

# FINANCIAL CRIME ENABLERS

## MONEY LAUNDERING

### INTRODUCTION

Australia continues to sustain very profitable crime markets, such as the illicit drug market, and as a result there is a need to launder the significant proceeds that these crimes generate.

Methodologies used to launder the proceeds of drug crime, for example, are likely to differ from the methodologies used to launder the profits of financial crime. The former requires larger amounts of illegal cash to be placed into banking or alternative remittance systems before it can be laundered, while financial crime proceeds are more likely to already be in the legitimate banking systems. It is likely that the majority of the profit from financial crime is laundered by transferring funds through a series of bank accounts in different jurisdictions. Corporate structures within Australia and overseas are also used to facilitate this process.

Regardless of the source of the proceeds of crime, in order to use the illegal funds to facilitate further criminal activity or to support a lavish lifestyle, it is necessary to launder them and to obscure their criminal origins.

### CURRENT SITUATION

Money laundering remains a fundamental enabler of financial crime and is a significant and potentially lucrative criminal enterprise in itself. As well, our stable financial markets and valuable real estate market make Australia an attractive destination for criminal groups and individuals looking to invest or launder the proceeds of crime.

Money laundering occurs on a global scale with proceeds of crime transferred between jurisdictions, commingled with legitimate monies and integrated into legitimate markets. Australian law enforcement has continued to gain significant insights into the operations of transnational money laundering organisations, the methodologies used by such groups and their connections to other serious and organised crime groups.



### MONEY LAUNDERING KEY OBSERVATIONS

- Money laundering remains a fundamental enabler of financial crime and is a significant and potentially lucrative criminal enterprise in itself.
- Some organised crime groups are using more global methods to launder proceeds of crime, including using the services of transnational money laundering organisations, money mules, remittance services and trade-based money laundering.

### ALTERNATIVE REMITTANCE SERVICES

It is almost certain that groups and individuals involved in financial crime are engaging transnational money laundering organisations to launder illicit profits through alternative remittance services both in Australia and overseas.

Alternative remittance services use money transfer methodologies such as informal value transfer systems to remit a value amount without the physical transfer of cash, whether this is legitimate cash or proceeds of crime.

### SMART AUTOMATIC TELLER MACHINES

Smart automatic teller machines capable of accepting cash deposits have the potential vulnerability of allowing people to make illicit cash deposits into third-party accounts. This practice, although not entirely anonymous, has been seen as an opportunity to move cash into accounts while avoiding face-to-face interactions with bank staff members, who could identify suspicious transactions and report them.

## STORED VALUE CARDS

Above threshold stored value cards (SVCs)<sup>2</sup> have been identified as being used to move large sums of money derived from the proceeds of crime through established financial networks, often offshore.

While above threshold SVCs are subject to anti-money laundering/counter-terrorism financing reporting, below threshold SVCs<sup>3</sup> have also been identified as being used to launder money, despite holding less monetary value. Below threshold SVCs are an attractive option, though, as they offer complete anonymity and do not attract reporting obligations. The limitation of storage value is often circumvented by purchasing multiple cards.<sup>4</sup>

## TRADE-BASED MONEY LAUNDERING

Trade-based money laundering (TBML) is defined as ‘the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origin or finance their activities’.<sup>5</sup>

There are a number of TBML techniques, including over- or under-invoicing, over- or under-shipment, false invoicing, and black market peso exchange. These techniques can be effectively applied either in isolation or in combination, exploiting the complex nature of trade and trade finance to conceal the movement of illicit value.

- 2 An SVC is regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and carries reporting obligations if the card can hold \$1,000 or more at any one time and cash can be withdrawn from the card, or if the card can hold \$5,000 or more at any one time and cash cannot be withdrawn from the card.
- 3 An SVC that does not meet the relevant thresholds, as set out for above threshold SVCs, is not regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
- 4 Australian Transaction Reports and Analysis Centre 2017, *Stored Value Cards Money Laundering and Terrorism Financing Risk Assessment*, viewed 12 April 2017, <[http://\\_www.austrac.gov.au/sites/default/files/stored-value-cards-risk-assessment-WEB.pdf](http://_www.austrac.gov.au/sites/default/files/stored-value-cards-risk-assessment-WEB.pdf)>.
- 5 In 2008, the Financial Action Task Force’s Paper on Best Practices broadened the definition of TBML to incorporate the use of TBML methodologies for terrorist financing. Financial Action Taskforce 2008, *Best Practices Paper on Trade Based Money Laundering*, FATF/OECD, France, viewed 12 April 2016, <[http://\\_www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf](http://_www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf)>.

## ONLINE WAGERING PLATFORMS

Serious and organised crime entities may have both access to and control of offshore wagering platforms. Betting activity through offshore platforms also conceals betting activity on corrupted sports and racing events, and the potential laundering of criminal wealth.

## USE OF COMPLEX OFFSHORE BUSINESS STRUCTURES

Money laundering methodologies can, and frequently are, combined with the use of offshore corporate entities to further obscure the criminal origin of such funds. The recent exposure of Mossack Fonseca client information provides insight into the ease with which offshore companies and associated bank accounts can be created in multiple jurisdictions and used to electronically transfer illicit funds around the world.

