FINANCIAL CRIME MARKETS

CYBERCRIME

INTRODUCTION

Cybercrime is a crime committed directly or indirectly against a computer, system or network. Cybercrime actors are usually skilled individuals or groups who are engaged in the planning and execution of cyber intrusions. Cybercrime actors need not be physically co-located with others in their group, and are also often located overseas from their victims. Cybercrime methodologies and tools, including malware, are widely discussed and traded online.

Cybercrime is predominantly a financially-motivated crime that relies on the use of computers and communications technologies. The government's 2016 Cyber Security Review found cybercrime is costing the Australian economy up to $1 billion in direct costs alone. Cybercrime against financial platforms and financial institutions is increasing, as is the sale of products and services that facilitate cybercrime. Cybercrime can be difficult to disrupt due to its highly technical nature, and due to cybercrime actors using a variety of anonymising techniques.

CURRENT SITUATION

The global cybercrime market is a low risk, high return criminal enterprise. Cybercrime-related goods and services are highly sought after and are traded through online marketplaces and forums. Cybercrime actors targeting Australia for profit are predominantly based offshore. They are adaptable, resilient and sophisticated, and obscure their identities.

A number of different types of financially-motivated cybercrimes continue to pose a risk to the Australian public, the government, and businesses. These include credential-harvesting malware, ransomware, distributed denial of service extortion and Business Email Compromise.[18]

CYBERCRIME KEY OBSERVATIONS

- Most entities involved in cybercrime target Australian victims and financial platforms from an overseas location.
- Cybercrime that seeks to generate significant profit continues to increase in both frequency and sophistication.

CREDENTIAL HARVESTING MALWARE

Credential harvesting malware obtains legitimate account and/or login information, usually online banking login details. The malware is frequently delivered to a victim's computer through phishing emails containing malicious attachments. It can also be delivered through exploit kits hosted on malicious or compromised websites. When the malware is installed on a victim's device, it monitors and collects information, including bank account numbers and passwords, when the victim accesses an online banking platform. This information can then be used to make fraudulent payments or transfer money out of the victim's account.

Credential harvesting malware is designed to operate covertly, so it can remain undetected until the victim notices their money is missing. Credential harvesting malware can also be used to obtain logins and passwords to other systems, such as email, which can be used to send out spam and phishing emails.

18 Australian Cyber Security Centre 2016, *2016 Threat Report*, ACSC, Canberra, viewed 3 May 2017, <https://_www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf>.

CASE STUDY

THIEVES USE MALWARE ON MOBILE PHONES TO STEAL BANK LOGIN DETAILS

In 2016, a credential harvesting malware strain was identified that targeted Australian mobile banking users. The malware displayed a false bank login page, when the victim attempted to access their mobile banking platform. This login page could not be bypassed and allowed cybercrime actors to obtain the victim's login details.

The cybercrime actors were then able to use the stolen credentials to log into a victim's account and transfer money out. The malware was also capable of stealing Google login information.[i]

i Tucker, H 2016, *Thieves have made a huge malware play to steal Australian bank login details on Android phones,* Business Insider Australia, Sydney, viewed 3 May 2017, <https://_www.businessinsider.com.au/thieves-have-made-a-huge-malware-play-to-steal-australian-bank-login-details-on-android-phones-2016-3>.

THE 2016 CYBER SECURITY REVIEW FOUND CYBERCRIME IS COSTING THE AUSTRALIAN ECONOMY UP TO $1 BILLION

RANSOMWARE

Ransomware is a form of malware that stops a victim from using their computer or files until a sum of money is paid. Ransomware can either encrypt a person's files or lock a device, blocking access entirely. Ransomware usually targets a victim's computer via phishing emails or through malicious or compromised websites. In the 2016–17 financial year, ACORN received approximately 2,500 reports of ransomware targeting.

Successful ransomware campaigns in Australia use branding of trusted and well-known corporations as part of their social engineering techniques, as identified in the Australian Federal Police email case study.

DENIAL OF SERVICE EXTORTION

A denial of service (DoS) is an attempt by a cybercrime actor to disrupt an individual or business by preventing legitimate access to online services (typically a website). This is achieved by flooding the targeted machine with requests, consuming the available bandwidth or the processing capacity of the computer hosting the online service.[19] When multiple sources are used to flood an online service, usually coordinated through a botnet,[20] it is referred to as distributed denial of service (DDoS). Cybercrime actors can threaten an individual or company with a DoS or DDoS, unless a fee is paid. The actors may first conduct a short DoS/DDoS to demonstrate they have the capability to perform the attack, and to show the disruption it could cause.

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is a criminal scheme targeting large and small businesses for financial gain. BEC traditionally involves 'spoofing' an identity, usually a high-level executive, in order to elicit payment. BEC is increasingly sophisticated, with attempts seemingly preceded by substantial research and preparation. BEC incidents are not always cybercrime and can be described as cyber-enabled crime.

Since the inception of ACORN in 2014, more than 2,000 reports of BEC have been registered with ACORN. BEC continues to have a substantial financial effect on Australia and internationally.

19 A DoS can also occur unintentionally through mis-configuration, or through a sudden and unexpected surge in legitimate usage.

20 A botnet is a number of internet-connected devices used by an owner to perform various tasks. The term most commonly has a malicious connotation.

