

# UNCLASSIFIED

## Australian Federal Police Submission

### Inquiry into Serious and Organised Financial Related Crime

May 2014

#### INTRODUCTION

1. The Australian Federal Police (AFP) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement's (PJCLE) inquiry into serious and organised financial related crime.
2. The AFP enforces Commonwealth criminal law and protects Commonwealth and national interests from crime in Australia and overseas, including prevention, deterrence and disruption of financial crime.
3. Financial related crime poses a significant and growing threat to Australia's national security as it subverts, exploits and distorts legitimate markets and economic activity. This crime type also undermines the ongoing stability of Australian institutions and Governments by having a corrosive impact on community confidence.
4. The AFP has endeavoured to address the ToR in a holistic manner throughout the submission rather than address each ToR individually.
5. This submission is designed to assist the Committee by providing:
  - Background to the threat of financial crime and its environment (Part 1).
  - Information on the AFP's national approach to serious and organised financial crime (Part 2).
  - An overview of financial crime offences and their legislative background (Part 3).
6. For the purposes of the submission, serious and organised financial crime includes money laundering, identity crime, serious and complex fraud and corruption. Specific terminology is used within the submission to describe the following issues:
  - *Financial related crime* is defined broadly by the International Monetary Fund as 'any non-violent crime resulting in financial loss'.<sup>1</sup>
  - *Identity crime* is broadly used to describe activities and offences in which a perpetrator uses a fabricated identity; a manipulated identity; or a stolen/assumed identity to facilitate the commission of a crime.<sup>2</sup>
    - *Identity theft* most often involves the theft or misappropriation of personal identity information and related financial information.

---

1 International Monetary Fund 2011, 'Financial System Abuse: Financial Related Crime and Money Laundering - Background Paper', International Monetary Fund: Washington DC

2 Australasian Centre for Policing Research 2006, 'Standardisation of definitions of identity crime terms: a step towards consistency', <<http://www.anzpaa.org.au/anzpire/acpr-publications>>

UNCLASSIFIED

## UNCLASSIFIED

- *Identity fraud* involves an assumption of another identity for fraudulent purposes and the production of false identities and financial documents to commit crimes.
- For the purposes of this submission, the AFP will refer to identity theft and identity fraud under the broader term 'identity crime'.<sup>3</sup>
- *Money Laundering* is the process of converting cash or other property derived from criminal activity to give it the appearance of having been obtained from a legitimate source.
- For the purpose of the Commonwealth Fraud Control Guidelines, *fraud against the Commonwealth* is defined as 'dishonestly obtaining a benefit, or causing a loss, by deception or other means'.

Fraud against the Commonwealth may include (but is not limited to):

- theft,
  - accounting fraud (false invoices, misappropriation etc.),
  - unlawful use of, or obtaining property, equipment, material or services,
  - causing a loss, or avoiding and/or creating a liability,
  - providing false or misleading information to the Commonwealth, or failing to provide it when there is an obligation to do so,
  - misuse of Commonwealth assets, equipment or facilities,
  - making, or using false, forged or falsified documents, and
  - wrongfully using Commonwealth information or intellectual property.
- While 'corruption' is not specifically defined in the Commonwealth Fraud Control Guidelines 2011, for the purposes of this submission *corruption or corrupt conduct* can be defined as:
    - conduct that involves a Commonwealth Officer abusing his or her office; or
    - conduct that perverts the course of justice; or
    - conduct that, having regard to the duties and powers of the Commonwealth Officer, involves corruption of any other kind.<sup>4</sup>

The AFP also considers that conduct committed by individuals or businesses that causes or attempts to cause Commonwealth Officers or foreign public officials to engage in corrupt conduct is also captured within the meaning of corruption.

---

<sup>3</sup> S Payneham 2006, 'Standardisation of definitions of identity crime terms : a step towards consistency', Prepared by The Australasian Centre for Policing Research (ACPR) (for the Police Commissioners' Australasian Identity Crime Working Party ; and The Australian Transaction Reports and Analysis Centre (AUSTRAC) Proof of Identity Steering Committee', report no 145.3

<sup>4</sup> s6(1) of the Law Enforcement Integrity Commissioner Act 2006 (Cth)

