and Organised Investment Fraud. This has included releasing media statements on the threat and providing case studies to illustrate the persuasive nature of the fraud and how anyone can be victimised. A case study is provided on the following page.



## CASE STUDY 4

### SERIOUS AND ORGANISED INVESTMENT FRAUD

This case study is a fictitious example of a Serious and Organised Investment Fraud, based on reported experiences of real victims.

Steve is a 65 year-old male, living alone. He is University educated, and previously owned his own investment advisory business. He considers himself quite savvy when it comes to money matters. He retired with a substantial sum of money for his and his wife's future. His wife is now deceased and he is now quite socially isolated.

Steve was unexpectedly 'cold-called' by fraud operators whom he described as very professional in their approach, with excellent knowledge of investment matters. In fact he admits he was 100 per cent taken in by them. Steve asked them a number of questions, which they were able to answer to his satisfaction, and the initial contact was followed up by 'senior advisors'.

Steve did not discuss this investment opportunity or his financial activities with anyone else, as he has extensive experience in the finance industry and generally relied on his own knowledge. But Steve admits in retrospect that he was not familiar with overseas investments. Because his superannuation funds were not doing very well, he was happy to give this new investment opportunity a try.

He made a number of transfers to the fraudsters, initially starting with a sum of \$10,000. He was referred to a very professional looking website and his own account, which showed his money increasing in value as the market 'went up'. He made further transfers, and again saw their value increasing. Overall, Steve sent \$200,000.

He only realised that the investments were fraudulent when the website unexpectedly went down and he was no longer able to access his account online or get through to the fraudsters on their phone numbers. He then 'Googled' the company name and found reports that it was a scam. There were comments from 56 others who had been victimised in a similar fashion.

Steve was devastated that he had been 'conned' and was too embarrassed to talk about his loss to anyone. He did not contact ASIC or other government agencies, such as the police, because he was initially so embarrassed and shocked.



Sometime later, he was contacted by local law enforcement officers who had come across his name when analysing bank transfers made to the fraudsters. They explained the nature of the Serious and Organised Investment Fraud to Steve.

Steve has been contacted again by the fraudsters, with offers to help him get his money back from the original investment. He was very cautious about these latest callers, and spoke with the local police before doing anything. They explained to him that this was a 'secondary fraud', and that he could expect to receive calls like this for some time as the fraudsters pass on victims' names to other scammers.

With this loss, as well as the decline in his original superannuation funds due to the global financial crisis, Steve is now concerned about his financial future. Instead of being a self funded retiree, he may now have to rely on a government pension.



## AUSTRALIAN AGENCIES THAT CONTRIBUTE TO THE PREVENTION AND DETECTION OF SERIOUS AND ORGANISED INVESTMENT FRAUD

In addition to Task Force Galilee's multi-agency approach, there are numerous agencies that currently engage in a range of prevention and detection strategies as part of their core business activities.

The primary agencies contributing to the detection, investigation and/or prevention of investment and Serious and Organised Investment Fraud activity in Australia include law enforcement agencies and regulatory agencies (e.g. ASIC, ACCC and AUSTRAC). However, a range of government agencies (e.g. ACMA, AGD, DIAC, ATO, ACBPS, DHS, DBCDE) and private sector agencies (banks and the superannuation sector) also have a role to play.

The types of actions agencies undertake to prevent, detect, disrupt and/or investigate investment and Serious and Organised Investment Fraud vary depending on their role and responsibilities. The AFP and all state and territory law enforcement agencies investigate Serious and Organised Investment Fraud as part of their broader fraud investigation responsibilities.

The following is a brief outline of the main regulatory agencies involved in countering investment and Serious and Organised Investment Fraud.

**The Australian Securities and Investments Commission (ASIC)** is Australia's key corporate, markets and financial services regulator. Their role is to ensure that Australia's financial markets are fair and transparent to instill confidence in Australia's economic reputation amongst investors and consumers. In order to ensure Australia's investment climate remains strong and resilient, ASIC undertakes a range of activities to detect, investigate and prevent serious and organised investment fraud. ASIC is proactive in its approach to reducing investment fraud. They release consumer alerts of Serious and Organised Investment Fraud via media releases and the ASIC website—<http://www.asic.gov.au/asic/asic.nsf>—as well as engaging with previous victims of investment fraud to prevent re-victimisation. ASIC also has a website <http://www.moneysmart.gov.au/> which provides information on frauds, a list of companies that have been implicated and actions to take to prevent being defrauded. The site also identifies ways of obtaining assistance when a member of the public thinks they have been defrauded. ASIC also provides a free monthly eNewsletter that provides information on frauds and other financial tips.

