SERIOUS FINANCIAL CRIME

THEME SUMMARY

The ACIC has identified five key elements of financial crime:

- cybercrime
- investment and financial market fraud
- revenue and taxation fraud
- superannuation fraud
- card fraud.

Financial crimes are diverse in nature and scale, and in the level of harm they cause. The modern globalised economy and advances in technology create new opportunities for organised crime to exploit vulnerabilities for illicit profit. The expansion of serious and organised crime into the financial sector poses a significant risk to the integrity of the Australian economy, financial markets, regulatory frameworks and revenue collection. This risk is particularly salient in the current economic environment, where damage to financial markets, government revenue base and the savings of private individuals can have far-reaching implications.

Conservative estimates put the cost of organised fraud[28] to the Australian economy at A$6.3 billion between 2013 and 2014—including revenue and tax evasion, superannuation fraud, card and financial transaction fraud. The intermingling of licit and illicit financial transactions makes it difficult to fully assess the extent of financial crime in Australia. The complexity and potential scale of financial crime poses an ongoing challenge not only to law enforcement but also to regulators.

CYBERCRIME

Cybercrime against individuals, businesses and governments can be conducted from anywhere in the world. The threat to Australia from cybercrime is transnational in nature with the majority of cybercrime affecting Australia originating from Russia and Eastern Europe. The primary threat is from temporary networks of people who collaborate but may live in geographically diverse locations. This means that cybercrime activities are inherently difficult to investigate.

Cybercrime is defined[29] as:

> crimes where computers or other information communications technologies are an integral part of an offence, such as online fraud, identity crime and the distribution of child exploitation material.

28 The cost of government support for victims, based on the approximate size of the illicit activity and the percentage of serious and organised crime involvement.
29 Australian Cyber Security Centre 2015, *ACSC 2015 Threat Report*, ACSC, Canberra, p.8.

Cybercrime is a low-risk, high-return criminal enterprise with potentially lucrative financial gains. Australia's high levels of technology use and relative wealth ensure the persistence of the cybercrime threat in Australia. The principal forms of serious and organised cybercrime affecting Australia involve ransomware, credential-harvesting malware, and distributed denial of service (DDoS) extortion. Computers and devices of private individuals and commercial entities as well as government systems are all at risk from cybercrime.

RANSOMWARE

Ransomware is a form of malware that stops a victim from using their computer, or files, until a sum of money is paid to a cybercrime actor. It targets a victim's computer via malicious emails and websites. Once installed, ransomware encrypts the victim's files, and then directs the victim towards a webpage with instructions on how to pay a ransom for their data to be decrypted. Cybercriminals have used ransomware to demand payments from A$500 to A$3,000 (in bitcoin), with some businesses subjected to targeted attacks requesting tens of thousands of dollars. In 2016, the ransomware Cryptolocker was discovered on the computer system of an Australian government agency after an employee clicked on an Australia Post-themed email. Cryptolocker re-imaged the staff member's workstation, resulting in thousands of files stored on an associated government server being encrypted by the ransomware.
The most effective ransomware campaigns in Australia use the branding of trusted and well-known Australian corporations as part of their social engineering techniques.

Australian government organisations have also been targets of credential-harvesting emails. Such emails direct users to access a document via a shared drive that subsequently requests credentials be entered in order to access the document. Once an email account has been compromised, the contacts within the account are then sent malicious emails appearing to be from the legitimate and trusted source.

CASE STUDY: ONGOING CYBERCRIME AGAINST FINANCIAL INSTITUTIONS

Malware continues to be used by cybercriminals to attack commercial and private enterprise. The Gozi Trojan, first discovered in 2007, is one of the longest-operating banking Trojans.

Despite three of its developers being arrested by the United States Federal Bureau of Investigation in 2013, Gozi and its various iterations continue to be used by multiple cybercriminal groups, posing a persistent threat to the financial sector. In 2016, Gozi was identified as active in Australia, Canada, Italy, Japan and Spain, amongst other nations.

In February 2016, cybercriminals fraudulently diverted US$851 million from the Bangladesh Bank. The cybercriminals infected the Bangladesh Bank's SWIFT payment system with malware that allowed them to deactivate system integrity checks, alter payment details, and suppress notification of the altered payments. While the majority of the stolen funds were recovered, US$81 million remains outstanding.

The successful theft of US$81 million highlights the significant financial rewards that can be obtained by directly targeting bank systems rather than bank customers. This has resulted in several cybercrime groups taking an increased interest in finding and exploiting vulnerable SWIFT systems. While less-developed countries have been attacked initially, Australia is also a potential target.