## PROFESSIONAL FACILITATORS

In order to set up the structures needed to launder the profits of financial crime, serious and organised crime groups and criminal individuals almost certainly use a range of professional facilitators, both within Australia and offshore. Members of serious and organised crime groups involved in financial crime are likely to have a degree of financial literacy and knowledge of the types of structures required to conceal their involvement in such criminal activity. However, the creation and maintenance of these structures almost certainly requires the use of professional facilitators.

## OUTLOOK

The electronic transfer of funds to multiple accounts in different jurisdictions is likely to remain the dominant method used to launder the proceeds of financial crime. However, transnational money laundering organisations, money mules and remittance services have been identified as being used by serious and organised crime groups involved in financial crime. These trends are likely to continue but will change, and methodologies will be displaced as continued success in law enforcement targeting of particular methodologies occurs.



The ability of those involved in serious and organised crime to launder money allows for re-investment, and therefore the perpetuation of criminal enterprises. Money laundering activities also have the potential to undermine the stability of financial institutions and systems, discourage foreign investment, distort international capital flows and damage diplomatic relations.

Further harm may be caused by the methods with which money laundering occurs. The primary goal of money laundering is to give illicitly-derived money the appearance of legitimacy. Consequently, funds are likely to be invested not on the basis of likely returns, but in businesses or schemes that provide the greatest chance of concealing the origins of the money. This can erode the 'level playing field' on which legitimate businesses compete, distort markets, and enhance the economic power of organised crime.

## TECHNOLOGY

### INTRODUCTION

Technology has enabled organised crime and has provided criminals engaging in financial crime with ready access to a significantly larger number of potential victims, personal identifying information and victim funds. Organised crime groups frequently seek out individuals skilled in the use of technology to enable them to target victims of financial fraud including card fraud, investment fraud and superannuation fraud.

The use of technology in facilitating financial crime is particularly attractive as it enables criminal groups and individuals to identify and target significantly larger groups of potential victims from any location in the world, while expending few resources. Similarly, the use of technology in financial crime can obscure the identity and location of criminal groups and individuals, which makes it a low risk activity with a potential for high return.

### CURRENT SITUATION

The use of technology to enable financial crime has grown steadily over the past 10 years in line with advancements in the accessibility and variety of available technology and financial platforms. As the rapid uptake of technology and the online environment grows, criminal groups and individuals exploit this as means to commit, facilitate or conceal criminality.

## TECHNOLOGY KEY OBSERVATIONS

- The use of technology to enable financial crime has increased significantly over the past two years, with the most serious financial crime now enabled by technology. It is almost certain that this increase will continue over the next two years.
- Those who possess specialist information and communications technology skills are almost certain to play an increasingly important role in supporting the activities of groups and individuals who intend to commit serious financial crimes.

The anonymity offered by virtual currencies and associated software applications is likely to be highly attractive to criminals. Bitcoin offers a level of anonymity for users that can be increased when it is used in combination with anonymising software. There are also a range of other virtual currencies, such as ZCash and Monero, which offer anonymity far exceeding that of Bitcoin.

The increased use of technology in the financial services sector provides clients with user-friendly access to a range of products. However, this also exposes an increasing number of individuals and businesses to a range of technology-enabled financial crimes. For example, online interfaces can be copied by organised crime groups and individual fraudsters, and receive redirected traffic so victims believe they are visiting a legitimate website. This creates the opportunity to target a large number of potential victims around the world.

As technology-enabled financial crime grows, professionals who possess high-level skills in information and communications technology (ICT) are almost certain to play integral roles in facilitating financial crimes.

Open-source information provides examples of networks of ICT specialists collaborating with others who possess knowledge of financial markets.<sup>6</sup>

Individuals, businesses, government and industry who rely on or are increasing the integration of technology in service delivery are particularly vulnerable. They will need to employ requisite technical expertise, cybersecurity practices and information security infrastructure to withstand and respond to the threat of technology-enabled financial crime.

### OUTLOOK

Rapid advances in technology have provided organised crime groups and ‘tech-savvy’ criminal individuals with new ways to target larger pools of victims with fewer resources and less risk of detection. It is almost certain that such groups and individuals will continue to use technology to enable financial crime as well as develop new methodologies to target further victims. It is almost certain that these criminal groups and individuals will increasingly exploit the use of ICT to facilitate financial crimes and seek out professional facilitators who possess the necessary knowledge to support technology-enabled financial crime.

## IDENTITY CRIME

### INTRODUCTION

Identity crime, although under-reported, is now among the most prevalent and constantly changing crime types. As well as enabling crime, it is also a crime in its own right, carried out by serious and organised crime groups and cybercriminals.

An increased reliance on personal identifying information (PII) for online services, along with the exploitation of technology by criminals, has seen identity crime become one of the most pervasive crime types in Australia.



### IDENTITY CRIME KEY OBSERVATIONS

- The theft, and subsequent on-selling, of personal identifying information is a highly lucrative crime that can enable other serious financial crimes such as superannuation fraud and refund fraud.
- Identity crime, particularly the harvesting of personal identifying information, is likely to increase as this data is increasingly stored online.

### CURRENT SITUATION

Criminal actors employ a variety of methodologies to gain access to PII, from the theft of sensitive documentation, to more sophisticated techniques that rely on the use of technology and cybercrime techniques such as phishing,<sup>7</sup> social engineering<sup>8</sup> or the deployment of credential harvesting malware. PII is a valuable commodity, traded and sold by criminals to serious and organised crime groups with a view to facilitating other financial crimes.

