



AUSTRALIAN CRIME COMMISSION

*Summary of Intelligence:
Financial Crime Impacting Australia*

**Parliamentary Joint Committee on Law Enforcement
Inquiry into Financial Related Crime**



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

Table of Contents

INTRODUCTION.....	4
Executive Summary	4
International Serious and Organised Crime Environment	5
Serious and organised financial crime	7
The Domestic Environment.....	8
MONEY LAUNDERING	11
Overview – A key enabler of Serious and Organised Crime	11
Threat Assessment	13
<i>Alternative Remittance Sector</i>	<i>14</i>
<i>Informal Value Transfer Systems</i>	<i>14</i>
<i>Trade-Based Money Laundering</i>	<i>16</i>
<i>Virtual Currencies.....</i>	<i>17</i>
<i>The Impact of Prevailing Global Economic Conditions.....</i>	<i>18</i>
FINANCIAL RELATED CRIMES	19
INVESTMENT AND FINANCIAL MARKET FRAUD.....	19
<i>Fraudulent investment schemes</i>	<i>20</i>
<i>Manipulation of the share market and exploitation of financial securities</i>	<i>21</i>
<i>New threats</i>	<i>22</i>
SUPERANNUATION FRAUD	23
REVENUE AND TAX FRAUD.....	26
<i>Phoenix Schemes</i>	<i>27</i>
CARD FRAUD.....	29

UNCLASSIFIED

UNCLASSIFIED

INTRODUCTION

Executive Summary

1. Internationally, three key factors frame the contemporary serious and organised crime environment: the infinitely complex, diverse and pervasive nature of serious and organised crime, fundamentally enabled by globalisation, technology and cyber capabilities; the challenges involved in developing appropriate and effective responses; and the local and regional effects of the global economic crisis.
2. Serious and organised crime has proven to be innovative and adaptive, capitalising on the opportunities afforded by the economic crisis and the limited resources available to combat organised crime, to grow their business and power, and exploit new or surging markets for significant financial gain. For example, serious and organised criminals have exploited reduced business profitability and investment capital shortages have been exploited to buy or take over failing companies for below market value, allowing them to gain interests in sectors crucial to economies and to purchase a 'legitimate' face for their activities.
3. Though the traditional illicit markets - including markets for drugs such as methylamphetamine, cocaine, heroin, MDMA and cannabis - will continue to be a feature of the serious and organised criminal environment, there is an international trend toward a greater involvement of serious and organised criminals in financial crime. These financial crimes include money laundering, investment and financial market fraud, superannuation fraud, revenue and taxation fraud and card fraud.
4. With regard to the scope of the challenge posed by financial crime, the United Kingdom (UK) Serious and Organised Crime Strategy, published in October 2013, valued the annual social and economic cost of fraud attributable to organised crime at UK £9.9 billion – second only to drugs at an estimated annual social and economic cost of UK £10.7 billion¹. The risk posed by financial crime is particularly salient in the current economic environment, in which damage to financial markets, financial institutions, government revenue bases and savings held by private individuals can have far reaching implications for the economic recovery or ongoing stability of nations.
5. Australia is inextricably and increasingly linked to international criminal markets and trends. The rise in the involvement of serious and organised crime in financial crime

¹ Home Office 2013, '*Serious and Organised Crime Strategy*', London [online]. Accessed 11/02/2014, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf >.

UNCLASSIFIED

UNCLASSIFIED

seen internationally has also occurred in Australia, with the risk posed by financial crime being on an upward trajectory.

6. With regard to money laundering, though regulated sectors such as banking and the alternative remittance sector continue to play an important role in facilitating money laundering, the use of informal value transfer systems and trade-based money laundering to facilitate international money laundering is increasing with illicit funds moved out of Australia through a range of international jurisdictions using different methodologies until the funds reach their final destination.
7. Importantly, Australia, with its relatively stable economy, is currently seen by international serious and organised crime entities as a safe place in which to invest illicit funds. In particular, the Australian real estate market has become attractive to criminal investors looking to protect the value of their assets, particularly as money laundering legislation tightens overseas. Indicators that the flow of illicit funds into Australia is increasing will necessitate a move away from the traditional law enforcement focus on the flow of illicit funds out of Australia, to a dual focus on both outgoing and incoming funds.

International Serious and Organised Crime Environment

8. The ACC and its partners have identified the emergence of the entrepreneurial individual as a key player in a number of significant illicit markets. This phenomenon, enabled by globalisation and technology, and observed internationally, has necessitated a shift in the way in which the threat posed by serious and organised crime can, or should be, contextualised. Significant harms can now be wrought by actors who operate outside traditional organised crime structures, who are committing serious crime. For example, an individual criminal actor, often enabled by cyber and technology crime, can perpetrate significant investment and financial market frauds, revenue and tax frauds, or traffic in illegal firearms.
9. Internationally, three key factors frame the contemporary serious and organised crime environment:
 - a. the seemingly infinitely complex, diverse and pervasive nature of serious and organised crime, enabled by technology and the cyber environment and by globalisation
 - b. the challenges that new criminal activities and methodologies pose to governments, enforcement and regulatory agencies, requiring fundamental changes to enable an effective response
 - c. the local and regional effects of the global economic crisis.

UNCLASSIFIED

UNCLASSIFIED

10. There is no doubt that serious and organised crime is now more complex, diverse and pervasive than at any other time in history. There is also no doubt that serious and organised crime is necessarily transnational and global in nature. While those individuals and groups involved in serious and organised crime will always vary in their capabilities, geographical reach and sophistication, it is apparent that there are groups, networks and individuals operating at an 'elite' criminal level and targeting illicit markets in a number of countries simultaneously. These entities are highly networked, highly professional, extremely well funded and operate with high-level specialist advice – including legal and financial advice - allowing them to either evade detection, or to exploit vulnerabilities in legislative and regulatory regimes internationally.
11. The sophisticated global business models used by organised crime, their wealth, use of technology and specialist professional facilitators masking their activities, and their ability to operate across multiple jurisdictions and across illicit markets, makes it increasingly difficult for resource limited enforcement agencies to identify, disrupt or prosecute these criminals.
12. The cyber and technology environment has shaped the development of many of the new markets, permitting entrepreneurial individuals to establish themselves within niche markets, and connect directly with users through the internet. This environment has allowed for the development of new and emerging payment systems such as virtual currencies, including bitcoin. These virtual currencies are rife for exploitation by organised criminal groups due to their unregulated nature within monetary systems.
13. Serious and organised crime has been quick and innovative in taking advantage of opportunities afforded by the global economic crisis. Organised crime has grown its business and power, and exploited new or surging markets for significant financial gain. For example, criminal entities have capitalised on reduced business profitability and shortages of investment capital to buy or take over failing companies for well below the market value, gaining interests in sectors crucial to economies and, in so doing, purchasing economic power and a 'legitimate' face for their activities. In the EU Serious and Organised Crime Threat Assessment (SOCTA) 2013, the global economic crisis was listed as a 'crime enabler', highlighting the fact that the crisis has had particular effects on the business of serious and organised crime within the EU.
14. The effects of the global economic crisis have varied between countries and across regions. Where the greatest impacts have been felt, there has been a clear tension between the need for governments to generate sufficient revenue for expenditure in sectors necessary to economies, and to ensure the provision of essential services and infrastructure, and the imperative of serious and organised crime to maximise their profits by operating outside of the legitimate economy. Those countries whose economies have been most profoundly affected by the economic crisis are those in which the illicit or 'shadow' economy is the strongest. Consequently, the way in which

UNCLASSIFIED

UNCLASSIFIED

serious and organised crime evolves and the adequacy of government investment in the rule of law, will have a very direct impact on the future global economic picture.