OUTLOOK

Australia's relative wealth and high uptake of social media and online services make it an attractive target for serious and organised crime groups and criminal individuals who use technology to facilitate their crime. Further, the increased use of technology in the financial sector both provides customers with convenient access to a range of services and presents increasing opportunities for technology-enabled fraud and cybercrime.

INVESTMENT AND FINANCIAL MARKET FRAUD

INTRODUCTION

Investment and financial market[21] fraud typically refers to the following types of criminal activities:

- fraudulent investment schemes, such as boiler-room fraud and Ponzi schemes, which attract victims with fake guarantees of high financial returns
- manipulation of the legitimate share market to artificially raise or lower the price of shares for financial benefit
- exploitation of financial securities,[22] such as fraudulent share schemes and off-market share transfers, and the use of margin lending facilities to make significant profit or launder the proceeds of crime.

INVESTMENT AND FINANCIAL MARKET FRAUD KEY OBSERVATIONS

- Serious and organised crime groups rely on technology, identity crime and the use of professional facilitators to commit investment and financial market fraud.

21 The major markets in the Australian financial system are the credit market, stock market, money market, bond market and the foreign exchange market. Australian Bureau of Statistics, *Financial system*, viewed 4 May 2017, <http://_www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/1301.0~2012~Main%20Features~Financial%20markets~267>.

22 Financial securities on offer in Australia include shares, bonds, derivatives and managed funds.

CASE STUDY

RANSOMWARE IMITATING AUSTRALIAN FEDERAL POLICE EMAILS

A successful ransomware campaign seen in Australia involved emails imitating a traffic infringement from the Australian Federal Police. The potential victim receives an email stating that they have received an infringement that requires a fine to be paid. The email contains an attachment purporting to be photographic evidence of the offence being committed. If downloaded, ransomware is installed on the victim's computer, files are encrypted and payment is demanded for decryption.

IN 2016–17, ACORN RECEIVED APPROXIMATELY 2,500 REPORTS OF RANSOMWARE TARGETING

CURRENT SITUATION

Australia is an attractive target for domestic and overseas-based serious and organised crime groups involved in investment and financial market fraud because of its comparatively stable economy, Australian investors' high subscription to share purchases, the perceived lower risk of detection and substantial illicit profits to be made.

The most recent reporting by the Australian Bureau of Statistics shows that approximately 1.6 million Australians experience personal fraud each year, at a combined personal cost of $3 billion.[23]

In 2016, the Australian Competition and Consumer Commission experienced a 47 per cent increase in the number of scam reports from the previous year, and investment schemes accounted for the second highest amount of reported losses at $23.6 million.[24] In 2016, ASIC received 367 reports about scams; however, the actual number of people affected by scams is likely to be much higher, as people often do not report that they have been scammed. The top five scams reported to ASIC are:

- overseas cold calling about investment opportunities
- overseas calls offering easy credit or loans after payment of an upfront fee
- sports arbitrage or gambling schemes
- money transfer schemes (job opportunity or other fraud)
- fake debt and invoice scams.

FRAUDULENT INVESTMENT SCHEMES

Transnational and Australia-based organised crime groups and entities commit investment and financial market fraud against Australia through deceptive activities including boiler-room fraud and Ponzi schemes. In these fraudulent investment schemes, victims are pressured into investing funds with promises of high financial returns in a short period of time. However, victims end up losing most or all of their invested funds.

Boiler-room fraud or cold-calling investment fraud involves the unsolicited contacting of potential investors, who are deliberately given false or misleading information to entice them to buy, sell or retain securities or other investments.

A Ponzi scheme is an investment fraud where, unknown to the investors, there is no legitimate investment and returns are simply paid to investors out of money from subsequent investors.

This provides an appearance of legitimacy and gives investors the incentive to invest more of their own money and to encourage others to invest in the scheme. The scheme generally fails when either the criminal entities flee with all of the proceeds, insufficient new investors can be found, or the scheme is discovered by authorities.

These investment frauds can be delivered to a significant number of victims in any country over the phone or internet from any region in the world, using technology that can hide both the identity and the location of the perpetrators.

The groups that operate boiler-room fraud and Ponzi schemes use various tactics to make their schemes seem legitimate including aggressive telemarketing campaigns, glossy brochures, professional-looking websites—sometimes stealing the identity of legitimate companies[25]—and fake investment reviews. To maximise the success of these scams, professional facilitators are used to provide investment advice for use in cold-calling scripts, to provide fraudulent identification to open bank accounts, create companies, and set up internet accounts and professional-looking websites.

A range of different fraudulent investments are offered by scammers, including sports betting and gambling systems, securities schemes, superannuation schemes and foreign exchange trading.

In some cases, criminal entities set up online accounts for investors so they can see their balances rise, giving them the incentive to invest more money. However, investors soon realise they have been scammed when their requests to withdraw money are ignored and contact is cut off.

23 Australian Bureau of Statistics 2016, *Personal Fraud*, viewed 4 May 2017, <http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0>.

24 Australian Competition and Consumer Commission 2017, *Targeting Scams*, viewed 18 July 2017, <https://_www.accc.gov.au/system/files/1162%20Targeting%20Scams%202017_FA1.pdf>.

