



AUSTRALIAN
**CRIMINAL
INTELLIGENCE
COMMISSION**

SERIOUS FINANCIAL CRIME IN AUSTRALIA

2017



CONTENTS

FOREWORD	6
INTRODUCTION	8
Defining serious financial crime	8
Tackling serious financial crime	9
Generating financial crime intelligence	11
FINANCIAL CRIME ENABLERS	12
Money laundering	12
Technology	14
Identity crime	15
Professional facilitators	17
Offshore service providers	19
Illegal phoenix activity	21
Abusive use of trusts	23
High-value commodities	25
Alternative banking services	27
FINANCIAL CRIME MARKETS	28
Cybercrime	28
Investment and financial market fraud	30
Revenue and taxation fraud	34
Superannuation fraud	37
Card fraud	39
Health and welfare fraud	43
FINANCIAL CRIME OUTLOOK IN AUSTRALIA	45
Key predictions	45
Opportunities	45
ACRONYMS	47

SNAPSHOT



MONEY LAUNDERING

‘Money laundering occurs on a global scale with proceeds of crime transferred between jurisdictions, commingled with legitimate monies and integrated into legitimate markets.’



TECHNOLOGY

‘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.’



IDENTITY CRIME

‘Identity crime, although under-reported, is now among the most prevalent and constantly changing crime types.’



PROFESSIONAL FACILITATORS

‘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.’



OFFSHORE SERVICE PROVIDERS

‘The anonymity afforded to clients of an OSP enables a range of criminal activity, including money laundering, and investment, superannuation and taxation fraud.’



ILLEGAL PHOENIX ACTIVITY

‘Illegal phoenix activities divert money that should be afforded to the Australian revenue and tax systems to criminal individuals through their businesses.’



ABUSIVE USE OF TRUSTS

‘Criminal groups and individuals use trust funds to conceal criminal wealth, support criminal activity and launder illicit funds.’



HIGH VALUE COMMODITIES

‘Precious gems and metals, art and antiquities ... present opportunities for organised crime and criminal entities to transfer and store illicit wealth.’



ALTERNATIVE BANKING SERVICES

‘Alternative Banking Services (ABS) are used by individuals and companies to move funds around the world outside existing regulated banking frameworks.’



CYBERCRIME

‘The global cybercrime market is a low risk, high return criminal enterprise.’



INVESTMENT AND FINANCIAL MARKET FRAUD

‘Australia will continue to be a target for domestic and offshore investment fraud activities.’



REVENUE AND TAXATION FRAUD

‘Identity crime related to refund fraud is an increasing problem.’



SUPERANNUATION FRAUD

‘Australia’s large pool of superannuation funds is an attractive target for criminal groups and individuals.’



CARD FRAUD

‘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.’



HEALTH AND WELFARE FRAUD

‘...it is anticipated that the targeting of online government portals will increase and that these systems may possibly be breached by offshore entities.’

**WORLDWIDE,
FINANCIAL CRIME
IS ON THE RISE**

FOREWORD

Serious Financial Crime in Australia 2017 is the inaugural unclassified report produced by the Australian Criminal Intelligence Commission that highlights the way serious financial crimes are impacting on the Australian community.

As a member agency of the Serious Financial Crime Taskforce, the Australian Criminal Intelligence Commission is responsible for assessing the financial crime threat picture. To do this, we collaborate with government partners, industry and the community to collect information and intelligence that inform these threat assessments and appropriate response strategies.

Serious financial crime impacts on all Australians. For some, it may be the direct loss of savings through an investment scam, or the compromise of their personal information, which is then used to commit credit card fraud.

For most, it is the indirect impacts of serious financial crime that are less obvious but more wide-ranging. For example, the loss of government revenue resulting from tax fraud and health and welfare fraud means there are fewer funds available to the government to spend on essential services such critical infrastructure, health and welfare benefits and education programs.

Serious financial crime threats are located both in Australia and offshore. We estimate that around 70 per cent of Australia's serious and organised criminal threats are based offshore or have strong offshore links. As a result, the Australian Criminal Intelligence Commission has been building closer relationships with international partners to facilitate knowledge-sharing of transnational crime threats, including serious financial crime threats that are impacting on Australia. This supports us in building more accurate threat assessments and informs effective response strategies.

Serious financial crime is committed by serious and organised crime groups and criminal entrepreneurs who have the expertise and resources—similar in some ways to the traditional 'white collar' criminals. However, the way in which financial crime is committed has evolved significantly compared to the traditional methods of the past.