Serious and organised financial crime

15. Though 'traditional' illicit markets – including the markets for drugs such as methylamphetamine, cocaine, heroin, MDMA and cannabis - will continue to be a feature of the serious and organised criminal environment, there is an international trend toward a greater involvement of serious and organised criminals in financial crime. These financial crimes include money laundering, investment and financial market fraud, superannuation fraud, revenue and taxation fraud and card fraud. Unlike the traditional illicit markets – which are seen as high risk / high return markets by criminal entities – financial crime is seen as low risk / high return and much more difficult for governments to respond to because of its complexity.
16. Significant profits can be derived from mass marketed 'boiler room' or cold-call investment scams, which can be delivered to large pools of victims in any country over the internet from any region, using technology that can hide both the identity and the location of the perpetrator. Similarly large profits can be derived from elaborate manipulations of share prices of publicly listed companies, carbon credit scheme frauds, and venture capital frauds in which capital is raised to invest in fraudulent or fictitious schemes. Once discovered, it can be difficult to identify the perpetrators of these schemes – perpetrators who can conceal their identity behind complex corporate structures incorporated in off-shore secrecy havens – and to follow and seize the money generated by the scheme, which can be laundered through multiple international jurisdictions using multiple methodologies.
17. With regard to the scope of the challenge posed by financial crime, the United Kingdom (UK) Serious and Organised Crime Strategy, published in October 2013, valued the annual social and economic cost of fraud attributable to organised crime at UK £9.9 billion – second only to drugs at an estimated annual social and economic cost of UK £10.7 billion².
18. And there are new and significant challenges from serious and organised crime emerging. A joint International Organization of Securities Commissions (IOSCO) and

² Home Office 2013, '*Serious and Organised Crime Strategy*', London [online]. Accessed 11/02/2014, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf >.

UNCLASSIFIED

UNCLASSIFIED

World Federation of Exchanges (WFE) staff working paper³, published in July 2013, pointed to the high incidence of cyber attacks on securities exchanges around the world. Of the 46 exchanges that responded to the IOSCO and WFE cyber attack survey on which the working paper was based, 53 per cent reported suffering a cyber attack in 2012 - the year for which the data was collected. Though the majority of the attacks were denial of service attacks and viruses, data theft, insider information theft, and account takeover / unauthorised financial transactions, were also identified as among the most common and potentially hazardous forms of cyber attack. The working paper does not attempt to identify which actors might be responsible for the attacks; however it is likely that at least some of the attacks were perpetrated by serious and organised crime, which could clearly benefit significantly from data theft, insider information theft, and account takeover. Importantly, as noted by the working paper, these kinds of attacks have the potential to result in massive financial losses and loss of confidence in the integrity of the securities markets, with the interconnectedness of world markets meaning that the effects in one market will be felt across others.

19. The risk posed by financial crime is particularly salient in the current economic environment, in which damage to financial markets, financial institutions, government revenue bases and savings held by private individuals can have far reaching implications for the economic recovery or ongoing stability of nations.

The Domestic Environment

20. The contemporary serious and organised crime environment in Australia is inextricably linked to international criminal markets and trends. The rise in the involvement of serious and organised crime in financial crime seen internationally has also occurred in Australia, with the risk posed by financial crime being on an upward trajectory.
21. In the Australian context, the greatest current financial crime risk is assessed to be associated with investment and financial market fraud. The recent investigative focus on investment and financial market fraud has significantly enhanced the intelligence picture with regard to this crime type, with strong indications emerging that serious and organised criminal exploitation of the market is occurring at all levels of sophistication. Notably, there are indications that highly sophisticated international organised crime groups, some of which have a history of undertaking similar fraud in other countries, are

³ Tendulkar, Rohini, 2013, 'Cyber-crime, securities markets and systemic risk', joint staff working paper of the IOSCO Research Department and World Federation of Exchanges, IOSCO & WFO, accessed 07/02/2014, available at: http://www.world-exchanges.org/files/statistics/pdf/IOSCO_WFE_Cyber-crime%20report_Final_16July.pdf >.

UNCLASSIFIED

UNCLASSIFIED

targeting Australia. The identification, investigation and prosecution of investment and financial market fraud require specialist capabilities as well as new skills and knowledge: investigations are complex, resource intensive, and often protracted.

22. The Australian superannuation industry maintains investments totalling \$1.62 trillion. These investments are equivalent to approximately 120 per cent of the Australian share market capitalisation and 90 per cent of Australia's annual gross domestic product (GDP).⁴ Consequently, the Australian superannuation sector is likely to be a highly attractive target for serious and organised crime, including 'elite' level international groups with access to professional advisers able to provide specialist guidance on how to avoid detection and prosecution by enforcement agencies or regulators.
23. The potential harm that can result from serious and organised criminal involvement in both investment and financial market fraud and superannuation fraud in Australia is acute. In relation to investment and financial market fraud, confidence in the integrity of the financial market is essential to attracting capital and investment, with a loss of confidence having the potential to result in the withdrawals of funds from the sector, threatening the stability of the markets and the economy. The Australian superannuation industry is a major contributor to the Australian financial sector, and large superannuation frauds perpetrated by serious and organised crime could result in significant costs for government. These costs would include financial support for victims, and social security benefits for those unable to provide for themselves in retirement.
24. Though regulated sectors such as banking and the alternative remittance sector continue to play an important role in facilitating money laundering, the use of informal value transfer systems (IVTS) to facilitate international money laundering is increasing. Informal value transfer systems are any network that receives money for the purpose of making an equivalent value available to a third party in another geographical location, without the physical transfer of money off-shore.
25. Trade-based money laundering – concealing flows of illicit funds in large volume legitimate transactions associated with international trade – is increasingly being identified. The movement of illicit funds out of Australia using trade-based money laundering may often be one step in money laundering processes that transit through a range of international jurisdictions, using different methodologies for each stage of the journey to the final destination of the funds.