25 Government of Western Australia Department of Commerce Consumer Protection 2016, *2016 Scams Review: Losses and victimisation rates during 2016 for consumer fraud in Western Australia*, DCCP, Perth, viewed 9 May 2017, <http://_www.scamnet.wa.gov.au/scamnet/d/Resource_Library/CRE3OUHQKFLP9RA4BGM995X7BMJBYP/RJOJCTQY9WAQTZG.pdf/scamsreview2016.pdf>.

CASE STUDY

INDIAN PENNY STOCK SCAM ON AN AUSTRALIAN STOCK EXCHANGE

In early 2017, ASIC detected the probable operation of a version of the Indian Penny Stock Scam on an Australian stock exchange.[i] The offshore service provider (OSP) running the fraudulent scheme listed offshore companies on an Australian exchange using initial shareholders who were all foreign citizens.

The share prices were often driven up by a single Australia-based broker executing very low volume trades. At the same time, these companies experienced an uncharacteristically significant amount of off-market transfers.

It is probable that the OSP was using the Australian exchange to create a reference price for their offshore company in Australia, from which off-market transfers were used as a vehicle to launder money and evade tax in foreign jurisdictions.

i The Penny Stock Scam in India involved large-scale money laundering and tax evasion through ramping up shares of small firms.

TO AVOID BEING A VICTIM OF INVESTMENT FRAUD, INVESTORS SHOULD USE AUSTRALIAN STOCKBROKERS AND LICENSED FINANCIAL SERVICE PROVIDERS

To reduce becoming a victim of investment fraud and increase the likelihood that investments are handled securely, investors should go through Australian stockbrokers and financial services providers licensed by ASIC. For investors wanting to deal with an overseas-based company that is not registered in Australia, it is recommended that investors visit the website of the International Organization of Securities Commission and check with the relevant authority where the overseas business is located, to confirm that they are appropriately registered to provide the services required.

SHARE MARKET MANIPULATION

Criminal entities can manipulate or exploit the legitimate share market for significant financial gain. One way of doing this is through share market manipulation scams such as 'pump and dump' schemes, which involve the use of false and misleading information to generate investor trading interest to artificially 'pump' up the price of a company's shares—normally a fraudulent or low value company. As more people invest, the share price increases and the scammers then sell or 'dump' shares at the peak of the price rise, giving them a considerable profit while causing the value of the shares to fall, leaving investors with shares that are either worthless or valued at a fraction of the purchase price.

EXPLOITATION OF FINANCIAL SECURITIES

Criminal entities exploit financial securities to make illegal profits, such as through fraudulent share schemes (via boiler-room fraud), or to launder the proceeds of crime. For example, legitimate share markets can be exploited to launder illicit funds, as they provide investors levels of anonymity, particularly when trading through professional brokers.

Illicit funds can also be laundered through activities such as off-market share transfers, which involve the transfer of shares between parties without using a stockbroker. This practice can be exploited to launder illicit funds by using fraudulent identities to conduct off-market transfers of shares into false names.

ASIC has seen an increase in organised crime networks seeking to exploit offshore entities on the Australian share market, particularly in cases where no capital is raised in Australia and the majority of investors are offshore. These entities regularly have poor liquidity,[26] which organised crime networks exploit to transfer value or generate illicit profits.

OUTLOOK

Investment and financial market fraud can distort Australia's markets by diverting legitimate capital to non-productive or illicit investments. Such activity may reduce investor confidence in the integrity of these markets, with a consequent reduction in willingness to invest in legitimate entities. At the social level, such fraud causes financial hardship, reliance on welfare, mental illness or, in extreme cases, self-harm or suicide.

Australia will continue to be a target for domestic and offshore investment fraud activities. Law enforcement agencies, financial regulators and other bodies work independently and collaboratively across Australia to prevent and detect investment and market fraud in Australia.

REVENUE AND TAXATION FRAUD

INTRODUCTION

Revenue and taxation fraud involves the intentional abuse of the taxation system with the aim of obtaining financial benefit. It includes a number of noncompliant activities resulting in criminal penalties such as fines or imprisonment. These activities range from failing to report income in order to avoid taxation obligations to the use of complex offshore secrecy arrangements to evade tax.[27] Revenue and taxation fraud in Australia is made possible through the use of technology, identity crime and professional facilitators.

CURRENT SITUATION

Organised crime groups, significant criminal individuals and some high-wealth individuals have been identified as committing revenue and tax fraud in Australia.

26 Liquidity describes how easy it is to convert assets to cash.

27 Australian Taxation Office 2015, *Tax crime explained*, viewed 6 April 2017, <https://_www.ato.gov.au/General/The-fight-against-tax-crime/Tax-crime-explained/>.

REVENUE AND TAXATION FRAUD KEY OBSERVATIONS

- Revenue and taxation fraud is committed by Australia-based crime groups but there are indications of offshore control of some syndicates committing refund fraud, offshore tax evasion and abusive use of trusts.
- Organised crime and other significant criminal individuals rely on technology, identity crime and professional facilitators to commit revenue and tax fraud.
- Revenue and taxation fraud has been committed through deceptive activities including illegal phoenix activity, abusive use of trusts, and the use of complex offshore secrecy arrangements.

While organised crime groups that commit revenue and tax fraud are primarily based in Australia, some syndicates who commit refund fraud, offshore tax evasion and abusive use of trusts are controlled by overseas-based entities.