Technology is playing an increasingly significant role in enabling financial crime. For example, technology has enabled large-scale phishing and targeted data hacks to obtain personal identifying information, which can then be used to facilitate other financial crimes such as card fraud.

We are also seeing an increase in cybercrime intrusions into superannuation and payroll platforms that contain a range of personal and financial information that could be used to enable further criminal activities.



The threat posed by technology-enabled financial crime and cybercrime activities will continue to grow as technology evolves and as government and industry continue to integrate technology into service delivery.

The complexity of financial crime is also increasing. The expertise of professional facilitators who help to navigate financial frameworks and technology systems to exploit vulnerabilities often makes it difficult to even identify that a crime has been committed. This proficiency is extremely valuable to individuals and groups wanting to test framework boundaries, exploit systemic vulnerabilities, or to circumvent laws and commit criminal acts. Professional facilitators play a fundamental role in navigating financial, regulatory and information systems to support financial crime.

Offshore service providers are also playing an increasing, more visible role in assisting tax evasion or, in some cases, laundering the proceeds of crime.

All of these factors—offshore threats, technology and professional facilitators—contribute to the complexity of financial crime affecting Australia.

The Australian Criminal Intelligence Commission was formed to strengthen our response to crime affecting Australia. Through our investigative, research and information delivery services, we are actively working with our law enforcement partners to stop criminals exploiting emerging opportunities and perceived gaps in law enforcement information.

As serious financial crime in Australia increases, so too do our law enforcement and intelligence capabilities to combat serious and organised crime. Through our Determination Targeting Criminal Wealth No. 2 Special Investigation, we are actively monitoring financially-motivated crime, working to disrupt and deter criminal groups, collecting evidence and intelligence about their illicit activities and connecting our law enforcement partners to this crucial information.

This special investigation into financially-motivated crime brings together our work investigating money laundering, serious and organised investment fraud, sophisticated tax evasion and confiscating criminal wealth. It enables us to work with our partners to:

- deliver financial intelligence that identifies high-value targets and provides new opportunities for law enforcement and regulatory partners
- build national knowledge of money laundering, nationally significant tax fraud and other financially-motivated crimes
- help make Australia unattractive for abusive financial arrangements and money laundering
- reduce the impact of serious financial crime on the Australian community
- produce intelligence that contributes to whole-of-government policies and law enforcement decision-making.

Our mission is to make Australia safer through an improved national ability to discover, understand and respond to current and emerging crime threats and criminal justice issues, including the ability to connect police and law enforcement to essential policing knowledge and information. By building a national threat picture, we can inform government partners, industry participants and the community about key threats, strategies to disrupt crime and opportunities to better position ourselves against emerging threats.



Michael Phelan APM
Chief Executive Officer
Australian Criminal Intelligence Commission

INTRODUCTION

Serious Financial Crime in Australia 2017 presents the national picture of serious financial crime currently impacting on the Australian community.

In 2015, the Australian Government established the Serious Financial Crime Taskforce, a multi-agency task force that unites the operational and strategic intelligence capacity and responsibilities of task force agencies to identify and respond to serious financial crime in Australia. The Serious Financial Crime Taskforce member agencies include:

- Attorney-General's Department (AGD)
- Australian Border Force (ABF)
- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Securities and Investments Commission (ASIC)
- Australian Taxation Office (ATO)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Commonwealth Director of Public Prosecutions (CDPP).

Serious Financial Crime in Australia 2017 draws on the collaborative work of the Serious Financial Crime Taskforce agencies, as well as intelligence and operational data held by a broad range of law enforcement, regulatory and other government agencies. The work undertaken by the Serious Financial Crime Taskforce identifies the key threat priorities for operational treatment, ongoing intelligence collection and proposed policy and legislative change. The current priorities of the Serious Financial Crime Taskforce include international tax evasion, illegal phoenix activity, abusive use of trust structures, and criminality related to offshore service providers and superannuation funds.

The objective of the Serious Financial Crime Taskforce is to maintain integrity and community confidence in the Australian economy, financial markets, regulatory framework and revenue collection.

As at August 2017, the efforts of the Serious Financial Crime Taskforce have recouped \$152.53 million for the Commonwealth, raised \$391.93 million in tax liabilities, executed 54 search warrants, completed 587 audits, prosecuted four people and convicted four people.¹

DEFINING SERIOUS FINANCIAL CRIME

Financial crime causing major harm to Australia extends beyond that being committed by serious and organised crime groups. In particular, a significant and growing threat is presented by sophisticated individuals and groups exploiting systemic vulnerabilities in taxation and revenue systems and government health and welfare programs. This is in addition to individuals using offshore structures to evade paying tax in Australia.