⁴ KPMG, 2012. 'Evolving Superannuation Industry Trends', accessed on 16/12/2013, available at www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/evolving-superannuation-industry-trends.pdf

UNCLASSIFIED

UNCLASSIFIED

26. Importantly, Australia, with its relatively stable economy, is currently seen by international serious and organised crime entities as a safe place in which to invest illicit funds. This situation has necessitated a move away from the traditional law enforcement focus on the flow of illicit funds out of Australia, to a dual focus on both outgoing and incoming funds.
27. Countering the rise in the risk posed by financial crime, and addressing the challenges posed by the changing money laundering environment, will demand close partnerships between enforcement agencies, government, regulators and the private sector. These partnerships will be essential to establishing the procedural, legislative and regulatory framework required to appropriately balance the need to filter foreign investment in Australia for illicitly obtained funds, while ensuring the necessary flow of foreign capital into Australian markets. For this reason, ASIC, the banking and finance sector, the ASX and the Australian Department of Treasury will be essential parties to any coordinated and effective future strategies to combat serious and organised crime in Australia.
28. The nature of the contemporary serious and organised crime threat to Australia has necessitated a greater focus on gaining a strategic appreciation of risk across the serious and organised crime environment in order to direct scarce resources to those threats causing, or likely to cause, the most harm. Australian authorities have been engaged in developing strategies and programs to maintain an understanding of the constantly evolving nature of serious and organised crime, including new markets, new market participants, and new methodologies. Authorities have also had to develop new partnerships, and new capabilities – including cyber and financial capabilities - to enable them to have an impact upon the criminal environment.

UNCLASSIFIED

UNCLASSIFIED

MONEY LAUNDERING

Overview – A key enabler of Serious and Organised Crime

29. Organised crime groups rely on money laundering as a way of legitimising or hiding proceeds or instruments of crime. Money laundering is a pervasive, corrupting process that can blend criminal and legitimate activities. It stretches across areas as diverse as mainstream banking, international funds transfers and foreign exchange services, gambling, shares and stocks, artwork, jewellery and real estate.
30. Financial profit is a main driver for organised crime groups. Legitimising the proceeds of crime and the instruments of crime (the means by which crime is committed) is crucial for organised crime groups and this activity poses an ongoing risk to the Australian community. Money laundering involves criminals attempting to hide or disguise the true origin and ownership of the instruments of crime and the proceeds of crime so that they can avoid prosecution, conviction and confiscation of criminal funds. Money laundering offences are defined in Part 10.2 of the *Criminal Code Act 1995* (Cwlth). The offences encompass a very wide range of criminal activity.
31. Money laundering is an extremely diverse activity. It is carried out in Australia at all levels of sophistication by most, if not all, organised crime groups, increasingly with the assistance of professional advisers, and using a constantly evolving variety of techniques. Although the banking system and money transfer and alternative remittance services are major channels for money laundering, organised crime groups consistently seek out new channels for money laundering.⁵
32. There is no single method of laundering money. Money launderers have shown themselves to be imaginative, creating new schemes to get around the counter-measures designed to identify and stop them. Some examples of strategies that criminals might use to launder money are:
- a. breaking up large amounts of cash and depositing the smaller sums in different bank accounts, or buying money orders or cheques and depositing them in other accounts, in an effort to place money in the financial system without arousing suspicion
 - b. moving money around to create complex money trails, making it difficult to identify its original source – usually through a series of quick transactions, or through businesses in other countries

⁵ Australian Transaction Reports and Analysis Centre (AUSTRAC) 2011, *Money laundering in Australia*, AUSTRAC, Sydney.

UNCLASSIFIED

UNCLASSIFIED

- c. using funds 'legitimised' through introduction into the formal financial system to facilitate criminal activity or legitimate business, or to purchase high-value goods or real estate
- d. using a number of people to carry out small transactions or cash smuggling
- e. using online gambling platforms, placing illegal proceeds of crime into gaming machines or purchasing casino chips and cashing them out shortly afterwards
- f. trade-based money laundering – concealing the movement of funds within large volumes of legitimate financial transfers associated with international trade.⁶

33. The absence of an agreed methodology for estimating the value of money laundering, and gaps in information on the financial dimension of organised criminal activity, hamper efforts to calculate an accurate figure for money laundering in Australia.

34. Money laundering can harm the Australian community in many ways, including:

- a. 'crowding out' legitimate businesses in the marketplace when businesses that are fronts for money laundering subsidise products and services so that they can sell them at levels well below market rates
- b. affecting the reputation and integrity of financial institutions when, usually without knowing, they become involved with the proceeds of illegal activity
- c. distorting investment patterns
- d. assisting in the financing of international and domestic terrorism
- e. financing and providing motivation for further criminal activities.⁷

35. Three key factors influence the selection of particular money laundering methodologies: efficiency, capacity and cost. On the basis of these criteria, organised crime groups continue to widely use alternative remittance dealers. International funds transfers by some dealers can conceal their clients' illicit money flows among the high volumes of aggregated (mainly legitimate) daily transactions.

36. Some organised crime identities are suspected of being involved in the financing and construction of internationally based casinos and of using this opportunity to launder funds, as well as continuing to launder illicit funds on completion of the project. Many casinos and gaming facilities offer services similar to those of financial institutions,

⁶ Australian Transaction Reports and Analysis Centre (AUSTRAC) 2011, *Money laundering in Australia*, AUSTRAC, Sydney.

⁷ *ibid.*

UNCLASSIFIED

including accounts, foreign exchange, electronic funds transfers, cheque issuing and safety deposit boxes. These ancillary services, in addition to the variety of gambling services offered and the high cash turnover, make the gaming sector highly attractive and effective for money laundering.

37. However, new money exchange platforms – in particular, virtual currencies (also known as cryptocurrencies) – remain a challenge for law enforcement as they often fall outside the anti-money laundering and counter-terrorism financing regulatory framework. Bitcoin is an example of a digital currency that can be bought and sold anonymously online and does not rely on a central bank or financial institution to facilitate transactions. The unregulated environment and the anonymity of transactions make currencies such as Bitcoin attractive to organised crime for money laundering.