TAX REFUND FRAUD

Tax refund fraud occurs when people claim refunds, rebates or offsets that they are not entitled to. This can happen in a number of ways, from claiming fictitious expenses to creating false documentation to support a claim. Tax refund fraud is also committed when people dishonestly understate their income or provide false payment summary details, and when fraudulent tax returns are lodged using false or stolen identities. Identity crime related to refund fraud is an increasing problem.[28]

OFFSHORE TAX EVASION

Globalisation and technological advances have made it easier for individuals to hold investments in offshore financial institutions, increasing the opportunity for tax evasion.[29] A high level of financial sector knowledge is required to successfully establish and operate large-scale fraud and tax evasion activities—this requires those committing the fraud to employ a professional to facilitate their activities. Facilitators include professionals in the accounting and law, money remittance, finance and insurance, import/export, and information and communications technology industries.

Project Wickenby, which targeted offshore tax evasion schemes, increased tax collections through improved compliance behaviour and enhanced the ability of Australian authorities to exchange information with other jurisdictions. The offshore tax evasion investigative work of Project Wickenby continues under the multi-agency Serious Financial Crime Taskforce.[30]

ILLEGAL PHOENIX ACTIVITIES

Organised crime groups and other criminal individuals evade tax through illegal phoenix activities. Illegal phoenix activity occurs when ‘a new company is created to continue the business of a company that has been deliberately liquidated to avoid paying its debts, including taxes, creditors and employee entitlements’.[31]

ABUSIVE USE OF TRUSTS

The abusive use of trusts contributes to revenue and tax fraud in Australia, with trust structures permitting individuals to anonymously control significant wealth. Serious and organised crime groups and significant criminal individuals have exploited trusts to avoid or evade tax by concealing income, artificially reducing income and mischaracterising financial transactions.

28 Australian Taxation Office 2015, *Refund fraud*, viewed 6 April 2017, <https://_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Refund-fraud/>.

29 Australian Taxation Office 2015, *International tax crime*, viewed 6 April 2017, <https://_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/International-tax-crime/>.

30 Australian Taxation Office 2015, *Project Wickenby task force*, viewed 6 April 2017, <https://_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Project-Wickenby-task-force/>.

31 Australian Taxation Office, *Illegal phoenix activity*, viewed 6 April 2017, <https://_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Illegal-phoenix-activity/>.

CASE STUDY

IDENTITY THEFT ENABLING TAX REFUND FRAUD

Over a two month period in 2010, a Thai national deceived three registered tax agents to lodge 217 fraudulent income tax returns with the ATO using stolen identities. The Thai national provided the tax agents with forged documents—provided by an associate in the fraud—which the tax agents accepted as genuine documents. The ATO detected the fraud as the unsuspecting individuals named in the fraudulent tax returns were not employed as reported. In March 2017, the offender was sentenced in New South Wales to three years jail for fraudulently claiming $1.335 million in tax refunds.[i]

i Australian Taxation Office 2017, *Refund fraudster sentenced to three years jail*, viewed 19 April 2017, <https://_www.ato.gov.au/Media-centre/Media-releases/Refund-fraudster-sentenced-to-three-years--jail/>.

THE SERIOUS FINANCIAL CRIME TASKFORCE WILL CONTINUE TO TARGET, IDENTIFY AND CHARGE CRIMINALS WHO COMMIT REVENUE AND TAXATION FRAUD

EXPLOITATION OF TAX RULES IN RELATION TO VALUABLE METALS

Groups or networks of industry participants including refiners, bullion dealers, gold kiosks, dealers and buyers within established supply chains involved in gold recycling arrangements have been identified as seeking to exploit the goods and services tax (GST) rules in relation to valuable metals to fraudulently obtain GST refunds. As pure gold cannot be sold with the addition of GST, the fraud involves the seller melting or tarnishing the pure gold and selling the resultant scrap gold with the 10 per cent premium. Instead of remitting the GST to the ATO, the seller keeps the GST while the buyer claims a GST credit from the government. The buyer then recycles the scrap gold back into bullion, creating a 'carousel' in which GST payments are never sent to the ATO and GST credits are repeatedly claimed.[32]

To counteract this fraudulent activity, the Australian Government has introduced a new regulation that applies retrospectively from 1 April 2017. A 'reverse charge' of GST now applies to business-to-business taxable supplies of gold, silver and platinum, which places the onus on the buyer of the valuable metal, rather than the seller to remit the GST to the ATO.[33]

OUTLOOK

The loss of government revenue from revenue and tax fraud has a flow-on effect for the Australian community, resulting in less tax revenue being available to spend on government services such as infrastructure, utilities, health and education.

Revenue and taxation fraud will remain a long-term issue in Australia as interactions between technology, identity crime and professional facilitators become increasingly complex and frequent. To address this issue, the Serious Financial Crime Taskforce and the ATO will continue to target, identify and charge organised crime groups and criminal individuals who commit revenue and taxation fraud.