The serious financial crime intelligence picture also highlights the complexity of some of the emerging financial crime issues, many of which require ongoing multi-agency cooperation to better understand financial crime and to develop mitigation strategies. Examples include the way in which identity crime enables financial crime and the constantly evolving challenges posed by cybercrime and technology-enabled financial crime.

The role of technology in enabling financial crime at all levels has emerged as a primary theme in *Serious Financial Crime in Australia 2017*.

¹ Australian Federal Police 2017, *Serious Financial Crime Taskforce*, viewed 2 June 2017, <https://_www.afp.gov.au/what-we-do/crime-types/fraud/serious-financial-crime-taskforce>.

From opportunistic tax refund fraud undertaken by individuals to the large-scale online theft of personal identifying information to enable the systematic theft of funds from investment and superannuation accounts, the use of technology enables an extensive spectrum of financial crime. This has implications for the development of systems, processes and procedures to deter and protect against technology-enabled crime, and for forward planning for the capabilities and specialist resources required to identify and investigate technology-enabled crime.

Professional facilitators remain critical enablers of financial crime, particularly serious and organised crime, with the range of professionals involved extending beyond the traditional legal and accounting facilitators to include liquidators, offshore service providers and real estate agents. This reflects the increasingly complex and globalised organised crime environment.

TACKLING SERIOUS FINANCIAL CRIME

Identifying and targeting serious financial crime remains a priority of the Australian Government, which has established a number of key initiatives aimed at addressing serious financial crime threats and reducing the impact of serious financial crime on Australians.

The high-profile financial crime initiative Project Wickenby was established in February 2006 and operated until 30 June 2015, targeting international tax evasion and those professional facilitators who promoted or participated in the abuse of offshore secrecy arrangements to support large-scale tax evasion. As at 30 June 2015, Project Wickenby had resulted in the conviction of 46 individuals, \$2.297 billion in tax liabilities raised, \$372 million from increased voluntary compliance and \$5 million in assets recovered under Commonwealth proceeds of crime provisions.

In addition to the success of Project Wickenby, the Australian Government has continued its commitment to tackling serious financial crime in Australia, by supporting a number of collaborative initiatives since 2011 that bring together government, private sector and regulatory stakeholders to target the key financial crime threats to Australia.

CRIMINAL ASSETS CONFISCATION TASKFORCE

The AFP-led Criminal Assets Confiscation Taskforce is a Commonwealth initiative, established in March 2011, which is dedicated to taking the profit out of crime by targeting criminals and their assets derived from unexplained wealth. The Criminal Assets Confiscation Taskforce brings together the resources of the AFP, ATO and ACIC, as an integrated approach to targeting the financial base of criminals and confiscating assets bought with proceeds of crime.

FRAUD AND ANTI-CORRUPTION CENTRE

In 2013, the AFP-led multi-agency Fraud and Anti-Corruption Centre was established to focus on serious and complex fraud against the Commonwealth, corruption by Australian Government employees, foreign bribery and complex identity crime involving the manufacture and abuse of official credentials.

The Serious Financial Crime Taskforce forms part of the Fraud and Anti-Corruption Centre and builds on the success of offshore tax evasion work carried out under Project Wickenby. The Serious Financial Crime Taskforce has a broader remit than the Fraud and Anti-Corruption Centre. It targets the highest priority serious financial crimes and focuses on operational activities, the collection and sharing of intelligence, the identification of potential reform measures with the aim of removing wealth derived from illegal activities, prosecuting facilitators and promoters of serious financial crime and the deployment of deterrent and preventative enforcement strategies.

TAX AVOIDANCE TASKFORCE—TRUSTS; FORMERLY TRUSTS TASKFORCE

In 2013, the ATO-led Trusts Taskforce was established to take compliance action against known tax scheme designers, promoters, individuals and businesses who have been involved in tax avoidance or evasion using trust structures. The Trusts Taskforce raised \$948 million in liabilities and collected \$279 million from individuals and businesses involved in tax avoidance or evasion using trusts. An additional \$55 million worth of assets have also been restrained under proceeds of crime legislation.

Since 1 July 2017, the work of the Trusts Taskforce has continued under the ATO's Tax Avoidance Taskforce - Trusts.

PHOENIX TASKFORCE

Established in 2014, the Phoenix Taskforce comprises of over 20 Federal, State and Territory government agencies providing a whole-of-government approach to combating illegal phoenix activity. The Phoenix Taskforce also works in collaboration with the Serious Financial Crime Taskforce to identify and treat serious financial crime related to illegal phoenix behaviour.