Threat Assessment

38. Significant new insights into the money laundering methodologies used by serious and organised crime groups operating in Australia have been achieved through targeted whole of government effort. In particular, Task Force Eligo - a nationally coordinated preventative task force involving the ACC, AFP, state police agencies and AUSTRAC, addressing the threat posed by alternative remittance services (ARS) and Informal value transfer systems (IVTS) has been a primary source of new intelligence with regard to money laundering. Though more is now known, it is not clear whether these methodologies are necessarily new, or whether they have been used for some time, and have only now been identified due to a greater resource focus on money laundering.
39. Importantly, while law enforcement has traditionally focused on funds leaving Australia (already laundered, or being sent off shore for the purpose of laundering), it is apparent that attention also needs to be paid to funds entering Australia that may be the proceeds of crime as transnational organised crime may be seeking to move illicit funds to Australia to make 'legitimate' investments. This trend has been precipitated by the global financial crisis, in the context of which Australia – with its relatively stable economy – is seen as a 'safe' country in which to invest or hide criminal wealth.
40. For organised crime operating in Australia, money laundering is increasingly a transnational enterprise, with the proceeds of crime generated in Australia typically being put through an international money laundering cycle, sometimes orchestrated by professional transnational money laundering syndicates.
41. Though the use of multiple methodologies to launder illicit funds appears to be the emerging paradigm, within those multiple methodologies, law enforcement has observed both IVTS and trade-based money laundering (TBML) to be gaining prominence.

UNCLASSIFIED

UNCLASSIFIED

Alternative Remittance Sector

42. Alternative remittance services, also known as money transfer businesses, enable the transfer of money and property within and between countries, often outside of the formal financial and banking system. In Australia, the corporate remittance sector is comprised of global money transfer businesses, ranging from remittance network providers, such as Western Union, MoneyGram and their affiliates, to independent remitters.
43. While alternative remittance operators provide a legitimate service, the remittance sector is recognised within the international anti-money laundering and counter-terrorism financing community as high-threat for money laundering and criminal exploitation. Common descriptors of remittance activity also include 'informal', 'parallel' and 'underground' banking. This signifies concerns that some services operate on the fringe of regulatory control in the cash or 'shadow economy' or harbour entities active in the criminal economy.
44. The alternative remittance sector (ARS) remains a key channel through which illicit funds are remitted offshore.

Informal Value Transfer Systems

45. Informal Value Transfer Systems (IVTS) is a term used to describe a number of traditional and historic methodologies used by members of global diaspora communities to remit funds outside of the formal financial and banking system. While businesses that utilise IVTS are technically encompassed within the ARS, they are often smaller and less formal than their large-scale commercial counterparts, such as Western Union.
46. IVTS networks represent some of the oldest and most established financial systems in the world and encapsulate a number of value transfer mechanisms that predate the modern Western notion of formal banking. Some IVTS mechanisms used today have existed as far back as 5800 BC⁸, and include Hawala (Middle East, Afghanistan, and Pakistan), Hundi (India), Fei ch'ien (China), and Phoe kuan (Thailand). These IVTS are still in operation across the globe and are often the preferred means of transferring value in many cultures.

⁸ United States Department of the Treasury: Financial Crimes Enforcement Network. (2003). *FinCEN Advisory Issue 33: Informal Value Transfer Systems*

UNCLASSIFIED

UNCLASSIFIED

47. As a result of international immigration and the natural establishment of cultural diasporas across the globe, these IVTS have spread on an international scale, and operate alongside the modern mainstream finance sector. Today, IVTS operations are found in most countries and often provide value transfer services to diaspora communities familiar with the operation of such services. IVTS services are provided by specific remittance businesses, or by operators of unrelated businesses, such as import and export businesses, travel agencies, and retail shops. Expatriates often use IVTS to send money back to their families and friends in their home countries⁹. This does not, however, preclude the use of these services by members of other cultures, or serious and organised crime.

48. The various IVTS methods referenced above generally operate on a similar model. This model is demonstrated below, which depicts a situation in which an individual (#1) in Country A wants to send money to an individual (#2) in Country B:

- i. Individual #1 gives currency to an IVTS operator in Country A.
- ii. The IVTS operator in Country A provides Individual #1 with a code or other identification mechanism.
- iii. The IVTS operator in Country A notifies his counterpart in Country B by phone, fax, or e-mail of the transaction amount to pay Individual #2 and the code.
- iv. Individual #1 contacts the intended recipient, Individual #2, in Country B and provides the code to that person.
- v. Individual #2 goes to the IVTS operator in Country B, gives the appropriate code, and picks up the specified funds sent to him.¹⁰

49. IVTS operator in Country A is now indebted to the IVTS operator in Country B; however, this will often be nullified by value transfers made from the IVTS operator in Country B to the IVTS operator in Country A.

50. No money is actually transferred. The IVTS operator in Country A uses the money received from senders to “stock” his cash supply for use in future payments for incoming requests to him. The situation is reversed in Country B where the IVTS operator’s cash is generated from senders in his country. Account settling may be accomplished through other methods such as:

⁹ United States Department of the Treasury: Financial Crimes Enforcement Network. (2003). *FinCEN Advisory Issue 33: Informal Value Transfer Systems*

¹⁰ *ibid*

UNCLASSIFIED

- a. the physical transfer of currency across borders between operators by couriers (cash smuggling)
- b. the use of the accumulated currency to purchase easily moveable commodities, which are then exported, subsequently sold, and the cash generated from the sale is provided to the second IVTS operator
- c. as payment for goods to be traded; by smuggling or trading gold and precious gems,
- d. or through invoice manipulation (overcharging or undercharging for goods or services) (known as trade based money laundering).¹¹

51. Individuals may prefer to use IVTS in lieu of formal financial institutions for various reasons, including:

- a. the absence of an adequate, accessible, stable, or secure formal financial system in the destination country
- b. transfers are more efficient, reliable, or cheaper than through formal institutions
- c. avoiding paying higher foreign exchange rates (IVTS operators can set their own exchange rates, which is part of their business marketing and bargaining techniques)
- d. to avoid reporting controls, such as those required under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- e. to avoid paying taxes, and/or
- f. to ensure anonymity and minimise paper trails.

52. The security, anonymity, and versatility of IVTS make it an attractive money laundering mechanism for serious and organised crime groups.

53. IVTS rely on cash being available in countries around the world for the practice of offsetting to operate effectively.

Trade-Based Money Laundering

54. Trade Based Money Laundering (TBML) is a methodology used by serious and organised crime to conceal the proceeds or instruments of crime as legitimate trade. Value can be

¹¹ United States Department of the Treasury: Financial Crimes Enforcement Network. (2003). *FinCEN Advisory Issue 33: Informal Value Transfer Systems*.

UNCLASSIFIED

transferred between individuals on a local and international scale through false-invoicing, over-invoicing, and under-invoicing for services or commodities that are imported or exported around the world.

55. The continued growth in trade, and the involvement of overseas based crime groups in Australia, suggests that TBML could emerge as a significant money laundering channel in the future. It is understood that TBML methodologies are being used as one component or stage of a money laundering process employed by global networks of money laundering facilitators operating across many different countries.