SUPERANNUATION FRAUD

INTRODUCTION

The superannuation industry in Australia primarily includes funds regulated by the Australian Prudential Regulation Authority (APRA), such as industry funds, corporate funds, retail funds and public sector funds, and self-managed superannuation funds (SMSFs), regulated by the ATO. As at June 2017, $1,444.1 billion in superannuation assets were held by APRA-regulated superannuation funds while $696.7 billion were held by SMSFs.[34]

CURRENT SITUATION

Australia's large pool of superannuation funds is an attractive target for criminal groups and individuals.[35] 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.[36]

SUPERANNUATION FRAUD KEY OBSERVATIONS

- Superannuation fraud in Australia is made possible through the use of technology, cybercrime and identity crime.
- Self-managed superannuation funds are particularly vulnerable to exploitation by serious and organised crime groups and entrepreneurial criminals.

32 Griffin, M 2017, 'Australia cracks down on gold industry tax fraud', *Sydney Morning Herald*, 2 April, [Online], accessed 18 April 2017, available at: <http://_www.smh.com.au/business/australia-cracks-down-on-gold-industry-tax-fraud-20170402-gvbvbq.html?deviceType=text>.

33 Australian Taxation Office, *Reverse charge in the valuable metals industry*, viewed 18 April 2017, <https://_www.ato.gov.au/Business/GST/In-detail/Rules-for-specific-transactions/Reverse-charge-in-the-valuable-metals-industry/>.

34 Australian Prudential Regulation Authority 2017, *Quarterly Superannuation Performance*, APRA, Sydney, viewed 12 September 2017, <http://_www.apra.gov.au/Super/Publications/Documents/2017QSP201706.pdf>.

35 Australian Transaction Reports and Analysis Centre 2016, *Australia's Superannuation Sector: Money laundering and terrorism financing risk assessment*, AUSTRAC, Canberra, viewed 28 April 2017, <http://_www.austrac.gov.au/sites/default/files/super-annuation-risk-assessment-WEB2.pdf>.

36 National Organised Crime Response Plan 2015–2018.

APRA-REGULATED SUPER FUNDS

APRA-regulated superannuation funds are susceptible to targeting by criminals, who are increasingly using technology, cybercrime and identity crime to commit superannuation fraud through activities such as hacking individuals' computers and using their personal identity information to fraudulently authorise the transfer of superannuation funds across to illegitimate SMSFs that are accessible to the criminal.

Early release scams are another form of superannuation fraud, where criminal entities offer super members access to their funds before the legal release age. Promoters of these illegal super scams often target people seeking debt relief, unemployed people and those from non-English-speaking backgrounds.

Victims' superannuation funds are rolled into a legitimate or illegitimate SMSF and are then stolen by the fraudster, or access to the funds is given to victims after a substantial fee is withdrawn for the criminal.[37]

Regulatory safeguards have been introduced to reduce the incidence of funds being illegally released from SMSFs. The ATO has improved the SMSF registration process to ensure only legitimate SMSFs are registered, and its new SMSF Member Verification System provides more certainty and transparency around rollovers from APRA-regulated super funds to SMSFs.

Penalties have also been introduced to prevent illegal early release of super funds. Promoters of illegal early release schemes face up to five years imprisonment, while those who access their superannuation benefits illegally will be taxed at the rate of 45 per cent on these amounts.

The accounts of members in APRA-regulated funds who have reached preservation age are particularly vulnerable to theft or fraud, as funds can be transferred in and out, like a bank account. The ability to withdraw funds from a superannuation account provides an opportunity for criminals to access these funds, if they can convince the account holder to invest in a fraudulent scheme.

APRA-regulated superannuation funds are responding to these vulnerabilities with the development of data analytic capabilities designed to detect unusual or suspicious activity. AUSTRAC also plays an important role in combating superannuation fraud by analysing reports received from industry pertaining to the use of fraudulent documentation in support of claims for early release of superannuation benefits, or death and disability insurance payments. AUSTRAC is sharing this intelligence with partner agencies for further investigation.

SELF-MANAGED SUPERANNUATION FUNDS

Like APRA-regulated super funds, SMSFs also experience theft of contributions and fund assets. The growing balance of funds in SMSF accounts and the desire by individuals to choose and control their own investments make them particularly vulnerable to incidents of fraud.[38] For these reasons, individual SMSF account holders are especially vulnerable to becoming victims of superannuation fraud by organised crime groups and individuals through fraudulent fund investments, non-existent schemes and being charged excessive fees by SMSF advisers. Unlike APRA-regulated super funds, if an SMSF member loses money due to theft or fraud, they do not have access to any compensation schemes.[39]

Superannuation fraud is also committed when an SMSF contravenes the 'sole purpose test'. To meet the sole purpose test and be eligible for the tax concessions normally available to super funds, a trustee of an SMSF must ensure that the SMSF is maintained for the sole purpose of providing retirement benefits to its members, or to dependants if a member dies before retirement.

An SMSF fails the sole purpose test if the trustee provides a pre-retirement benefit to its members or anyone else, directly or indirectly—such as personal use of a fund asset.[40]

37 Australian Securities and Investments Commission, *Superannuation scams*, viewed 27 April 2017, <https://_www.moneysmart.gov.au/scams/superannuation-scams>.

38 Drury, B 2015, 'Cyber gangs are targeting your super', *Sydney Morning Herald*, [Online], accessed 24 April 2017, available at: <http://_www.smh.com.au/money/super-and-funds/cyber-gangs-are-targeting-your-super-20150218-13igpg>.

39 Australian Securities and Investments Commission 2017, *Self-managed super fund (SMSF)*, viewed 27 April 2017, <https://_www.moneysmart.gov.au/superannuation-and-retirement/self-managed-super-fund-smsf>.