**The Australian Competition and Consumer Commission (ACCC)** promotes competition and fair trade in the marketplace to benefit consumers, business and the community. Its primary responsibility is to ensure that individuals and businesses comply with the Commonwealth's competition, fair trading and consumer protection laws. As a result, detecting fraudulent businesses and





generating public awareness of fraudulent activities is a key responsibility of the agency. To assist in the detection of fraudulent activities, the ACCC maintains a website called SCAMwatch, which provides the general public with information on known frauds including banking and online account frauds, identity theft, job and employment frauds and investment and Serious and Organised Investment frauds. It also provides tips and advice on how to recognise, avoid and report frauds. Furthermore, SCAMwatch (<http://www.scamwatch.gov.au>) provides email alerts on new and emerging frauds for members of the public who subscribe to the alert list.

**The Australian Transactions Report and Analysis Centre (AUSTRAC)** is Australia's anti-money laundering and counter-terrorism financing regulator and specialist financial intelligence unit. AUSTRAC contributes financial transaction report analysis to assist investigative and law enforcement agencies in combating financial crime. AUSTRAC also provides financial intelligence assessments in relation to international fraud syndicates, such as Serious and Organised Investment Fraud syndicates, and in the past has successfully assisted authorities to trace substantial transfers between accounts linked to the suspects.

Other government agencies also provide a supplementary role to investment and Serious and Organised Investment fraud detection. While the **Department of Broadband, Communication and Digital Economy (DBCDE)** does not focus specifically on investment fraud activities, they routinely engage in broader fraud and cyber crime awareness activities that can encompass elements of Serious and Organised Investment Fraud. This includes the Cyber Security Awareness Program. This program comprises several components:

- National Cyber Security Awareness Week
- Stay Smart Online website to provide tips and information on cyber security
- a free Alert Service to provide subscribers with up to date information in plain English on the latest security threats and the actions they can take to address them
- an interactive educational package for school children
- research to increase understanding of community awareness of cyber security so that messages can be refined and better targeted.

The DBCDE is also responsible for the Do Not Call register. The register allows individuals and businesses to register their telephone or fax numbers on a list that marketers must not use to make unsolicited calls. The Register was legislated in the *Do Not Call Register Act 2006, Do Not Call Register (Consequential Amendments) Act 2006*, and was amended in May 2010 by the *Do Not Call Registration Amendment Bill 2010*.

The **Australian Taxation Office (ATO)** provides information to enforcement and regulatory agencies through a number of information sharing arrangements with government and financial agencies. They also jointly sponsor (with ASIC) community awareness and education campaigns to help consumers avoid fraudulent schemes.

The **Department of Immigration and Citizenship (DIAC)** has collaboration and information sharing arrangements with a range of enforcement and regulatory agencies to refer any known fraud matters or suspicious offers to the relevant agencies.

Law enforcement and regulatory agencies both in Australia and overseas collaboratively focus on preventing investment and Serious and Organised Investment Fraud. The strategies developed range from single to multi-leveled and include:

- collaborating with international bodies and establishing public-private partnerships with key stakeholder agencies
- victim support strategies to prevent re-victimisation
- fraud and prevention advice to the elderly
- education programs with local bank representatives to promote fraud warnings to rural areas
- educating younger audiences on fraud awareness and computer security through cartoon campaigns—for example, the Queensland Police Service has developed ‘Fiscal the Fraud Fighting Ferret’ cartoons to increase awareness of various frauds (see <http://www.scamwatch.gov.au/content/index.phtml/itemId/934544>)
- presenting to key industry bodies such as share registrars on investment and Serious and Organised Investment fraud and liaising with banking agencies for assistance with tracing accounts
- contacting potential victims advising them of their vulnerability after they seized a master list of contacts from Serious and Organised Investment Fraud offenders<sup>56</sup>
- developing education campaigns and public seminars for the general public providing points of identification which could suggest they are being targeted by an investment and/or Serious and Organised Investment fraud operation and actions to take
- publishing advice on how to protect against investment and Serious and Organised Investment fraud on government websites