Virtual Currencies

56. Virtual currencies, such as Bitcoin, allow payments to be made online between computer users via peer-to-peer transfers. Virtual currencies are not supported by any traditional bank; however, online exchange houses, such as the former Mt.Gox, which was based in Japan until its collapse in 2014, have been established to facilitate the global exchange of virtual currencies into standard currency, primarily US dollars.
57. The value of virtual currencies fluctuates significantly. Due to their continued increase in value, virtual currencies such as Bitcoin were being seen as a vehicle for investment, particularly by Chinese speculators. Recent media reporting that the Chinese exchange no longer permits customers to trade Yuan for Bitcoin has led to a downturn in their value and, at least for the moment, reduced the attractiveness of Bitcoin as an investment.
58. Unlike regular currency, or electronic funds, virtual currencies are not representative of a physical commodity, though they can be traded (bought or sold) in exchange for standard currency. Typically, this occurs via electronic transfer, like many online purchases; however, in some instances, virtual currencies can be purchased with physical cash through direct deposits into a dealer's bank account.
59. Virtual currencies, like Bitcoin, are entirely electronic, and are stored and traded from personal online wallets, which are computer applications designed specifically to store virtual currencies. Peer-to-peer transfer of virtual currencies can occur instantaneously between wallets without having to transfer via a third party, such as a bank or virtual currency exchange. This offers an entirely legitimate means of transferring value outside of the formal finance sector.
60. The anonymity that this process affords, and the ease with which virtual currencies can be exchanged within and across borders, make them attractive to serious and organised crime. Virtual currencies are also attractive to individuals seeking to engage in criminal activities and the 'darknet', such as the former Silk Road, which relied solely on Bitcoin for the trade in illicit goods, including illicit drugs.

UNCLASSIFIED

UNCLASSIFIED

61. Although virtual currencies such as Bitcoin are seen as vulnerable for exploitation by organised crime seeking to facilitate money laundering activities, evidence that this is occurring on a large scale is yet to be identified.

The Impact of Prevailing Global Economic Conditions

62. Australia's relatively stable economy makes it attractive to legitimate foreign investors and organised crime alike. In particular, the Australian real estate sector is seen as stable, with low risk of significant depreciation in prices in the short term, and strong prospects of growth in the long term. Consequently, it is likely that organised crime, looking for somewhere 'safe' to invest criminal wealth, will be seeking to invest in the Australian real estate market.

UNCLASSIFIED

UNCLASSIFIED

FINANCIAL RELATED CRIMES

63. Key financial crimes impacting on the Australian community and economy include:

- a. investment and financial market fraud
- b. superannuation fraud
- c. revenue and tax fraud, and
- d. card fraud.

64. These crimes are treated separately to money laundering and its individual methodologies due to the role of money laundering as a key enabler of multiple and diverse crimes. Although organised crime groups are known to engage in numerous criminal markets simultaneously, and while the proceeds of the above mentioned crimes can fund other criminal ventures, including the importation and trafficking of illicit commodities, crimes in the mainstream economy are not considered enabling activities.

INVESTMENT AND FINANCIAL MARKET FRAUD

65. Investment and financial market fraud refers collectively to the following types of frauds as they impact on Australians:

- a. fraudulent investment schemes, such as boiler-room fraud¹² (also called cold-call investment fraud) and Ponzi schemes¹³, which attract victims with promises of high financial returns and claims of low risk investment strategies
- b. manipulation or exploitation of the legitimate share market to artificially raise or lower the price of securities for financial benefit – for example, ‘share ramping’ or ‘pump and dump’¹⁴ schemes
- c. exploitation of financial securities¹⁵ to commit fraud or launder or conceal the proceeds of crime – for example, off-market share transfers and fraudulent share schemes.

¹² Boiler-room fraud refers to the unsolicited contacting of potential investors who are deliberately given fraudulent, false, misleading or deceptive information designed to entice them to buy, sell or retain securities or other investments.

¹³ A Ponzi scheme is a type of fraud that uses money from new investors to make interest payments to earlier investors. These schemes typically offer high rates of return and fail when no new investors can be found.

¹⁴ A ‘share ramping’ or ‘pump and dump’ scheme involves the use of false and misleading information to generate investor trading interest to ‘pump’ up the price of a company’s shares. These schemes differ from classic market manipulation because of the use of false and misleading information to affect share prices. The schemes differ from insider trading as they do not involve the illegal use of inside information.

UNCLASSIFIED

UNCLASSIFIED

66. It is noted that some boiler-room frauds promote investment in fraudulent superannuation schemes, or defraud individuals of money that they invest under the auspices of their self-managed superannuation funds (SMSFs). Because of the particular nature of the superannuation market, these schemes are covered in further detail in the 'Superannuation fraud' chapter of this assessment.
67. Australia remains an attractive target for domestic and overseas-based organised crime involved in investment fraud, because of its comparatively stable economy, and Australian investors' high subscription to share purchases.

Fraudulent investment schemes

68. Boiler-room fraud is a complex, sophisticated and mostly transnational activity that generates significant illicit profits with minimal risk of disruption, making it attractive to organised crime. The global economic downturn may have benefited serious and organised crime involved in boiler-room fraud, as investors who are receiving low interest on their savings, or low dividends on their investments, become susceptible to schemes offering higher than usual returns. Task Force Galilee found that the Australian victims of boiler-room investment frauds saw the schemes as attractive because of the economic climate at the time, in which returns on traditional investments, such as Australian shares and property, were very minimal and investors were seeking alternative investment opportunities.
69. The majority of boiler-room fraud targeting Australians is currently understood to be perpetrated from bases offshore, but a new domestic investment fraud threat has recently been identified. Recent legislative changes have seen the introduction of the Future of Financial Advice (FOFA) reforms, which aim to improve the trust and confidence of Australian retail investors. A key component of these reforms is regulating the types and amount of commissions that can be charged by brokers/advisers and the types of investment products for which they can charge commissions. These changes commenced on 1 July 2012, with compliance mandatory from 1 July 2013.
70. Although regulation in the area of providing financial advice has tightened, the AFS licensing process still has limitations. The process is a point-in-time assessment of the licensee entity, not of its owners or employees, and does not guarantee the probity or quality of the licensee's services, or that investors cannot incur a loss from dealing with the AFS licensee. Although regulators conduct probity checks, which include police checks and bankruptcy searches on applicants for an AFS licence, it may be difficult to

¹⁵ The large number of securities on offer in Australia include shares, bonds, derivatives and managed funds.

UNCLASSIFIED

establish previous involvement in fraudulent activity either in Australia or in other international jurisdictions.