40 Australian Taxation Office 2017, *Sole purpose test*, viewed 17 July 2017, <https://_www.ato.gov.au/super/self-managed-super-funds/investing/sole-purpose-test/>.

Contravening the sole purpose test is a tax crime that the ATO is carefully monitoring. In addition to an SMSF losing its tax concessions, trustees could face civil and criminal penalties.

OUTLOOK

Losses to individual superannuation funds through fraudulent activities have the potential to increase financial hardship, causing a greater reliance on welfare payments and a loss of trust in the superannuation system.

The Australian Government introduced 'Stronger Super' reforms in 2012–13, which included measures to strengthen the governance, integrity and regulation of the Australian superannuation industry, particularly SMSFs. The reforms included giving the ATO powers to address wrongdoing and noncompliance by SMSF trustees, establishing a register of SMSF auditors (administered by the Australian Securities and Investments Commission), and making specialist knowledge and competencies mandatory for SMSF auditors and financial advisers providing services to SMSFs.[41]

CARD FRAUD

INTRODUCTION

Card fraud is the fraudulent acquisition and/or use of debit and credit cards or the card details. Card fraud may involve fraudulent applications, the theft of cards or card details, skimming of card details at automatic teller machines (ATMs), production of counterfeit cards, and phishing and hacking to obtain card details.

CURRENT SITUATION

According to the Australian Payments Network, card-not-present fraud[42] continues to be the most prevalent type of fraud on Australian cards. Seventy-seven per cent of fraud on all Australian cards, perpetrated either in Australia or overseas in the 2015–16 financial year, is attributed to card-not-present fraud.[43]

CARD FRAUD KEY OBSERVATIONS

- The global growth in technology in service delivery has presented expanding opportunities for organised crime, with card fraud being an increasing area of exploitation.
- The increase in online and cashless transactions suggests that the incidence of card-not-present fraud will also rise.
- Card fraud in Australia has frequently been undertaken by offshore crime groups that travel to Australia for the sole purpose of committing card fraud.

Over the five-year period from the 2010-11 financial year to the 2015–16 financial year, card-not-present fraud on all Australian cards increased from $164 million to $402 million respectively.[44] The rise in card-not-present fraud correlates with the increase in popularity of online shopping and the associated increase in the storage of these details online.

The intersection between smartphone technology and mobile payment platforms has enabled contactless payments using a smart device that contains linked credit card details. The rise in mobile payment services, which are intended to enhance customer convenience, follows the increasing use by Australians of smartphones to make online payments and purchases, and to access banking services.

41 The Treasury, *Stronger Super*, viewed 28 April 2017, <https://_strongersuper.treasury.gov.au/content/Content.aspx?doc=publications/government_response/key_points.htm#super_funds>.

42 Card-not-present fraud occurs when valid card details are used to make purchases over the phone or internet—without the need for the card to be presented during the transaction—and without the authority of the card owner.

43 Australian Payments Clearing Association 2016, *APCA releases interim payments fraud data*, media release, 16 December, APCA, Sydney, viewed 19 March 2017, <http://_www.apca.com.au/docs/default-source/2016-Media-Releases/apca-releases-interim-payments-fraud-data.pdf>.

44 Australian Payments Network Limited 2016, *Fraud Statistics 2016 Financial Year Sheet - Payment Fraud Statistics 1 July 2015-30 June 2016, Australian Payments Fraud Details and Data 2016*, APNL, Sydney, viewed 25 August 2017, <http://_www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2016r.pdf>; Australian Payments Clearing Association 2011, *Fraud Statistics 2011 Financial Year Sheet - Payment Fraud Statistics 1 July 2010-30 June 2011*, APCA, Sydney, viewed 25 August 2017, <http://_www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2011-(revised-december-2013).pdf?sfvrsn=16>.

CASE STUDY

CREDIT CARD DETAILS STOLEN AFTER HACK

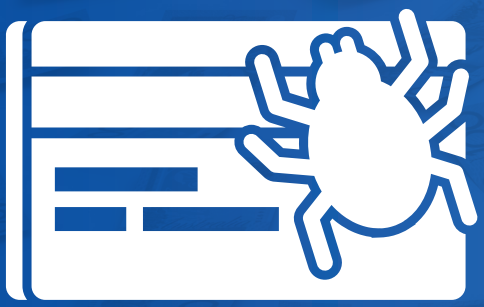
In March 2017, a school photography company warned users of their online payment system that their website had been breached and the details of credit cards compromised. Users of the photography company reported that their credit cards had been used to pay for ride sharing, accommodation and airfares in Europe and the United States, with one user claiming there were charges of $3,000 fraudulently attributed to their credit card.[i]

The website was reportedly compliant with Payment Card Industry Data Security Standards.[ii]

---

i Silva, K 2017, 'Hackers steal thousands after Queensland School Photography targeted online', Australian Broadcasting Corporation, Sydney, viewed 21 March 2017, <http://_www.abc.net.au/news/2017-03-14/fraudsters-target-queensland-school-photos-stealing-thousands/8350502>.

ii Branco, J 2017, *Credit card details stolen after school photographer's website hacked*, Brisbane Times, Brisbane, viewed 21 March 2017, <http://_www.brisbanetimes.com.au/queensland/credit-card-details-stolen-after-school-photographers-website-hacked-20170313-guxcwj.html>.