<sup>56</sup> See for example Cumbo, J 2010, Master list of boiler room victims found, December 7, *Financial Times*, <http://www.ft.com/cms/s/2/518efafa-01f1-11e0-b66c-00144feabdc0.html#axzz1r8unDKJf>, accessed 5 April 2012.





- sending letters to service providers to alert them to the suspected illegal activities of their clients and to advise them to cease providing their services to that company
- developing information leaflets on how to recognise investment fraud Serious and Organised Investment Frauds
- hosting conferences on serious fraud issues (e.g. Financial Services Authority (FSA) 'International Boiler-room' Fraud Conference UK 10 September 2008; International Organised Fraud Symposium 2011 "Fraud - The Global Pandemic" 27–28 September 2011 at the Hyatt Regency, Sanctuary Cove Queensland)
- hosting press conferences where victims speak out on their experience.

The **Australian Bureau of Statistics**<sup>57</sup> (ABS) conducts a 'Personal Fraud Survey' throughout Australia which provides insights into personal fraud, the characteristics of victims of fraud and the characteristics of incidents of fraud.

The **Australian Institute of Criminology**<sup>58</sup> (AIC) along with the Australasian Consumer Fraud Taskforce (ACFT) conducts an annual on-line survey to gather information about fraud and scams. The AIC, as an ACFT taskforce member, collects and analyses this information to improve the prevention, detection, investigation and prosecution of scams.

The **Australasian Consumer Fraud Taskforce**,<sup>59</sup> (ACFT) comprises 22 government regulatory agencies and departments with responsibility for consumer protection regarding frauds and scams. The ACFT also has a range of community, non-government and private sector organisations as partners in the effort to increase the level of scam awareness. The purpose of the ACFT is to help government members work together to:

- enhance the Australian and New Zealand governments' enforcement activity against frauds and scams
- run an annual coordinated information campaign for consumers—the **National Consumer Fraud Week** in March (timed to coincide with **Global Consumer Fraud Prevention Month**)
- involve the private sector and community groups in the information campaign and encourage them to share information they may have on scams and frauds
- generate greater interest in research on consumer frauds and scams.

57 Australian Bureau of Statistics, Personal Fraud 2010–2011, <http://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/1FF970676E24FDFECA2574740015CA71?opendocument>

58 The Australian Institute of Criminology, [http://www.aic.gov.au/crime\\_types/economic/fraud/acft.aspx](http://www.aic.gov.au/crime_types/economic/fraud/acft.aspx), accessed 15 June 2012.

59 Australasian Consumer Fraud Taskforce, <http://www.scamwatch.gov.au/content/index.phtml/itemId/725675>, accessed 15 June 2012.

## INTERNATIONAL RESPONSE

Australia is not alone in attempting to disrupt and prevent Serious and Organised Investment Fraud. The AFP's International Liaison Officer Network provides Australian law enforcement agencies with a mechanism to collaborate with their international counterparts in relation to fraud and other crimes. In the United Kingdom for example, a centralised fraud agency, the Financial Services Authority (FSA) has been established. The FSA is actively engaged in numerous prevention, education, detection and investigation activities in relation to investment fraud. The FSA is also collaborating with the City of London Police and the Serious Organised Crime Agency (SOCA) to tackle investment fraud, with the aim of disrupting fraudulent operations at each stage of the process.

The City of London Police has implemented *Operation Archway* since 2007 to counter Serious and Organised Investment Fraud activity. Based within the National Fraud Intelligence Bureau (NFIB), Operation Archway collects information and statistics on investment fraud ('share purchase fraud').

There is also an international website dedicated to warning investors of stock and securities fraud called Global Investor Alerts—<http://www.globalinvestoralerts.com/>. This website provides investors with a central point where they can check if a company that is cold-calling them is registered with the financial authorities or is black-listed, search for information about the stock and securities the company offers and check if any warnings have been issued against the company. The website also provides assistance for victims of investment and Serious and Organised Investment fraud seeking to file claims with financial authorities or undertake legal action.