71. The mining and resource sectors pose unique and significant risks of exploitation for investment fraud purposes. The potential yield of the investment product marketed to potential investors is speculative by nature and based on claims by industry professionals. Organised criminals perpetrating this type of fraud in Australia are understood to have paid geologists and company research firms to fraudulently inflate the potential of mining tenements and exploration projects, which are then marketed to unsuspecting investors.
72. As with the speculative nature of capital raisings in the mining and resources sector, biotech and pharmaceutical development securities are vulnerable to exploitation by organised crime for investment fraud purposes. Because of the number of years that it can take from proof of concept stage to establishing a viable operation, it is very difficult for investors to determine whether a promoted product is fraudulent.
73. Due to the relatively low perceived risk of detection by law enforcement, and the substantial illicit profits to be earned, some organised criminal entities previously involved in other illicit markets are now becoming involved in investment fraud.
74. Investment and financial market fraud is complex, difficult and resource intensive for law enforcement and regulators to investigate. In the case of law enforcement, new professional skills and new capabilities are often required, and investigations can be protracted. All of these factors limit the number of investment fraud cases that can be investigated

Manipulation of the share market and exploitation of financial securities

75. Organised crime is increasingly involved in financial market fraud. Some of these frauds are transnational, with separate networks in different jurisdictions.
76. Task Force Wickenby investigations have increased the level of understanding of the risks posed to Australian investors by the abusive use of the securities market and secrecy jurisdictions. Of primary concern is the opacity of the beneficial ownership of Australian listed shares, which provides the opportunity for organised crime entities to hide their involvement in fraudulent and other illegal activities, including money laundering and tax evasion.
77. A significant proportion of shares listed on the Australian Securities Exchange (ASX) are owned by non-residents, with the beneficial owner of these shares sometimes obscured by the use of nominee or custodial service provider (CSP) arrangements. Foreign ownership of Australian shares and ownership through CSPs are not illegal, but these types of arrangements impair the ability of law enforcement and regulators to identify

UNCLASSIFIED

UNCLASSIFIED

the beneficial owner of the shares, giving organised crime an opportunity to facilitate illegal activities anonymously.

78. Given the size of the market involved, the opacity of the beneficial ownership of Australian shares represents a significant risk and provides opportunity for misconduct or illegal activities, including market manipulation, insider trading, tax evasion, money laundering and criminal infiltration of the market by organised crime groups, who can hide their identities behind offshore structures and nominees.
79. Law enforcement has seen the emergence of overseas and secondary securities markets being used by individuals wishing to bypass comparatively stringent recording and disclosure regulations imposed by the larger mainstream markets when listing securities for sale to the public. Second-tier stock exchanges such as the National Stock Exchange (NSX)¹⁶ have less stringent requirements with regard to the character and background of company directors, which makes it easier for those with a criminal background to be involved in listing companies. Once listed on a stock exchange, companies selling fraudulent stocks have a mechanism for taking money from unsuspecting investors.

New threats

80. Globalisation and innovation will continue to result in the creation of new investment products, services and technologies that may be used to facilitating investment and financial market fraud in the future. Recently, foreign exchange trading fraud in Australia has emerged, particularly using online trading platforms. Foreign exchange trading – speculating on the value of one currency against another – is particularly vulnerable to exploitation by organised crime as there is no central exchange for the market in the way that there is for securities. Consequently, it is largely unregulated and very volatile.
81. Given the size of the global foreign exchange market, the volume of transactions, the lack of regulation and the volatility of the market, investment fraud syndicates are likely to see the foreign exchange market as a vehicle for defrauding investors globally.
82. Although evidence of organised crime involvement in foreign exchange trading fraud in Australia has yet to be identified, cases have been prosecuted in the US. The US Commodity Futures Trading Commission (CFTC) reports that it has witnessed a sharp rise in foreign exchange trading frauds in recent years. The perpetrators of these frauds have been seen to use ‘wealth creation’ webcasts, webinars, podcasts, emails and other

¹⁶ The National Stock Exchange (formerly the Newcastle Stock Exchange) provides small or emerging companies with a platform to list securities. The market capitalisation requirements to list on the NSX are considerably lower than those for the ASX (A\$500,000 compared with A\$10 million).

UNCLASSIFIED

UNCLASSIFIED

online seminars on the internet to solicit clients worldwide. One scheme in particular accepted at least US \$53 million from at least 960 clients worldwide, including from investors in Australia.¹⁷

SUPERANNUATION FRAUD

83. The superannuation industry in Australia encompasses a complex array of fund types, ranging from ‘do-it-yourself’ funds – or self-managed superannuation funds (SMSFs), which are regulated by the Australian Taxation Office (ATO) – to large industry and retail funds that are overseen by the Australian Prudential Regulation Authority (APRA). Because of the inherent complexities of this industry, a range of opportunities exist for fraud, including the theft of contributions and fund assets, fraudulent fund investments, non-existent schemes and excessive fees charged by advisers.
84. There are a number of factors that make the Australian superannuation sector particularly attractive to organised crime:
- a. With a compulsory superannuation regime, and superannuation assets in Australia currently estimated at A\$1.3 trillion, highly sophisticated offshore organised fraud networks have established, and will continue to establish, complex fraudulent schemes to steal superannuation savings.
 - b. Superannuation assets continue to increase and at 30 June 2013 were estimated to be \$1.62 trillion.¹⁸
 - c. There is a very large pool of compulsory superannuation savings, with an incremental increase in compulsory contributions to 12 per cent due by 2019.
 - d. Many Australians are disengaged from their superannuation, rarely checking the balance or performance of their fund, which increases the risk that detection of any fraud will only occur upon retirement.
 - e. The complex nature of superannuation regulation in Australia, in which different regulatory bodies, including the Australian Securities and Investments Commission (ASIC),¹⁹ APRA and the ATO all have separate and distinct roles, makes it difficult to trace malfeasance across the sector.

¹⁷ <<http://www.cftc.gov/PressRoom/PressReleases/pr6353-12>>, viewed 9 January 2014.

¹⁸ Australian Prudential Regulation Authority, Statistics, Quarterly Superannuation Performance, June 2013 (issued 22 August 2013), page 5

¹⁹ ASIC’s role in connection with the superannuation industry is in relation to regulation of the licensing of financial service providers.