### REFUND FRAUD

Refund fraud is characterised by the submission of false income tax returns or activity statements with the aim of fraudulently obtaining refunds. Organised crime groups and individuals use a range of methods to achieve this, from using a false identity or, increasingly, using stolen information to impersonate someone else.

6 Vengerik, B Dennesen, K, Berry J & Wrolstad, L 2014, *Hacking the street? FIN4 likely playing the market*, FireEye, California, viewed 15 May 2016, <[https://\\_www2.fireeye.com/rs/fireeye/images/rpt-fin4.pdf](https://_www2.fireeye.com/rs/fireeye/images/rpt-fin4.pdf)>.

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

8 Social engineering is the use of deception to manipulate individuals into revealing PII that may be used for fraudulent purposes.

# CASE STUDY

## SUPERANNUATION-RELATED IDENTITY THEFT

A serious and organised cybercrime group hacked a superannuation fund member's home computer system, gaining access to PII including emails, banking details and travel plans. Post-hack, the group was also able to monitor the victim's superannuation fund transactions. When the victim travelled overseas the group made an online request from the victim's email for a superannuation payment variation.

The superannuation fund called the victim's contact number to confirm the variation request. However, the serious and organised crime group had diverted the victim's phone number to one it controlled. In this instance the fraud was able to be stopped after the victim noticed unusual transactions and changes on their bank account statement and the funds were frozen by the victim's bank.



**AUSTRALIA'S LARGE POOL  
OF SUPERANNUATION  
FUNDS IS ATTRACTIVE  
TO CRIMINALS**

In the 2014-15 financial year, the ATO identified and prevented incorrect refund payments valued at approximately \$754 million<sup>9</sup> out of a total legitimate refund pool of \$95 billion.

### SUPERANNUATION FRAUD

Australia's large pool of superannuation funds is an attractive target for criminals. Identity crime enables superannuation fraud through the illegal acquisition of PII that is then used to fraudulently access superannuation funds. Increasingly, technology and cybercrime techniques are facilitating illegal access to PII and are also supporting superannuation fraud activities.

Superannuation fraud in Australia is made possible through the use of technology, cybercrime techniques and identity crime. Historically, identity crime enabled fraud targeting superannuation accounts was conducted by criminal entities stealing statements from the mail and using the PII contained in these statements to create fake identity documents that were then used to steal funds. Now criminal entities are using online methods to enable fraudulent access to superannuation accounts.

### OUTLOOK

Identity crime will likely increase in frequency as the volume of PII stored online increases. As more financial services are provided online, there is a requirement for more personal identifiers, such as personal identification numbers, passwords, access codes and security questions, to be created and stored. These personal identifiers are of value to criminal entities and will continue to be harvested, sold and used in fraud and to access systems for other criminal purposes.

Identity takeover is likely to emerge as the primary identity crime methodology used to facilitate financial crime, rather than identity creation. As government agencies and private institutions increase services offered online, it is likely that new identity crime enabled financial crime methodologies will be observed.

<sup>9</sup> The ATO advises that there can be difficulties quantifying refund fraud as there are sometimes difficulties in distinguishing between refund fraud, which is intentional, and refund integrity matters, which are unintentional.

## PROFESSIONAL FACILITATORS

### INTRODUCTION

Professional facilitators are industry professionals and subject matter experts who provide their specialist skills and knowledge, either wittingly or unwittingly, for the benefit of individuals and groups looking to engage in serious financial crime activities.

Professional facilitators may or may not be complicit in assisting criminal groups and individuals in financial crime. Some professional facilitators are unknowingly involved, some are recruited through extortion or intimidation, and others willingly participate, often making significant personal financial gains from the association.

### CURRENT SITUATION






























Increasingly, the globalised and complex nature of the financial sector, and the legislative and regulatory rules that govern it, make it necessary to engage professionals with specialist knowledge and skills. As such, professional facilitators—and the employees of professional facilitators, who also have specialist knowledge and/or access to restricted data—are attractive resources for those seeking to engage in serious financial crime.



### PROFESSIONAL FACILITATORS KEY OBSERVATIONS

- Professional facilitators are intrinsic enablers of serious financial crime, with the range of professions used to facilitate financial crime extending beyond those traditionally considered to be exploited such as lawyers and accountants, to include real estate agents, liquidators and financial advisers. Australia's current anti-money laundering/counter-terrorism financing controls are yet to reflect this diversity, creating significant opportunities for these facilitators to enable the movement of funds without the requirement to report to authorities.

**TABLE 1: PROFESSIONAL FACILITATORS INVOLVED IN SIGNIFICANT FINANCIAL CRIME ACTIVITIES**

	LAWYERS	ACCOUNTANTS/ FINANCIAL ADVISERS	LIQUIDATORS/ PRE-INSOLVENCY ADVISERS	OFFSHORE SERVICE PROVIDERS	ICT PROFESSIONALS	REAL ESTATE AGENTS
MONEY LAUNDERING						
SUPERANNUATION FRAUD						
INVESTMENT AND FINANCIAL MARKET FRAUD						
REVENUE AND TAX FRAUD						
ILLEGAL PHOENIX BEHAVIOUR						
ABUSIVE USE OF TRUSTS AND COMPANIES						
TECHNOLOGY-ENABLED FINANCIAL CRIME						

Some of the primary professional facilitators identified across some of the key financial crime markets are outlined in Table 1.