## SUMMARY

Analysis of Australia's response and the response by international agencies to Serious and Organised Investment Fraud indicate that this type of fraud is widely recognised, and reports of Serious and Organised Investment Fraud in Australia are increasing. This could be due to many factors including greater awareness of the crime, improved reporting rates or a general increase in Serious and Organised Investment Fraud operations. As the report demonstrates, Serious and Organised Investment Fraud is not an opportunistic crime, but in fact is a calculated, sophisticated, organised criminal event. These factors also highlight why law enforcement agencies and regulatory agencies globally face difficulties with Serious and Organised Investment Fraud prevention, detection, disruption and prosecution.

As Serious and Organised Investment fraudsters are continually evolving their modus operandi, the responses to this crime need to be flexible and responsive. Therefore, it is unlikely that there is one strategy that is a panacea to the crime, particularly as Serious and Organised Investment Fraud involves many different elements. One of the main challenges in developing responses to Serious and Organised Investment Fraud is the overall lack of available, proven good practice examples in Serious and Organised Investment Fraud disruption.

Raising awareness and education campaigns has been a common strategy for Australian and international agencies to prevent Serious and Organised Investment Fraud. These campaigns are largely directed at potential victims, alerting them to this fraud type, characteristics of the fraud and explanation of what to do if a person suspects an investment fraud operation is active.

Information sharing and collaboration is also considered an essential part of responding to investment and Serious and Organised Investment fraud. This is a key characteristic of Australia's response and is a central focus to Task Force Galilee's prevention and intervention strategy development.

As a prevention measure, law enforcement and regulatory agencies both nationally and internationally highlight it is essential prior to investing to check numerous sources to ensure the legitimacy of the investment. Investors are also encouraged not to become complacent. Due diligence is required even if an investor has a financial advisor because they may also be unaware of the fraud. It has been suggested that investment and Serious and Organised Investment frauds (e.g. Bernie Madoff fraud) could have been prevented with 'due diligence' and verifying information by either investors or hedge fund managers.<sup>60</sup>

<sup>60</sup> See Kentouris, C 2009; Funds, investors assess operations In Madoff wake, *Securities Industries News*, vol. 21(3), pp 1, 14; Cohen, R & Blinken, S 2009, Investing with Care: How to Avoid Investment Scams and Surprises, *Nonprofit World*, Jul/Aug, vol. 27(4), pp 14-15.

In addition to always seeking independent financial advice prior to making an investment, Task Force Galilee recommends the following tips to reduce the risk and impact of investment and Serious and Organised Investment fraud:

**Visit** [www.moneysmart.gov.au](http://www.moneysmart.gov.au) or call 1300 300 630 for further information.

**Alert** your family and friends to this fraud, especially anyone who may have savings to invest.

**Report** suspected fraud to the Australian Securities and Investments Commission, via [www.moneysmart.gov.au](http://www.moneysmart.gov.au) or 1300 300 630, or your local police. Any information that can be provided such as company name, location and contact details will assist with subsequent investigations and enquiries.

**Hang up** on unsolicited telephone calls offering overseas investments.

**Check** any company you are discussing investments with has a valid Australian Financial Services Licence at [www.moneysmart.gov.au](http://www.moneysmart.gov.au)

**Always seek independent financial advice before making an investment.**





## REFERENCES

Australian Crime Commission Board (ACC Board) 2011, *Protect your retirement savings—Australian Crime Commission Board warns of investment scams targeting Australians*. Australian Crime Commission Board media release 28 September, <http://www.crimecommission.gov.au/media/protect-your-retirement-savings%E2%80%94australian-crime-commission-board-warns-investment-scams-tar-0>

Attorney-General's Department (AGD) 2003, *The national research project into good practice in community crime prevention*, Barton, Canberra: Australian Government Attorney-General's Department

Australian Securities and Investments Commission (ASIC) 2002a, *Hook, line & sinker: Who takes the bait in cold calling scams?* ASIC: Canberra [http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/HookLineSinkers.pdf/\\$file/HookLineSinkers.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/HookLineSinkers.pdf/$file/HookLineSinkers.pdf), accessed 20 December 2011.