UNCLASSIFIED

85. The Australian superannuation industry maintains investments totalling \$1.62 trillion, with \$970 billion or 60 per cent of that sum contained in APRA-regulated funds, \$506 billion or 31 per cent in SMSFs and the remainder in public sector and other schemes.²⁰ These investments are equivalent to about 120 per cent of the Australian share market capitalisation and 90 per cent of Australia's annual gross domestic product (GDP).²¹ Australian superannuation is expected to achieve continued growth as a result of the tax advantages derived from it and the compulsory nature of the Superannuation Guarantee, and will accumulate almost \$7 trillion (130 per cent of GDP) over the next 25 years.²² Therefore the Australian superannuation industry is a major contributor to the Australian financial sector and is a source of wealth attractive for targeting by opportunistic individuals and organised crime.
86. The Australian superannuation industry is broadly segmented into funds regulated by APRA, including industry funds, corporate funds, retail funds and public sector funds, and SMSFs regulated by the ATO. Nearly one-third of all superannuation assets now reside in SMSFs, with the average account holder's balance for these funds as at June 2012 being \$525,000. With SMSFs the fastest-growing area of superannuation, some commentators have characterised them as 'the vehicle of choice for the wealthiest 945,000 Australians'.²³
87. Traditionally, SMSFs have been more attractive for fraudulent exploitation than APRA-regulated funds as they are self-managed and not prudentially regulated, with ultimate responsibility and risk associated with investments residing with individual trustees and members. The fact that SMSFs hold, on average, the largest balance of superannuation assets provides an opportunity for low-volume, high-impact fraud on individual funds that may be managed by financially inexperienced individuals.
88. A common methodology traditionally used by organised crime committing superannuation fraud has been to target APRA-regulated superannuation funds and then to rollover these funds into an SMSF where they are accessed illegally, bypassing provisions that prohibit access to funds until retirement. This methodology circumvents

²⁰ Australian Prudential Regulation Authority 2014, *Annual superannuation bulletin, June 2013*, issued 9 January 2014, viewed 13 January 2014.

²¹ KPMG 2012, *Evolving Superannuation Industry Trends*, November 2012, Retrieved 16 December 2013, from <www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/evolving-superannuation-industry-trends.pdf>.

²² Australian Government Budget 2012–13, Budget Paper, Canberra. Retrieved 16 December 2013 at <www.budget.gov.au/2012-13/content/bp1/html/bp1_bst4-03.htm>.

²³ Tim Mackay 2013, 'Advanced SMSF strategies', *Charter* magazine, Institute of Chartered Accountants Australia, July 2013.

UNCLASSIFIED

UNCLASSIFIED

the usually strong controls of APRA-regulated funds, but its effectiveness has now been reduced by changes to the rollover process.

89. A more sophisticated and resource-intensive methodology used to commit superannuation fraud involves directly targeting superannuation funds through a network of financial advisers who promote investments in fraudulent schemes, particularly offshore investments. This methodology for targeting potential superannuation fraud victims remains a high risk, but at present the extent of these activities is not known.

90. Methodologies used by organised crime in committing superannuation fraud include:

- a. the use of trusted professionals such as financial planners, who are complicit in the fraud
- b. the deliberate use of investment structures that are complex, multi-layered and opaque, and in foreign jurisdictions
- c. increased use of technology and cybercrime

91. As SMSFs and APRA-regulated superannuation funds transition more to the online environment, there is potential for superannuation funds to fall victim to high-tech crime. With online processing systems, superannuation funds may fall victim to phishing and key logging scams.

92. The risk of serious financial crime has materialised in collapses such as Trio Capital. Trio Capital “was the largest superannuation fraud in Australian history. Roughly \$176 million in Australians' superannuation funds is lost or missing from two fraudulent managed investment schemes.”²⁴

²⁴ Parliamentary Joint Committee on Corporations and Financial Services into the collapse of Trio Capital, May 2012 Report page 17

UNCLASSIFIED

REVENUE AND TAX FRAUD

93. Revenue and taxation fraud involves the intentional and dishonest evasion of tax obligations. The ATO is responsible for the administration of tax products, which include income tax, goods and services tax (GST) and excise. Revenue and taxation fraud has the potential to adversely impact on revenue collected and refunds paid, undermine self assessment and voluntary compliance which underpins the taxation system, and affect public confidence in the integrity of tax administration.
94. Organised criminal groups and significant criminal individuals based in Australia and overseas are exploiting Australia's tax system, primarily through fraudulent refund activity. However, the information and intelligence currently available indicate that the level of traditional organised crime involvement in revenue and tax fraud is low. Those involved in this crime type display varying levels of expertise and sophistication, often matched to the complexity of the fraud committed, and increasingly rely on technology to support their activities.
95. Revenue and tax fraud by organised criminals is often enabled by a myriad of complex business and trust structures and professional facilitators, such as tax agents, accountants and legal experts – some of whom may be complicit in the fraud. Identity crime is also used to enable this type of fraud. The creation of 'corporate vehicles' such as companies or trusts in secrecy jurisdictions²⁵ by professional facilitators allows organised crime to conceal the beneficial ownership of those companies, as well as masking the true purpose behind the establishment of the companies.
96. In relation to refund fraud, some of the methods identified as being used by organised crime are:
- a. deliberate falsification or overclaiming of input tax credits, deductions, offsets or expenses
 - b. failure to declare income where there is an obligation to do so – which can lead to the payment of a higher refund
 - c. the use of false information or identity details to claim a refund
 - d. using stolen, purchased or fabricated proof of identity documents to obtain a tax file number (TFN) or GST registration in a real or false name

²⁵ Secrecy jurisdictions are those jurisdictions in which legislation governing the banking and finance sector is intended to protect the privacy of those incorporating companies in that jurisdiction.

UNCLASSIFIED

- e. theft, purchase or borrowing of another person's TFN and/or Australian business number (ABN) to lodge fraudulent claims using a third-party identity.

97. Two examples of organised, systematic attacks on the tax system in the last 12-18 months are:

- a. an attack consisting of large number of fraudulent claims for tax refunds, using stolen identities, executed by a syndicate outside of Australia; and
- b. a sustained, systematic series of fraudulent refund claims which continued – and adapted – even as we actively investigated the syndicate.

Phoenix Schemes

98. Phoenix activity is the deliberate and systematic liquidation of a corporate trading entity which occurs with the fraudulent or illegal intention to:

- a. avoid tax and other liabilities, such as employee entitlements
- b. continue the operation and profit taking of the business through another trading entity.²⁶

99. A new company is created to carry on the same or similar business, typically with the same ownership. Fraudulent phoenix activity threatens the integrity of the tax revenue and superannuation systems, deprives the community of necessary funds for essential services, and provides phoenix operators with an unfair competitive advantage against businesses operating legitimately in the same sector. The act of “phoenixing” reduces integrity in regulatory systems by being used to avoid enforcement and/or payment of liabilities or obligations such as court imposed fines and orders; contractual and statutory obligations; compensation payouts; current/future warranty claims; defect/rectification claims, etc. The taxation products and obligations most at risk from fraudulent phoenix activity include PAYGW, GST, Superannuation Guarantee and Income Tax.