These commonly identified professional facilitators may use their professional positions or expertise to support serious financial crime activities in unique and varying ways:

- **Lawyers** can provide knowledge of tax law, company law and trust law, and advice on the use of company structures and trusts.
- **Accountants and financial advisers** often work closely with legal professionals to assist in concealing illicit wealth and advise on tax evasion strategies.
- **Liquidators and pre-insolvency advisers** may be used to facilitate illegal phoenix activities.
- **Offshore service providers** often work closely with legal professionals and can facilitate the creation of offshore corporate structures and associated bank accounts.<sup>10</sup>
- **Information and communications technology professionals** are critical to groups and individuals seeking to engage in financial crime who particularly require the use of technology, cybercrime and secure or encrypted communications practices.
- **Real estate agents** can facilitate the concealment of illicit wealth and money laundering through buying and selling high-value property.

In addition to these traditional professions that may facilitate serious financial crime, there are non-professional individuals who may be able to provide access to specialised knowledge, information or infrastructure, such as restricted datasets or computer systems, through their industry positions. These facilitators can provide expert opinion obtained from working within a particular sector or position regarding vulnerabilities that may be exploited to support serious financial crime.

## OUTLOOK

As outlined in *Organised Crime in Australia 2017*, serious and organised crime groups and individuals engaging in financial crime are likely to seek opportunities to increase illicit profits, avoid law enforcement detection, protect assets and conceal criminal wealth. Professional facilitators will continue to be fundamental in enabling financial crime, whether it is to launder funds or move money and/or assets offshore through complex financial structures or the exploitation of regulatory vulnerabilities.

## OFFSHORE SERVICE PROVIDERS

### INTRODUCTION

Offshore service providers (OSPs) facilitate the creation of offshore corporate structures and associated bank accounts as well as provide administration services, nominee directors or shareholders. These companies are often set up for legitimate tax minimisation purposes.

While the services offered by OSPs are legal, they are an attractive resource for serious and organised crime groups looking for ways to conceal beneficial (or true) ownership of assets and transfer illicit funds between jurisdictions. OSPs frequently use countries with strict secrecy provisions to incorporate companies, providing additional layers of anonymity.



### OFFSHORE SERVICE PROVIDERS KEY OBSERVATIONS

- Offshore service providers are likely to favour international jurisdictions that have a lower perceived risk and strong reputation for strict secrecy provisions, enabling additional levels of anonymity for their clients.

<sup>10</sup> More information is available in the next chapter 'Offshore service providers', which addresses the specific offshore services they provide to Australian citizens.



The anonymity afforded to clients of an OSP enables a range of criminal activity, including money laundering, and investment, superannuation and tax fraud. The use of multiple jurisdictions to register corporate entities, open bank accounts and hold assets can make investigation and disruption by law enforcement and regulatory agencies difficult, time consuming and expensive.

## CURRENT SITUATION

The use of OSPs to enable a range of serious financial crime is an ongoing issue. Investigations conducted under Project Wickenby uncovered widespread use of international OSPs to facilitate tax evasion and to conceal the beneficial ownership of a range of assets. OSPs continue to be used to create and administer offshore entities for the same purposes.

The publication of Mossack Fonseca client data has provided insight into the current extent to which Australian citizens and residents make use of OSPs. To date, over 1,000 entities have been identified as having used the services of Mossack Fonseca. However, while Mossack Fonseca was used to create offshore structures, the majority of Australian entities dealt with intermediaries in Australia or other jurisdictions, who in turn used Mossack Fonseca to register offshore entities. A number of clients were therefore not even aware that Mossack Fonseca was the entity that had registered their offshore entities. These layered arrangements can make it difficult to identify the beneficial ownership of corporate entities and associated assets.

While legitimate business people may be endeavouring to avoid or minimise tax, organised crime groups are more likely to use corporate structures created and administered by OSPs to hold funds derived from the sale of illicit commodities, as well as to return the funds to Australia to support an extravagant lifestyle and provide capital for legitimate investments.

## OUTLOOK

During the next two years, serious and organised crime groups and criminal individuals are likely to continue to use OSPs to maintain anonymity and facilitate criminal activity. The use of OSPs to create and administer offshore corporate entities is, and will almost certainly remain, legal. While OSPs provide a legitimate service, the existing legislation in many of the jurisdictions in which they operate provides scope for organised crime groups and individuals to exploit the system. It is also highly likely that many OSPs knowingly operate in a way that allows clients to conceal their identity and beneficial ownership of assets behind corporate structures.

The release of the Mossack Fonseca data, a growing recognition of the loss of taxation revenue and the exploitation of OSPs by a broad range of criminal groups has resulted in legislative change designed to restrict the criminal use of offshore corporate structures. The European Union has recently adopted changes to its anti-money laundering rules that will require each member state to maintain a public register showing the beneficial owners of companies and business-related trusts and enable the connection of these registers to facilitate cooperation between countries. Likewise, the United Kingdom has created a public register of the beneficial ownership of corporate entities.