CARD-NOT-PRESENT FRAUD ACCOUNTS FOR 77% OF FRAUD ON ALL AUSTRALIAN CARDS

However, there are vulnerabilities in payment platforms that can be exploited by organised crime groups and tech-savvy criminals. Malware aimed at compromising smartphones may provide hackers with access to card details stored within mobile payment applications.[45] The 2015 ISACA Mobile Payment Security Study[46] identified the top four vulnerabilities of mobile payments as the use of public wi-fi, lost or stolen devices, phishing[47] or shmishing,[48] and weak passwords.

While card skimming continues to occur, counterfeit/skimming fraud on Australian cards in Australia saw a negligible increase from the 2014–15 financial year ($6.7 million) compared with the 2015–16 financial year ($7 million).[49]

However, counterfeit/card skimming fraud on Australian cards overseas has seen a significant rise from $17.1 million in the 2014–15 financial year to $39.8 million in the 2015–16 financial year.[50] The rise of these types of card fraud is explained by Australian cards being compromised by fraud overseas in locations where preventative measures, such as chip technology, have not been as widely introduced as they have been in Australia.

Fraud on lost or stolen cards occurring either in Australia or overseas also increased from $28.1 million in the 2014–15 financial year to $34.3 million in the 2015–16 financial year[51] but still accounts for a small percentage of the overall card fraud on Australian cards.

OUTLOOK

The harm experienced by individual victims of card fraud can range from inconvenience and reduced confidence in card security through to long-term effects on personal credit ratings, identity theft and compromising of privacy. While the impact of card fraud on the banking industry is felt through damage to reputation and disruption to services, any financial losses are most likely passed on to customers through increased fees and banking costs.

Australia is reported to be moving towards a cashless society that will be more reliant on mobile and contactless payment services.[52] Australia's use of cash will almost certainly decline in future, while debit and credit card transactions will continue to rise. Internationally, the movement towards a cashless society has seen an increase in online payment fraud and card fraud. It is likely that similar card fraud trends will be evidenced in Australia as contactless and mobile-based payment services are increasingly adopted.

45 Attorney-General's Department 2016, *Mazar malware attacking Android phones*, viewed 22 February 2016, <https://_www.staysmartonline.gov.au/alert-service/mazar-malware-attacking-android-phones>.

46 ISACA 2015, *2015 Mobile Payment Security Study Global Result*s, viewed 19 March 2017, <http://_www.isaca.org/SiteCollectionDocuments/2015-Mobile-Payment-Security-Study-Global-Data-Sheet_mis_Eng_0915.pdf>.

47 Phishing refers to identity theft tactics surrounding email and internet use.

48 Shmishing, also called smishing, refers to identity theft involving texts or short messages.

49 Australian Payments Clearing Association 2015, *Australian Payments Fraud; Details and Data 2015,* APCA, Sydney, viewed 19 March 2017, <http://_www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2015.pdf>; Australian Payments Clearing Association 2016, *Australian Payments Fraud; Details and Data 2016,* APCA, Sydney, viewed 19 March 2017, <http://_www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2016.pdf>.

50 Australian Payments Clearing Association 2016, *Fraud Statistics 2016 Financial Year Sheet - Payment Fraud Statistics 1 July 2015-30 June 2016*, APCA, Sydney, viewed 25 August 2017, <http://_www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2016r.pdf>; Australian Payments Clearing Association 2010, *Fraud Statistics 2010 Financial Year Sheet - Payment Fraud Statistics 1 July 2009-30 June 2010*, APCA, Sydney, viewed 25 August 2017, <http://_www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2010-(revised-december-2012).pdf?sfvrsn=8>.

51 Australian Payments Clearing Association 2016, *Fraud Statistics 2016 Financial Year Sheet - Payment Fraud Statistics 1 July 2015-30 June 2016*, APCA, Sydney, viewed 25 August 2017, <http://_www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2016r.pdf>; Australian Payments Clearing Association 2010, *Fraud Statistics 2010 Financial Year Sheet - Payment Fraud Statistics 1 July 2009-30 June 2010*, APCA, Sydney, viewed 25 August 2017, <http://_www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2010-(revised-december-2012).pdf?sfvrsn=8>.

52 Hunter, F 2016, 'Cashless future will save billions and requires red tape abolition: Alex Hawke', *The Canberra Times*, [Online], 17 February, accessed 14 June 2017, available at: <http://_www.canberratimes.com.au/federal-politics/political-news/cashless-future-will-save-billions-and-requires-red-tape-abolition-alex-hawke-20160216-gmv8ka.html>.