CREDENTIAL-HARVESTING MALWARE

Mirai is an example of malware that is comparatively unsophisticated; the source code is readily available for use by actors at the lowest levels of sophistication. Mirai malware turns Internet of Things[30] devices into 'bots' to be used by actors for malicious purposes such as DDoS. Mirai operates by scanning the internet for a suite of devices with known default credentials, including DVRs, printers and home internet routers. It uses those credentials to install itself onto the device, and then scans the internet for new vulnerable devices to infect. Despite its relative simplicity, Mirai has been used to implement some of the largest DDoS incidents.

On 20 September 2016, the Mirai botnet launched a DDoS attack against OVH, a major web hosting company based in France. A DDoS attack was also launched against the website of an independent IT security journalist, Brian Krebs, forcing his website offline despite it being protected by one of the leading DDoS protection services, Akamai. Regardless of its relative simplicity, this attack by Mirai was considered one of the largest DDoS attacks ever seen.

DDOS EXTORTION

DDoS extortion occurs when a specific cyber-actor threatens to launch DDoS activities against an organisation unless a fee is paid. DDoS extortion threats have been raised against small, medium and large businesses including financial institutions in Australia. The instances of DDoS extortion have increased, with threats coming from both domestic and international serious and organised criminal syndicates.

BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) is a cybercrime scheme that targets large and small businesses for financial gain. BEC can take many forms but most commonly involves impersonating a high-level employee in order to change invoice details or request immediate funds transfers. BEC requires few technical skills; most effort is spent on social engineering and research on targets.

BEC is starting to gain ground in Australia and—since the inception of ACORN in November 2014—victim reports have increased. Due to its increasing prevalence, BEC is now being quantified in Australia for the first time. Analysis of ACORN data found 749 cases reported in the 2015–16 financial year, and 243 cases reported within the first quarter of the 2016–17 financial year.

30 The Internet of Things (IoT) is made up of physical objects that have embedded network and computing elements, and communicate with other objects, or computers, over a network, usually the internet.

INVESTMENT AND FINANCIAL MARKET FRAUD

Domestic and transnational serious and organised crime groups involved in investment and financial market fraud continue to target Australia. Online platforms and exploitation of markets are playing an increasingly important role in investment and financial market fraud, which refers to three different types of fraud:

- fraudulent investment schemes, such as boiler-room fraud and Ponzi schemes[31]
- manipulation or exploitation of the legitimate share market to artificially raise or lower the price of securities
- exploitation of financial market securities to commit fraud or to launder the proceeds of crime—for example, off-market share transfers and fraudulent share schemes.

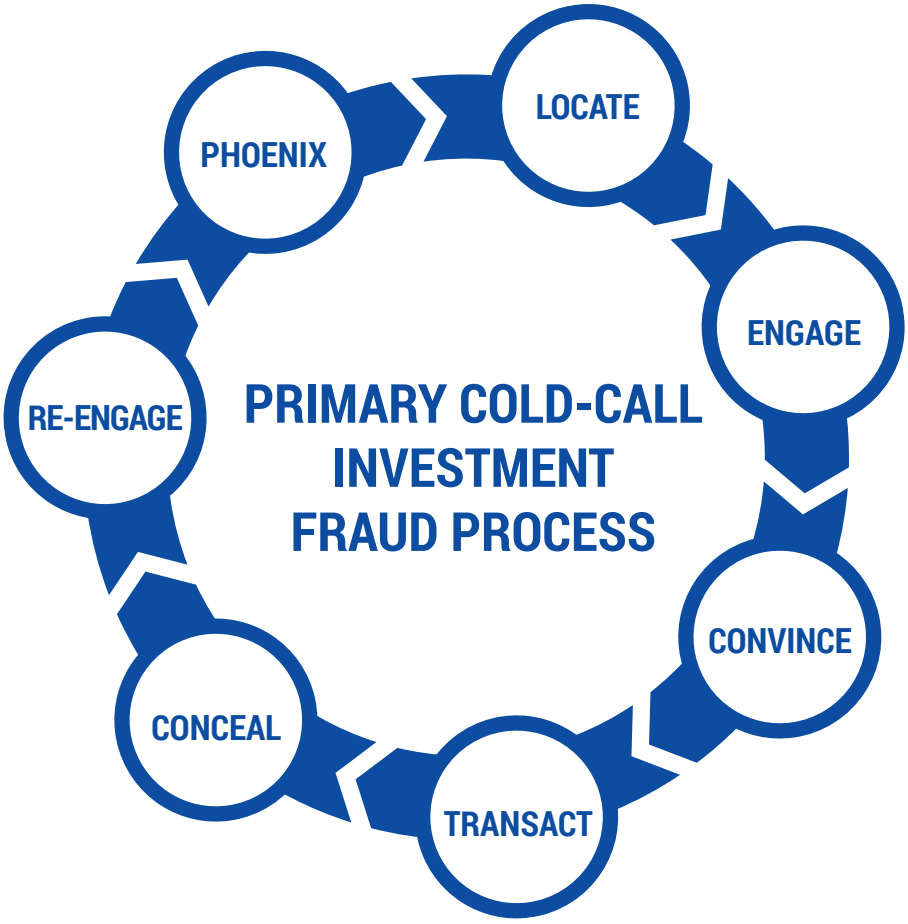
Boiler-room or cold-call investment fraud operations pose an enduring issue for law enforcement. In January 2017, a 51-year-old man was extradited from South Australia to face five counts of fraud in Queensland over his alleged involvement in multiple Gold Coast-based investment companies offering shares in products that were ultimately flawed. Approximately A$6 million was taken from unsuspecting individuals who had invested in predictive betting software that promised to provide high levels of financial returns accompanied by tax-free gains. Once delivered, the software failed to work and the organisers of the scheme refused to return the funds to investors.