Following the recent statutory review of Australia's anti-money laundering/counter-terrorism financing regime,<sup>11</sup> consideration is being given to legislative change designed to improve reporting requirements and enhance AUSTRAC's ability to capture financial intelligence related to the operation of OSPs.

A number of different models have been proposed, ranging from OSPs voluntarily registering with AUSTRAC to the use of domestic levers to compel registration or a requirement for Australian businesses to register offshore affiliates.

11 Attorney-General's Department 2016, *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations*, AGD, Canberra, viewed 2 May 2017, <[https://\\_www.ag.gov.au/Consultations/Documents/StatutoryReviewAnti-MoneyLaunderingAndCounter-TerrorismFinancingActCth200/report-on-the-statutory-review-of-the-anti-money-laundering.pdf](https://_www.ag.gov.au/Consultations/Documents/StatutoryReviewAnti-MoneyLaunderingAndCounter-TerrorismFinancingActCth200/report-on-the-statutory-review-of-the-anti-money-laundering.pdf)>.

## ILLEGAL PHOENIX ACTIVITY

### INTRODUCTION

Illegal phoenix activity is ‘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’.<sup>12</sup> Illegal phoenix operators have an unfair advantage when competing with other similar businesses because they accumulate debts they have no intention of repaying.

At its simplest, illegal phoenix activity involves running up debts in a company until it becomes insolvent and is placed into liquidation. The phoenix company is often a labour supply or employing entity with negligible assets and, once liquidated, the employees are transferred to a new company typically controlled by the same person or group.

### CURRENT SITUATION

Illegal phoenix activities divert money that should be afforded to the Australian revenue and tax systems to individuals through their businesses. Illegal phoenix activity results in employees not being paid the wages and superannuation to which they are entitled. Foreign workers are often exploited as part of the illegal phoenix activity.

Serious and organised crime groups have been identified as using illegal phoenix behaviour as a business strategy. Illegal phoenix activity is attractive to serious and organised crime groups partly due to the illicit profits that can be made by intentionally not paying goods and service tax, income tax or superannuation costs.

A current concern is the growth in the ‘pre-insolvency adviser’ market and its role in facilitating and promoting illegal phoenix activity. Unlike registered liquidators, pre-insolvency advisers operate in an unregulated environment. Some pre-insolvency advisers have been found to promote and facilitate illegal phoenix activities, for example by encouraging directors and accountants to transfer assets to new entities for less than market value, or to destroy or alter company records.<sup>13</sup>

<sup>12</sup> Australian Taxation Office, *Illegal phoenix activity*, viewed 2 May 2017, <<https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Illegal-phoenix-activity/>>.

<sup>13</sup> Australian Taxation Office 2016, *Phoenix Taskforce swoops on pre-insolvency industry*, viewed 18 July 2017, <<https://www.ato.gov.au/media-centre/articles/media-releases/phoenix-taskforce-swoops-on-pre-insolvency-industry/>>.



### ILLEGAL PHOENIX ACTIVITY KEY OBSERVATIONS

- The loss of tax and revenue caused by illegal phoenix activity has a negative impact on the Australian community as less money is available for community needs.
- The Australian Government has set in motion investigations and many modifications to the laws governing business to protect Australia from illegal phoenix activity.

There is no specific offence titled ‘illegal phoenix activity’ and this makes applying effective sanctions difficult, but there are applicable offences within the *Corporations Act 2001* that can be applied to the actions taken by directors and their advisers that result in illegal phoenix activity.

### PHOENIX TASKFORCE

The Australian Government is addressing illegal phoenix activity through information sharing, with government agencies working together on the multi-agency Phoenix Taskforce to identify those attempting to compromise the system. Through focused detection efforts, government agencies have increased the number of companies identified as using illegal phoenix behaviours.

### OUTLOOK

The ATO and ASIC experience demonstrates that phoenix operators and those who assist them are adaptable and, over time, become more deceptive and fraudulent. Regulators are responding to illegal phoenix models. Activities include not only enforcement, but disruption measures based on better market intelligence and an increasing use of data analytics to identify the high risk operators and their advisers.

# CASE STUDY

## PRE-INSOLVENCY ADVISERS LODGED FALSE DOCUMENTS WITH ASIC

An ASIC investigation culminated in charges being laid against two pre-insolvency advisers for lodging false documents with ASIC under a fictitious director identity. The fraud was undertaken to facilitate illegal phoenix activity by stripping assets from companies subject to liquidation.

The pre-insolvency adviser who created the fictitious identity was convicted of aiding and abetting the lodgement of false documents with ASIC and sentenced to six months imprisonment, suspended upon entering into a recognisance order to be of good behaviour for 12 months with a \$1,000 surety.