CASE STUDY

BULGARIAN NATIONALS COMMIT CARD FRAUD IN AUSTRALIA

In March 2017, a Bulgarian national pleaded guilty to providing false documents and committing fraud as a result of participating in a card skimming ATM fraud with a fellow Bulgarian national. The two perpetrators attached skimming devices to the ATM, which recorded encrypted information about people's accounts, including their personal identification numbers. The information was then used to create new cards, which were used to make unauthorised cash withdrawals from the accounts. The individual entered Australia to commit the card fraud, departed and returned to commit further offences. The offender was sentenced to 3½ years prison and will be deported to Bulgaria at the completion of the sentence.[i]

i 'ATM fraudster to be jailed, then deported', *the Age*, [Online], 9 March 2017, accessed 19 March 2017, available at: <http://_www.theage.com.au/victoria/atm-fraudster-to-be-jailed-then-deported-20170309-guubv1.html>; Cooper, A 2016, 'Bulgarians skimmed more than $380,000 from Melbourne ATMs, court hears', *The Age,* [Online], 3 March, accessed 19 March 2017, available at: <http://_www.theage.com.au/victoria/bulgarians-skimmed-more-than-375000-from-melbourne-atms-court-hears-20160303-gn9kz1.html>.

CARD SKIMMING FRAUD ON AUSTRALIAN CARDS OVERSEAS ROSE FROM $17.1M IN 2014–15 TO $39.8M IN 2015–16

HEALTH AND WELFARE FRAUD

INTRODUCTION

Criminal groups and individuals are committing health and welfare fraud by exploiting vulnerabilities in government benefit and rebate frameworks, such as those that support family day care services. Sophisticated exploitation of health and welfare systems demonstrates a wide variety of criminal methodologies including collusion, the compromise of online systems and identity fraud.

Government revenue loss through fraudulent claims on health and welfare payments has the significant effect of reducing funds available for government services and programs, including legitimate health and welfare claims.

CURRENT SITUATION

Entities and groups that are targeting government welfare, health and child support systems to commit fraud are predominantly opportunistic in nature. Many of the groups identified as perpetrating fraud are centred in communities that are geographically or culturally connected, or are businesses (such as medical practitioners or child care operators), rather than serious and organised crime groups.

That is not to say, however, that the welfare fraud being committed in Australia is not sophisticated, or that it does not target vulnerabilities in welfare programs in a systematic way. The Department of Human Services has identified an increasing number of cases in which the same individuals are committing fraud across a number of programs or using deceptive practices that demonstrate a level of sophistication.

Investigations or compliance activities into fraudulent claims for or overpayment of associated Commonwealth benefits may discover information relating to other types of health and welfare fraud. Individuals involved in one type of health and welfare fraud often seek to exploit vulnerabilities in other Commonwealth benefits schemes. For example, educators and parents involved in family day care fraud often receive other Commonwealth benefits, including Newstart and youth allowances, and single parent and disability support pensions. While there may be legitimate claims to a number of Commonwealth benefit schemes, the involvement in one type of health and welfare fraud increases the likelihood of being involved in other types of Commonwealth benefit fraud.

HEALTH AND WELFARE FRAUD KEY OBSERVATIONS

- Health and welfare fraud is predominantly an opportunistic crime carried out by people with both access to and knowledge of health and welfare services and systems.
- Serious organised crime groups have not traditionally been involved in this type of financial crime.
- Health and welfare fraud is anticipated to grow in line with the increased migration of government services to online platforms.

Taskforce Integrity, a joint operation between the Department of Human Services and the AFP, targets geographic locations with a higher risk of welfare fraud and noncompliance. The task force aims to change localised cultures of noncompliance and positively influence customer behaviour by encouraging self-correction. The activities of Taskforce Integrity range from individual compliance reviews through to investigations of organised and complex fraud.

A factor compounding the prevalence and scale of this type of fraud is that the child care benefit and child care rebate programs are provided by Australian Government departments, while compliance with the conditions of the programs are administered by the state and territory departments of education.

While the majority of health, welfare and child support frauds against Australian welfare systems have been undertaken domestically, it is anticipated that the targeting of online government portals will increase and that these systems may possibly be breached by offshore entities.

OUTLOOK

Health and welfare fraud has a genuine negative impact on government revenue, reducing the funds available to allocate to government services and programs. The theft of medical records, tax information or personal identifying information, with a view to use in defrauding the government of welfare, health and/or child support payments, also has a personal impact on the victims of this identity theft.

CASE STUDY

EXPLOITATION OF SCHEME FOR VULNERABLE CHILDREN IN CHILD CARE FRAUD

Between September 2013 and March 2015, a child care centre was identified as charging families with children in care approximately $9,000 per week, including 14 at-risk children, in order to exploit the government rebate for the Special Child Care Benefit. No invoice was given to the parents as the child care provider received 100 per cent of the claimed benefit.

This scam defrauded the government of $3.6 million—one of the largest child care frauds in Australia. The charges laid against the child care operator included 66 counts of dishonestly obtaining financial advantage by deception, 15 counts of using forged documents and one count of dealing with money and property believed to be proceeds of crime worth more than $1 million.

The child care provider was sentenced to seven years in prison.[i]

---

i Balogh, S & Morton, R 2017, 'Seven years' jail after taxpayers footed bill for $3.6m childcare rort', *The Australian*, [Online], 27 May, accessed 16 June 2017, available at: <http://_www.theaustralian.com.au/news/nation/seven-years-jail-after-taxpayers-footed-bill-for-36m-childcare-rort/newsstory/2703cec51163ddcc045fa6a1a3e4e5d2?nk=17472f53799716159c71d6ee21428a07-1496197212>.

THOSE INVOLVED IN HEALTH AND WELFARE FRAUD OFTEN SEEK TO EXPLOIT VULNERABILITIES IN MULTIPLE COMMONWEALTH BENEFITS SCHEMES