The availability of computer programs that create orders to buy and sell securities has provided further opportunities for serious and organised crime groups to engage in market manipulation. These computer programs create artificial interest in a particular security by driving the price either up or down. Once this has occurred, securities that are held can be sold (at a higher price) or bought (at a lower price). Such activity is known as ‘spoofing’.

CASE STUDY: TRANSNATIONAL ELECTRONIC MARKET MANIPULATION

In mid-2015, an online share-trading account was created by an individual believed to be based in Russia. This account was used to purchase Australian-market-listed securities. The individual was also able to gain access to a number of other legitimate share-trading accounts and raise funds through the sale of shares held within them. These funds were then used to purchase shares in the same companies as those held in the recently created share-trading account, thereby pushing up the price. Once the price had increased to a certain level, the individual sold the original shares, realising a profit. In this instance, the scheme was detected and authorities were able to stop the transfer of the profits offshore.

31 A Ponzi scheme is a fraudulent investment scam where a promoter promises investors a return on investment, but this return is generated from new capital obtained from new investors rather than profit earned from legitimate sources. Operators usually entice new investors by offering higher returns than other investments. The scheme often falls apart because the promoter starts to spend the money too quickly or the pool of investors dries up.



LOCATE	Telemarketer cold calls potential victims offering investment opportunities.
ENGAGE	Follow up contact from a sales consultant who uses an established 'script' to entice potential victims to enter into a contract with the company.
CONVINCE	Further sales techniques are employed to convince potential victims to invest, often including repeated calls and referrals to the company website that appears legitimate.
TRANSACT	The victim enters into a contract with the company and transfers funds–often between A$5,000–50,000.
CONCEAL	Invested funds are withdrawn/transferred to a separate bank account controlled by the parent syndicate. The victim's trading account may appear to be growing on the company website, but they are unable to access their investment funds.
RE-ENGAGE	The victim is re-contacted and offered upgraded investment package options to invest further funds.
PHOENIX	Company income decreases as the availability of potential victims is reduced–often a direct result of bad publicity. The parent syndicate folds the company and the scheme is re-launched under a new company name.

REVENUE AND TAXATION FRAUD

Revenue and taxation fraud involves the intentional abuse of the taxation system with the aim of obtaining financial benefit. It encompasses numerous non-compliant activities and can result in criminal sanctions such as fines or imprisonment. Such activities range from failing to report income in order to avoid taxation obligations to the use of complex offshore secrecy arrangements, also to evade tax. The use of professional facilitators continues to be a key enabler of revenue and taxation fraud, most notably in fraudulent phoenix activity, offshore tax evasion and the abusive use of trusts.

The Australian Taxation Office (ATO) is the principal revenue collection agency of the Australian Government and is responsible for the administration of tax products, which includes administering both income tax and the goods and services tax. In the last six months of 2016, the ATO reports tax crime investigations led to:

- 138 fraud charges
- 10 jail terms
- the seizure of illegal tobacco plants and illegal stills with a total potential excise value of more than A$18.7 million
- the execution of six search warrants relating to fraudulent phoenix activity
- the identification of attempted taxation fraud worth A$1.4 million
- the identification of false taxation claims of over A$10.8 million.