The pre-insolvency adviser's business partner—a chartered accountant who jointly ran the pre-appointment insolvency service—lodged the false and misleading documents appointing the fictitious identity as a company director with ASIC. The accountant was later convicted of this offence and sentenced to eight months imprisonment, to be served by way of an intensive correction order.<sup>i</sup>

<sup>i</sup> Australian Securities and Investment Commission 2015, *15-031MR Gold Coast chartered accountant sentenced following ASIC investigation*, media release, 19 February, ASIC, Canberra, viewed 3 May 2017, <[http://\\_asic.gov.au/about-asic/media-centre/find-a-media-release/2015-releases/15-031mr-gold-coast-chartered-accountant-sentenced-following-asic-investigation/](http://_asic.gov.au/about-asic/media-centre/find-a-media-release/2015-releases/15-031mr-gold-coast-chartered-accountant-sentenced-following-asic-investigation/)>; Australian Securities and Investment Commission 2013, *13-356MR Former Gold Coast businessman pleads guilty to charges of creating a phantom company director and obstructing ASIC*, media release, 20 December, ASIC, Canberra, viewed 20 July 2017, <[http://\\_www.asic.gov.au/about-asic/media-centre/find-a-media-release/2013-releases/13-356mr-former-gold-coast-businessman-pleads-guilty-to-charges-of-creating-a-phantom-company-director-and-obstructing-asic/](http://_www.asic.gov.au/about-asic/media-centre/find-a-media-release/2013-releases/13-356mr-former-gold-coast-businessman-pleads-guilty-to-charges-of-creating-a-phantom-company-director-and-obstructing-asic/)>.



**ILLEGAL PHOENIX BEHAVIOUR  
IS A BUSINESS STRATEGY  
FOR ORGANISED CRIME**

Legislative changes go some way to addressing the problem. The *Insolvency Law Reform Act 2016* (the Act) modified the registration requirements for corporate insolvency practitioners to align with those of personal insolvency practitioners. Registered liquidators are no longer registered indefinitely, but instead must renew their registration every three years, in line with bankruptcy trustee registration requirements. The Act also introduced a new discipline process for registered liquidators.

Further, the Act increases ASIC's surveillance powers to review registered liquidator conduct, similar to the Australian Financial Security Authority's supervision of registered trustees. These initiatives, and the potential for further law reform, aim to mitigate the opportunity for illegal conduct and further improve integrity in the industry through enhanced options for addressing registered practitioner misconduct.

In September 2017, the Australian Government approved an initiative that would issue all Australian company directors with a unique Directors Identity Number. This initiative will provide a national reporting mechanism that enables government agencies to identify links between company directors and other companies and people that may be connected to illegal phoenix activity.

## ABUSIVE USE OF TRUSTS

### INTRODUCTION

Trusts are widely used for legitimate business and investment purposes,<sup>14</sup> including asset protection and tax liability reduction. The *abusive* use of trusts specifically refers to situations in which individuals have used trust structures to hide their control of a trust fund and extract wealth without being accountable for their tax obligations. An individual is able to control substantial assets using a trust structure. The control of those assets is often concealed by using a nominee or a trustee company whose officers and shareholders are not traceable. Individuals have exploited trusts to avoid or evade tax by concealing income, artificially reducing income and mischaracterising financial transactions.



### ABUSIVE USE OF TRUSTS KEY OBSERVATIONS

- Abusive use of trusts continues to contribute to revenue and tax fraud in Australia, with trust structures permitting individuals to effectively control significant wealth anonymously.
- There is scope for Australia to implement measures to promote transparency of beneficial ownership of trust funds, with indications that reforms may occur in the future.

### CURRENT SITUATION

The abusive use of trusts contributes to the overall total of revenue and tax fraud in Australia. Serious and organised crime groups and significant criminal individuals based in Australia and overseas have been identified as exploiting Australia's tax system through the abusive use of trust structures. Criminal groups and individuals use trust funds to conceal criminal wealth, support criminal activity and launder illicit funds.

The lack of transparency and the complexity inherent in legislative and regulatory frameworks surrounding trusts enable serious and organised crime groups and criminal individuals to conceal financial dealings using trust structures and provide anonymity to the beneficial owners.

Given the complexities of trust structures, there is an enhanced requirement to use professional facilitators. Tax agents, accountants and legal practitioners facilitate the creation, use and management of trusts; however, a small number of these same specialists have been identified as being noncompliant.

<sup>14</sup> Australian Taxation Office, *Trusts*, viewed 27 March 2017, <<https://www.ato.gov.au/general/trusts/>>.

# CASE STUDY

## ABUSIVE USE OF TRUST ACTIVITIES

The abusive use of trusts was employed to evade paying in excess of \$50 million in tax in the property development sector over a period of 10 years. It involved the siphoning off of profits from the main entities to trusts and companies controlled by the principal and their siblings, with these profits then being remitted offshore.

In some cases, completed properties were transferred below market value to related trusts, before being revalued to market prices and fully mortgaged, with the finance raised purportedly invested in a sham offshore property development syndicate. This had the effect of understating assessable profits, creating insolvency and recovery difficulties, and transferring wealth offshore without tax being paid. The case also involved related 'straw directors' (including offshore nominee directors), and raised doubts about the independence of appointed liquidators.



**TRUST FUNDS CAN BE USED TO  
CONCEAL CRIMINAL WEALTH,  
SUPPORT CRIMINAL ACTIVITY  
AND LAUNDER ILLICIT FUNDS**

## TRUSTS TASKFORCE

Professional facilitators who promote the misuse of trust structures were among those targeted by the former Trusts Taskforce.<sup>15</sup> Since its inception in 2013, the ATO-led Trusts Taskforce raised \$948 million in liabilities and collected \$279 million from individuals and businesses involved in tax evasion using trusts. An additional \$55 million worth of assets have also been restrained under proceeds of crime legislation.<sup>16</sup> Since 1 July 2017, the work of the Trusts Taskforce has continued under the ATO's Tax Avoidance Taskforce—Trusts.