Australian Securities and Investments Commission (ASIC) 2002b, *International cold calling investment scams*, Report no 14. Canberra: ASIC [http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/International\\_Cold\\_Calling\\_report.pdf/\\$file/International\\_Cold\\_Calling\\_report.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/International_Cold_Calling_report.pdf/$file/International_Cold_Calling_report.pdf), accessed 20 December 2011.

Budd, C & Anderson, J 2011, *Consumer fraud in Australasia: Results of the Australasian Consumer Fraud Taskforce online Australia surveys 2008 and 2009*. Technical and Background Paper no. 43, Canberra: Australian Institute of Criminology <http://www.aic.gov.au/publications/current%20series/tbp/41-60/tbp043.aspx>, accessed 20 December 2011.

Cornish, DB & Clarke, RV 2003, Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention, in Smith M & Cornish DB (eds), *Theory for situational crime prevention*, Monsey, NY: Criminal Justice Press.

Eckblom, P 2010, *Crime Prevention, Security and Community Safety Using the 5Is Framework*, England: Palgrave MacMillan.

Fitzgerald, D 2011, Fools gold: Offenders rush to cash in on metal's surging price. *The Australian*, 26 August.

Layton, C & Jennett, C 2005, Partnerships in policing and evidence-based practice in crime prevention: Are they incompatible? Conference paper presented at: *Delivering crime prevention : making the evidence work* Carlton Crest Hotel, Sydney 21-22 November 2005 [http://www.aic.gov.au/criminal\\_justice\\_system/policing/~media/conferences/2005-cp/jennett.ashx](http://www.aic.gov.au/criminal_justice_system/policing/~media/conferences/2005-cp/jennett.ashx), accessed 20 December 2011.

Levi, M and Smith, R G, 2011, 'Fraud vulnerabilities and the global financial crisis,' in *Trends and issues in Crime and Criminal Justice*, No. 422, Australian Institute of Criminology, Canberra.

Maranzana, P & Finger, L 2011, London accountants in 'boiler room' scam. *Accountancy vol 147*(1409): 11-11, 1/3p.

Pawson, R & Tilley, N 1997, *Realistic evaluation*, London: Sage.

Peed, C 2002, Problem-Solving Tips, *A Guide to Reducing Crime and Disorder Through Problem-Solving Partnerships*. Washington DC: US Department of Justice <http://www.popcenter.org/library/reading/pdfs/Tips.pdf>, accessed 20 December 2011.

Seymour-Rolls, K & Hughes, I 1995, 2000, Participatory action research: Getting the job done, *Action Research Reports* <http://www.scu.edu.au/schools/gcm/ar/arr/arow/rseymour.html>

Stanford, RA, Cosmo, N & Nadel, A 2009, Alleged Investment Scams: A Scorecard. *BusinessWeek Online*; 2/18/2009, p9.

Titus, RM & Gover, AR 2001, Personal fraud: The victims and scams in repeat victimisation, in Farrell, G & Pease, K (eds), *Crime prevention studies*, vol 12. Monsey, NY: Willow Tree Press.

Van Staden, L, Leahy-Harland, S & Gottschalk, E 2011, *Tackling organised crime through a partnership approach at the local level: a process evaluation*. Research Report 56: Summary. UK: Home Office. <http://www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/crime-research/horr56/horr56-summary?view=Binary>, accessed 20 December 2011.

Scott, M & Goldstein, H 1988, Key elements in problem-oriented policing. (online only: <http://www.popcenter.org/about/?p=elements>), accessed 20 December 2011.

## FURTHER INFORMATION

For further information or queries regarding this product please contact ACC Product Disseminations on (02) 6243 6666 or email [products@crimecommission.gov.au](mailto:products@crimecommission.gov.au).

### WE VALUE YOUR FEEDBACK

The ACC is committed to continual improvement and values your feedback on its products.

We would appreciate notification of any positive outcomes associated with this report by contacting ACC Product Disseminations at [products@crimecommission.gov.au](mailto:products@crimecommission.gov.au)

Thank you for your time and effort in providing feedback.