It is estimated that fraudulent phoenix activity costs the Australian economy A$3.2 billion each year. Fraudulent phoenix activity involves the deliberate liquidation of a company in order to avoid paying creditors, taxes and employee entitlements. Once a company has been liquidated, the perpetrators transfer the remaining assets to a new entity and continue to operate the same or a similar business under a new name, retaining the same ownership. The end results of phoenix activity are financial loss to suppliers due to unpaid debits; financial loss to employees through unpaid superannuation entitlements; and loss to the community due to unpaid taxation revenue.

Professional facilitators are key enablers of offshore tax evasion, as a high level of expert knowledge is required to successfully establish and operate large-scale fraud and tax evasion activities while avoiding detection. Australia-based facilitators have been seen to promote the services of offshore financial service providers. Facilitators include professionals in the import/export, accounting, legal, money remittance, finance, insurance and ICT industries. There is also evidence of superannuation and estate planning structures and strategies being part of integrated tax evasion design by private wealth groups.

Globalisation and technological advances have made it easier for individuals to hold investments in offshore financial institutions, increasing the opportunity for tax evasion. In April 2016, 11.5 million documents were leaked from the Panamanian law firm, Mossack Fonseca, exposing how secretive offshore tax regimes can be exploited to conceal wealth and evade tax. The leaked documents revealed the names of more than 1,000 Australians. Eighty of these names were matched with the ACIC's criminal intelligence holdings, and several were recorded on the National Criminal Target List.

The significance of the exploitation of offshore secrecy arrangements to evade tax is observed in recent advice provided by the ATO that, on the successful completion of Project Wickenby,[32] over $2.2 billion in tax liabilities had been raised and 46 criminal convictions secured.

While the establishment of an offshore structure or trust is often for a genuine purpose, many structures and trusts are being used to evade tax, to avoid corporate responsibility, to disguise and hide unexplained wealth, to facilitate criminal activity, and to launder the proceeds of crime. It remains difficult to identify the level of involvement by serious and organised crime in the abusive use of trusts due to the inherent complexity of the legislative and regulatory frameworks surrounding trusts and trust structures. Revenue and taxation fraud will remain a long-term issue for law enforcement as interactions between key enablers such as technology, identity crime and professional facilitators become increasingly complex and frequent.

SUPERANNUATION FRAUD

Australia's large pool of superannuation savings continues to be an attractive target for organised crime groups. The complex nature of superannuation schemes offers a range of opportunities for fraud including the theft of contributions and fund assets, fraudulent fund investments, non-existent schemes, and excessive fees charged by advisers.

The volume of funds held in superannuation schemes in Australia is significant: over 14.8 million Australians held a super fund account as at 30 June 2016, and approximately 43 per cent of those have more than one super account.

There are various superannuation schemes available in Australia, including MySuper, retail funds, industry funds, public sector funds, corporate funds, rollover funds and self-managed super funds (SMSFs). The Australian Prudential Regulation Authority (APRA) supervises regulated superannuation funds (other than SMSFs), approved deposit funds, and pooled superannuation trusts—all of which are regulated under the *Superannuation Industry (Supervision) Act 1993.*

APRA is responsible for over A$2,198 billion in superannuation assets. APRA-regulated superannuation funds are susceptible to targeting by serious and organised crime groups: a recent increase has been observed in the use of targeted online methodologies to fraudulently access an individual's superannuation account. Superannuation funds are responding to this activity by developing data analytic capabilities designed to detect unusual or suspicious activity.

SMSFs are particularly vulnerable to incidents of fraud, in part due to the desire of individuals to source and control their own investments. At the end of the 2015–16 financial year, Australians held A$622 billion in SMSFs—a substantial and attractive pool of funds to serious and organised criminal groups.

AUSTRAC plays an important role in combating superannuation fraud, and continues to receive reports from industry on the use of fraudulent documentation in support of claims for early release of superannuation benefits or death and disability insurance payments.