Since the release of the Mossack Fonseca data, transparency and beneficial ownership, along with the role of professional facilitators, became particularly prominent issues for law enforcement, regulatory agencies and government. There is substantial overlap between trusts and offshore tax evasion.

## OUTLOOK

The revenue and tax fraud that occurs through the abusive use of trusts has an impact on the Australian community with the loss of government revenue resulting in less tax funds being available to spend on essential government services such as infrastructure, transport, health and education.

There is scope to improve the transparency of trusts in Australia. Early indications for change are noted in the Australian Minister for Justice's announcement at the United Kingdom Anti-Corruption Summit in May 2016, making a commitment to consult on options for a beneficial ownership register for companies. If measures recently implemented in other countries to improve corporate and trust transparency have an impact, similar reforms may occur in Australia. These reforms would go some way to increasing transparency of beneficial ownership, particularly measures relating to trusts, which would potentially reduce revenue and tax fraud in Australia.

## HIGH-VALUE COMMODITIES

### INTRODUCTION

High-value commodities continue to provide an effective vehicle for organised crime groups and criminal entities to commit financial crime.

<sup>15</sup> Australian Taxation Office 2017, *Trusts Taskforce*, viewed 27 March 2017, <[https://\\_www.ato.gov.au/general/trusts/in-detail/compliance/trusts-taskforce/](https://_www.ato.gov.au/general/trusts/in-detail/compliance/trusts-taskforce/)>.

<sup>16</sup> *ibid.*



## HIGH-VALUE COMMODITIES KEY OBSERVATIONS

- Organised crime groups will continue to use high-value commodities as a way to exchange and conceal proceeds of crime.

They are used to store and transfer value and launder the proceeds of crime, due to the opportunity they afford to conceal illicit profits in legitimate assets that can be purchased with minimal regulatory oversight, and can over time accumulate ostensibly legitimate value.

High-value commodities include real estate, precious gems, valuable metals, art, antiquities, luxury vehicles and gold bullion. Gold bullion is not only used to store or transfer value but provides a way to exploit different tax treatments for gold and obtain fraudulent refunds.