The Phoenix Taskforce aims to share data and intelligence to capture both phoenix companies and those potentially aiding businesses by providing unlawful insolvency advice.

In 2015–16, the Phoenix Taskforce conducted almost 1,000 audit and review cases involving phoenix behaviour, raising \$250 million in liabilities.

AUSTRALIAN CYBERCRIME ONLINE REPORTING NETWORK

Established in 2014, the Australian Cybercrime Online Reporting Network (ACORN) is the ACIC-led national policing initiative of the Commonwealth, state and territory governments that enables the public to securely report instances of cybercrime through a national online system. As well as facilitating the public's reporting of cybercrime events, ACORN helps the government to better understand the enablers of cybercrime so that it can educate members of the public to recognise common types of cybercrime. This increased understanding also informs response strategies that make Australian citizens less attractive for cybercriminals to target.

In the 2016–17 financial year, ACORN received 874 reports with a total estimated loss of more than \$20 million—a figure that is more than double the estimated loss of \$8.6 million reported to ACORN in the 2015–16 financial year.

AUSTRALIAN FINANCIAL CRIMES EXCHANGE

In November 2016, the AGD-led Australian Financial Crimes Exchange was launched, partnering the ANZ, the Commonwealth Bank, the National Australia Bank and Westpac with the Australian Government to provide leading security capabilities, technology and intelligence on a centralised platform. This platform allows financial institutions to share fraud and cybercrime-related data. This aims to improve responses to these types of financial crimes and reduce the impact on customers and shareholders.

FINTEL ALLIANCE

Launched in March 2017, the AUSTRAC-led Fintel Alliance is a public-private partnership aimed at combating money laundering and terrorism financing. The Fintel Alliance supports the real-time exchange of financial intelligence, data, tracking tools and methodologies on a global scale. The three operational goals of the Fintel Alliance are:

- to help private sector partners more easily identify and report suspicious transactions
- to help law enforcement partners more quickly arrest and prosecute criminals
- to work with academia to build knowledge and gather insight.

The United Kingdom's National Crime Agency is the first international member of the Fintel Alliance Operations Hub. With membership from Australian Government agencies, industry partners and international law enforcement, the Fintel Alliance aims to protect the integrity of Australia's financial systems from organised crime and terrorism financiers impacting on Australia.

BLACK ECONOMY TASKFORCE

In 2017, the Australian Government established the Black Economy Taskforce, a policy response initiative to examine the practices of those who operate entirely outside the tax and regulatory system or who do not correctly report tax obligations.

Cash businesses present a variety of opportunities to launder money, including through:

- illicit funds being mingled with legitimate business earnings
- illicit funds being used to purchase stock, equipment and premises which in turn can increase the resale value of that business
- false sales records being created to inflate business turnover, which allows for the injection of illicit funds.

GENERATING FINANCIAL CRIME INTELLIGENCE

It is difficult to quantify the annual loss of funds to financial crime committed by serious and organised crime groups and criminal individuals or the real sum lost to the Commonwealth and victims through various forms of fraud. However, what does seem apparent is that both of these financial crime impacts present important risks to Australia.

Through the work programs of these various financial crime initiatives, it is expected that a more comprehensive intelligence picture of the impact of serious financial crime on the Australian community and the disruption effects of public-private collaboration and interactive targeting efforts will be generated.

Serious Financial Crime in Australia 2017 focuses on the 'enablers' and 'markets' of financial crime.

Enablers play a unique role in enabling or facilitating serious and organised financial crime. There are some criminal groups and individuals who specialise in one or more of these enabling activities, providing services to other individuals and groups engaged in serious financial crime.

For example, a specialised money laundering syndicate would provide a money laundering service to a group involved in organised fraud, enabling that group to move the proceeds of their fraud activities offshore. Each of the enablers can facilitate financial crime to varying extents; however, some enablers have a more fundamental role than others. Enablers can work in unison, with one crime group using several enablers concurrently.

Financial crime markets represent those markets where the participants exchange goods or services, but those goods or services are delivered or presented in an illegal, malicious or fraudulent manner. For example, criminal groups and individuals seeking to defraud the government of income tax or health and welfare benefits would misrepresent their position in order to gain additional benefits they are not entitled to or evade paying tax. Therefore, revenue and taxation fraud and health and welfare fraud are regarded as financial crimes where criminals are 'market participants' in the tax system or government programs. The financial crime markets addressed in this report reflect the highest priority markets, where the impact on Australians and the Australian economy is the most significant.



**FINANCIAL CRIMES ARE
DIVERSE IN NATURE,
SCALE AND THE LEVEL
OF HARM THEY CAUSE**