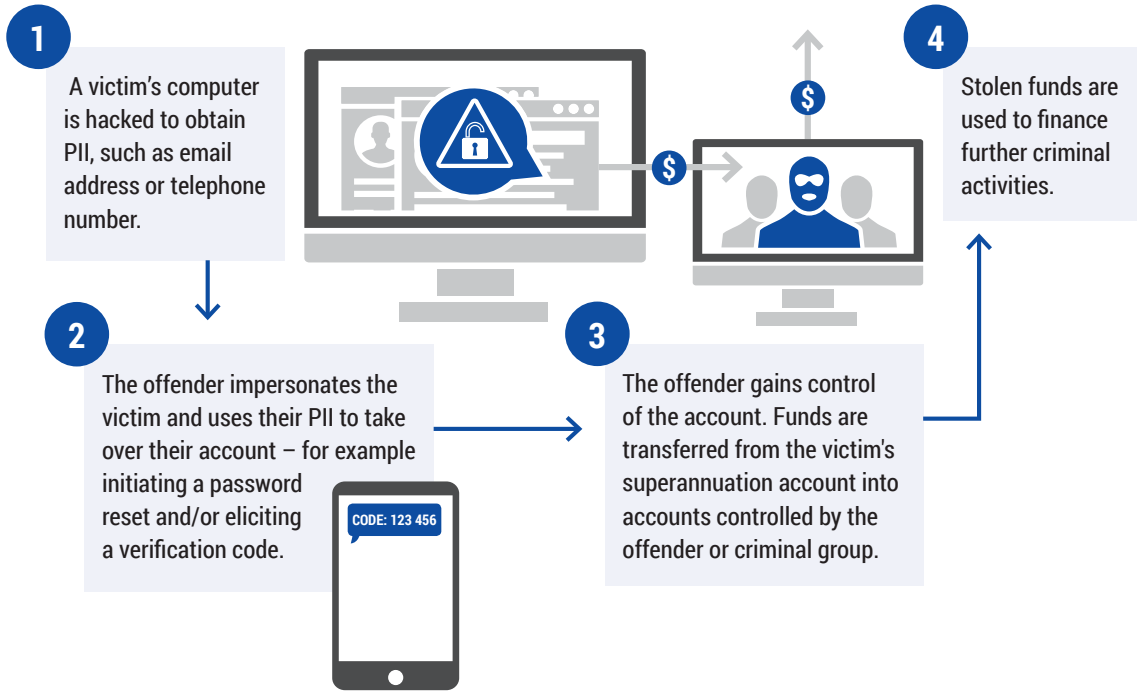
32 Project Wickenby, a cross-agency task force, was established in 2006 to protect the integrity of Australia's financial and regulatory systems by preventing people from promoting or participating in the abuse of offshore secrecy arrangements.

Individuals who have reached preservation age[33] are particularly vulnerable to theft or fraud, as funds can be transferred in and out of their account, much like a bank account. The ability to withdraw funds from a superannuation account provides an opportunity for serious and organised crime groups to access these funds if they can convince account holders to invest in a fraudulent scheme.

CASE STUDY: PAYPAL PHISHING

In early 2017, PayPal users were targeted by a phishing campaign directing victims to fake internet pages designed to look identical to legitimate websites in an effort to steal users' login credentials and other personal information.

HACKERS' USE OF PERSONALLY IDENTIFIABLE INFORMATION (PII) TO FRAUDULENTLY AUTHORISE FUNDS TRANSFERS



33 Access to superannuation benefits is generally restricted to members who have reached preservation age, which currently ranges from 55 to 60 years of age, depending on date of birth.

CARD FRAUD

Card fraud is the fraudulent acquisition and/or use of debit and credit cards, or card details, and may involve:

- fraudulent applications
- theft of cards/card details
- skimming of card details at automatic teller machines
- production of fake cards
- phishing/hacking to obtain card details.

In the 2015–16 financial year, Australians spent A$703 billion on cards; A$521 million of this spending (across 2,665,806 transactions) was fraudulent. This represents a card fraud rate of 74.2 cents per A$1,000 spent, an increase from the previous 12 months (60.4 cents per A$1,000).

The Australian Payments Network (APN) attributes 77 per cent of all fraud on Australian cards to card-not-present (CNP) fraud. CNP fraud occurs when card details are fraudulently used to make purchases or other payments without the card, via phone or online shopping, betting and/or gaming platforms or other websites of a similar nature.

The introduction of chip and PIN technology has resulted in a decline in card-present fraud; however, this kind of fraud also remains a problem. In response to these new technologies, organised crime groups have altered their methodologies—for example, by uploading skimmed data to blank cards to obtain cash or to purchase high-value goods in other countries. In the 2015–16 financial year, card counterfeit and skimming fraud perpetrated in Australia and overseas on Australian-issued cards accounted for almost A$47 million.

The intersection between smartphone technology and mobile payment platforms has enabled contactless payments using smart devices containing linked credit card details. The rise in mobile payment services follows the increasing use by Australians of smartphones to make online payments and purchases and to access banking services. Vulnerabilities exist within these payment platforms that can be exploited by serious and organised crime groups via the use of malware. As Australia moves towards a cashless society, there are increased opportunities for online payment and card fraud.