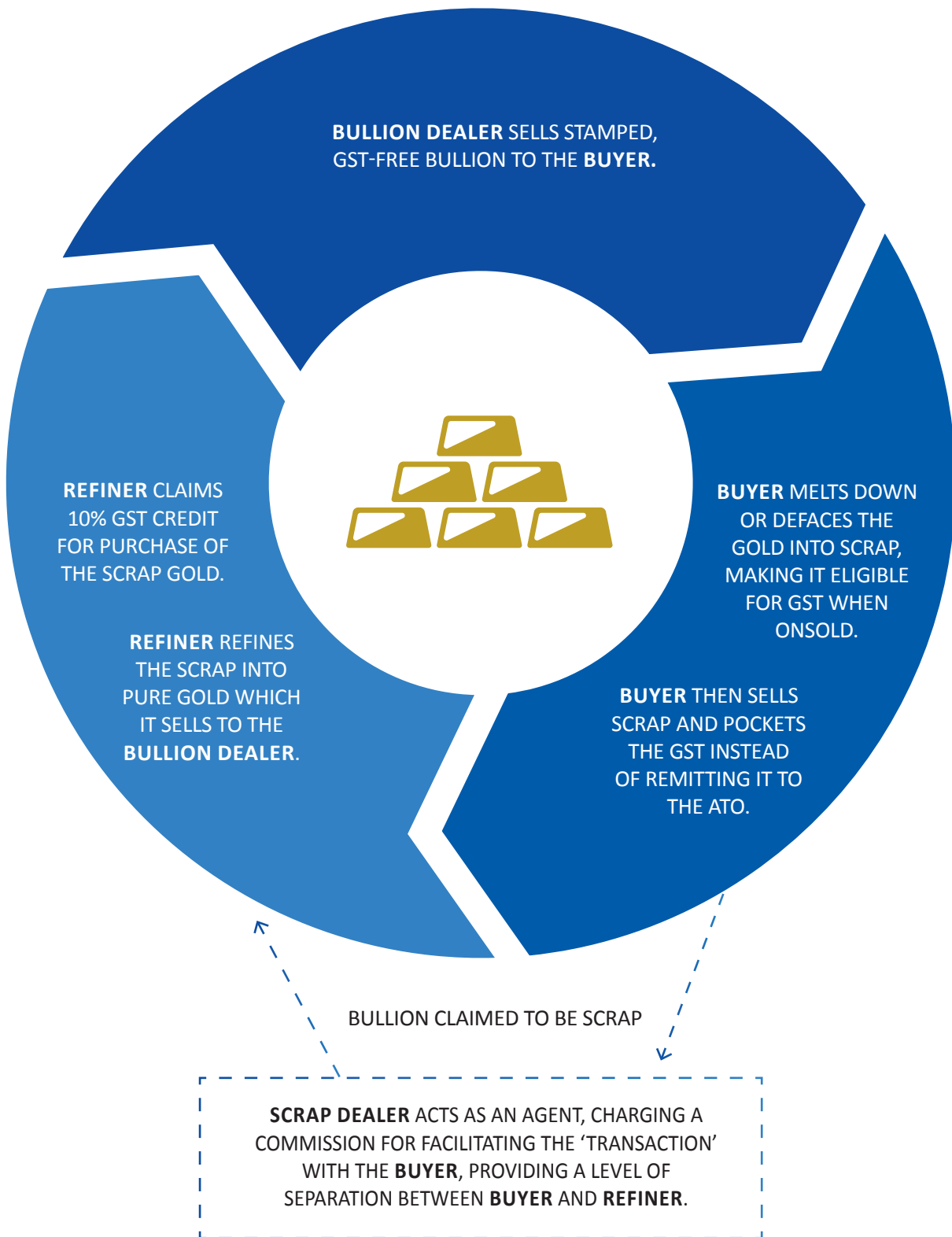
## CURRENT SITUATION

### Australian real estate

The real estate sector in Australia is a strong investment vehicle for Australian and international investors. For those seeking to launder money or conceal proceeds of crime, the advantages of investing illegal profits in Australian real estate are that, not only is the value of investment likely to increase, the beneficial (true) ownership of the property can be concealed. In addition, professionals facilitating real estate transactions—such as real estate agents, conveyancers and lawyers—are not subject to most controls under Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime. They currently have no legal obligation to report suspicious transactions, despite these professions posing high money laundering/terrorism financing risks.<sup>17</sup>

<sup>17</sup> Attorney-General's Department 2016, *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations*, AGD, Canberra, viewed 10 May 2017, <[https://\\_www.ag.gov.au/Consultations/Documents/StatutoryReviewAnti-MoneyLaunderingAndCounter-TerrorismFinancingActCth200/report-on-the-statutory-review-of-the-anti-money-laundering.pdf](https://_www.ag.gov.au/Consultations/Documents/StatutoryReviewAnti-MoneyLaunderingAndCounter-TerrorismFinancingActCth200/report-on-the-statutory-review-of-the-anti-money-laundering.pdf)>.

**FIGURE 1: GOLD BULLION ENABLING GST FRAUD**



### Precious gems, valuable metals, arts and antiques

Precious gems, valuable metals, art and antiques also present opportunities for organised crime groups and criminal entities to transfer and store illicit wealth. Jewellery and precious gems in particular can be accepted within the criminal fraternity as a form of currency, where the transfer of value or the encashment of items are largely untraceable. The significant value of small items of jewellery and precious gems also enables more convenient storage, transfer and concealment than the equivalent value in cash. The goods are also free from reporting obligations when purchased using cash or when being moved out of Australia.

### Gold bullion

The high value of gold and its availability and portability provide significant opportunity for exploitation of the existing goods and services tax (GST) provisions, particularly in organised crime networks. GST fraud using gold bullion has been previously identified through the work of ATO Operation Nosean (see Figure 1). This type of fraud involved altering or misclassifying pure gold bullion and coins—which are not legally taxed—as lesser quality or scrap gold, which is taxed at 10 per cent, to fraudulently claim refunds in the form of GST tax credits.

This work of the ATO identified how valuable metals have created unique opportunities for criminal exploitation, but new government rules, enacted on 1 April 2017, require a reverse charge of GST to apply to all business-to-business taxable supplies of gold, silver and platinum, which places the onus on the purchaser of the valuable metal, not the supplier, to remit the GST to the ATO.

### OUTLOOK

Vulnerabilities in the AML/CTF framework have been highlighted as enabling criminal exploitation of high-value commodities. Focus has been placed on the current lack of reporting regulations for designated non-financial businesses and professions (DNFBPs), such as real estate agents, legal professionals and high-value dealers of valuable metals and precious gems—not including bullion dealers, who are regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). The 2016 review of Australia's AML/CTF regime recommended that options be developed to regulate DNFBPs under the AML/CTF Act.

## ALTERNATIVE BANKING SERVICES

### INTRODUCTION

Alternative banking services (ABSs) are used by individuals and companies to move funds around the world outside existing regulated banking frameworks. ABSs generally offer low-cost international value transfers and virtually instantaneous delivery of funds.



### ALTERNATIVE BANKING SERVICES KEY OBSERVATIONS

- The use of alternative banking services currently appears to be more common in international jurisdictions than in Australia.

### CURRENT SITUATION

An ABS acts as an online banking interface that sits above and coordinates multiple bank accounts in various international locations. It provides a platform that hides the connection between the user of the service and any funds that are transferred, enabling members of the service to transfer value in a way that conceals the identity of the sender, recipient and beneficial owner. While the funds that enter the ABS account are pooled, the online banking platform provides the mechanism through which individual accounts within the ABS are managed.

Legitimate entities that favour these services include small businesses that operate transnationally, as they are attracted to the low transfer fees, which enable them to remain competitive, and geographically-dispersed families who need to transfer money in a timely manner. However, the anonymity that ABSs provide to clients also makes them attractive to serious and organised crime groups and criminal individuals. These criminal entities may exploit ABSs to enable a range of criminal activities including money laundering, tax evasion and various types of fraud.

### OUTLOOK

It is likely that ABSs will continue to provide a viable method for serious and organised crime groups and criminal individuals involved in financial crime to enable the movement of funds globally. However, the use of ABSs currently appears to be more common in international jurisdictions than in Australia.