100. In a 2012 report prepared by PricewaterhouseCoopers (PwC) entitled, '*Phoenix activity: Sizing the problem and matching solutions*' the total impact of phoenix activity was estimated to be \$1.78 –\$3.19 billion per annum, comprising:

- a. The cost to employees - \$191 million - \$655 million per annum

²⁶ The Fair Work Ombudsman research report into phoenix activity in Australia, *Phoenix activity, Sizing the problem and matchingsolutions*, June 2012, Page 2

UNCLASSIFIED

- b. The cost to business - \$992 million and \$1.93 billion per annum
- c. The cost to government revenue - \$601 million - \$610 million per annum
- d. Therefore total cost on the Australian economy (which excluded unpaid SG) was estimated to be between \$1.79 billion and \$3.19 billion per annum.²⁷

101. The ATO has identified an increase within the known fraudulent phoenix population of individuals with criminal links. Of great concern is the emerging number of professional advisers who hold tax or legal qualifications and promote or facilitate fraudulent phoenix behaviour.

102. In recognition of the threat posed by phoenix operators, the Federal Government announced in the May 2013 budget a funded measure for Standard Business Reporting and the Australian Business Register (ABR). This concerns establishing a phoenix 'watch list' database of people who have engaged in phoenix activity, or have a high likelihood of doing so in the future. This measure will facilitate information exchange between the Australian Securities & Investments Commission, Fair Work Ombudsman, State & Territory Revenue Agencies and the ATO, and aims to permit these agencies to better target their activities and improve their management of the phoenix risk.

²⁷ PwC, *Phoenix activity: Sizing the problem and matching solutions*, June 2012

UNCLASSIFIED

CARD FRAUD

103. Card fraud is defined as the fraudulent acquisition and/or use of debit and credit cards, or card details, for financial gain. Card fraud may involve acquiring legitimate cards from financial institutions by using false supporting documentation (application fraud), or stealing legitimate credit and debit cards. It may also involve phishing,²⁸ card-not-present fraud, the creation of counterfeit cards, hacking into company databases to steal customer financial data, and card skimming.
104. In Australia, as in many other developed nations, there has been an increase in the use of credit and debit cards as a method of payment for goods and services, including over the Internet. Although this increase has provided greater convenience for consumers, it has been accompanied by higher levels of fraud and theft of funds in relation to electronic transactions.
105. The Australian Payments Clearing Association (APCA) has reported that, for the financial year 2012–13, there were just fewer than 1.4 million frauds perpetrated using Australian-issued cards. This is an increase from 2011–12, when just over 1.2 million frauds occurred, and 2010–11, when just over 950,000 frauds occurred. The value of card fraud transactions also increased in 2012–13 to \$280.5 million, compared with just over \$270 million in 2011–12 and \$238 million in 2010–11.
106. Card-not-present fraud is the largest segment of the card fraud market, representing nearly 81 per cent of card fraud transactions and 76 per cent of the transactions' value in 2012–13, according to APCA figures. Though the number and value of card-not-present frauds increased in 2012–13, the rate of growth in card-not-present fraud, in terms of both the number of transactions and their overall value, slowed in 2012–13. This is represented in Table 1.

²⁸ Phishing refers to attempts to obtain sensitive personal and banking information (such as bank account numbers, passwords and credit card numbers) to be used for criminal gain. Criminals send emails making false claims in order to trick users into revealing personal details, or establish fake websites, with links sent through electronic communication including email, instant messaging, texts and online advertising.

UNCLASSIFIED

Table 1: Percentage increase in volume and value of card-not-present fraud on previous financial years

Financial year	Percentage increase in number of card-not-present transactions on the previous year	Percentage increase in the total value of card-not-present transactions on the previous year
2010–11	38 per cent	53 per cent
2011–12	27 per cent	16 per cent
2012–13	15 per cent	5 per cent

107. The increase in card-not-present fraud is likely to be the result of a confluence of factors such as improved security measures to prevent point-of-sale fraud – including the introduction of personal identification number (PIN) and chip technology – the displacement of organised crime previously involved in large-scale card skimming, and a continual increase in online spending by Australians.

108. The introduction of PIN and chip technology in Australia has reduced the opportunities for organised crime to engage in fraudulent credit card transactions at the point of sale where the card being used to make the purchase is physically present. This is because a card’s unique chip is used to verify the transaction details, rather than the magnetic stripe. Although the banking sector is moving toward the use of PIN and chip technology for all Australian-issued cards, the replacement of all non-chip cards may take several years to complete.

109. Technology-based improvements in ATM, EFTPOS and card security will also continue to influence card fraud methodologies used by serious and organised crime groups. As technology continues to enhance security features, organised crime will develop countermeasures.

110. Overseas-based organised crime groups continue to target Australia for card fraud, with Asian and Romanian card skimming syndicates having recently received coverage in the media. Some of these syndicates are involved in activity in multiple crime markets, with the funds obtained from card fraud being used to support other lines of illicit business.

Case study: Romanian crime syndicate A\$30 million card fraud

In November 2012, 16 members of a Romanian crime syndicate were arrested in a joint Australian Federal Police and Romanian National Police operation in Romania. The syndicate exploited weaknesses in the security systems of 100 Australian small businesses, which were hacked to steal the credit card details of up to 500,000 Australians who had used their cards at the businesses to buy goods or services.

UNCLASSIFIED

UNCLASSIFIED

Though investigators have not been able to establish exactly how many card details were stolen from the Australian businesses, 30,000 of them had, at that time, already been used to illegally buy goods worth more than \$30 million.

The stolen credit card data was allegedly used to create fake credit cards, enabling thousands of counterfeit transactions to be carried out around the world, including in Europe, Hong Kong, Australia and the United States.

111. The existence of black market web portals – underground forums set up by criminals to openly trade in a range of illicit commodities, including stolen banking details – allows OCGs to purchase credit card numbers for less than A\$1 each if bought in bulk. Further details such as cardholder name and expiry date can be purchased for about A\$7, and full card details, including identity data, can be bought for between A\$70 and A\$80.²⁹ The ability to purchase and trade sensitive card data and customer information through the Internet is almost certain to enable organised criminal involvement in card-not-present fraud, and may also contribute to identity fraud in instances where full identity details are purchased.
112. The use of internet-capable mobile devices to conduct financial transactions continues to increase. However, an estimated 50 per cent of people using mobile phones for online transactions do not use basic precautions such as passwords, security software or back-up files for their mobile device.³⁰ These types of behaviours allow organised crime to continue targeting devices to gain information for fraudulent use.

²⁹ Commonwealth of Australia 2010, Official Committee Hansard: House of Representatives – *Standing Committee on Communications*, 17 March 2010, Canberra.

³⁰ Opperman, Ian 2013, 'Sneaky cyber thieves cloud digital future', *Australian Financial Review*, 26 November 2013.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED



© ACC 2011. All rights reserved.