## UNCLASSIFIED

### THE FINANCIAL RELATED CRIME ENVIRONMENT IN AUSTRALIA

7. Financial related crime poses a significant and growing threat to Australia's national security as it subverts, exploits and distorts legitimate markets and economic activity. The corrosive impact on community confidence caused by financial related crime also undermines the ongoing stability of Australia's institutions and governments.
8. Criminals who commit financial related crimes are becoming increasingly sophisticated and entrepreneurial in nature. Organised crime groups (OCGs) are increasingly using legitimate businesses to exploit lawful commerce and economic activity. This presents unique challenges for law enforcement as it increasingly blurs the lines between legitimate and illegitimate transactions. Given the nature of financial crime, there has been widespread recognition that combatting the threat requires a unified and coordinated approach.
9. The Commonwealth Organised Crime Strategic Framework was launched by the then Attorney-General in November 2009, with a view to providing Commonwealth Agencies with a single unified strategic policy direction, as well as promoting a more integrated and collaborative approach to combating organised crime. This Framework characterised organised crime as an issue of national security for the first time.
10. The key elements of the Framework included:
  - An Organised Crime Threat Assessment to provide a shared picture among relevant stakeholders of the most significant threats and harms arising from organised criminal activity, and
  - An Organised Crime Response Plan (OCRP) to align Commonwealth efforts to respond to identified and emerging organised crime threats.

#### **Fraud**

11. Fraud against the Commonwealth is a serious matter for all Australian Government departments and agencies, and for the community. The Australian Institute of Criminology (AIC) estimates that fraud costs the Australian economy billions of dollars each year. Fraud against the Commonwealth may be committed by private citizens (external fraud) and/or by Commonwealth employees (internal fraud), including staff and contractors. Government agencies that handle large sums of public money such as taxation revenue and welfare payments are particularly affected. They are also at risk of public servants and contractors exploiting security weaknesses in systems to obtain financial advantage dishonestly. Fraud risks also arise in connection with implementing new, large-scale government programs. The incidence and financial impact of internal fraud is generally lower than external fraud, although both deplete government resources and have a negative impact on the administration of agencies.

## UNCLASSIFIED

12. Pursuant to the Commonwealth Fraud Control Guidelines 2002, the AIC produces a report on fraud experienced by Australian Government agencies and the fraud control arrangements they use to minimise the risk of fraud. According to the Fraud against the Commonwealth 2009–10 annual report to government, the 152 Australian Government agencies surveyed reported experiencing almost 706,000 incidents of fraud (internal and external) worth almost \$498m during 2009-10.<sup>5</sup>
13. Investment fraud also presents a significant threat to the Australian financial sector, with a direct and damaging impact to individuals.
14. It is estimated that current total assets in the Australian superannuation system are in the vicinity of \$1.6 trillion. The asset pool is projected to grow to \$4 trillion in the next 10 years and \$7.6 trillion by 2033.<sup>6</sup>
15. Investment fraud is not an opportunistic crime, but in fact a calculated, sophisticated, organised criminal event. This criminal activity is typically, partly or wholly conducted offshore and involves foreign registered companies outside the reach of the Australian jurisdiction. These factors highlight why law enforcement agencies and regulatory agencies globally face difficulties with investment fraud prevention, detection, disruption and prosecution.
16. In 2012 a parliamentary inquiry into the largest superannuation fraud in Australia's history—Trio Capital—found the case exposed the significant vulnerabilities within the superannuation system.
17. In April 2013 the former Minister for Financial Services and Superannuation released the Government's response to the report by the Parliamentary Joint Committee on Corporations and Financial Services on the collapse of Trio Capital (the Trio Report) as well as the report by Mr Richard St. John on Compensation arrangements for consumers of financial services.
18. The Government accepted the vast majority of the report's recommendations including:
  - a. legislative changes to strengthen the professional indemnity insurance requirements of providers of financial services that deal with retail consumers,
  - b. changes to improve the communication of risks to investors and to ensure the adequacy of regulatory processes and consultation papers by Treasury on powers to support ASIC in its enforcement role, and
  - c. Improvements to the governance arrangements of managed investment schemes.

---

<sup>5</sup> Australian Institute of Criminology 2013, 'Fraud against the Commonwealth 2009–10 annual report to government', <[http://www.aic.gov.au/media\\_library/publications/mr/18/mr18.pdf](http://www.aic.gov.au/media_library/publications/mr/18/mr18.pdf)>

<sup>6</sup> September 2013 Deloitte report: The Dynamics of the Australian Superannuation System – the next 20 years – 2013-2033

## UNCLASSIFIED

19. Currently, superannuation fraud is addressed through a range of legislation administered by ASIC (corporations law), APRA (superannuation law) and ATO (taxation law, self-managed superannuation funds). The treatment options are primarily regulatory in nature (civil penalty provisions, taxation) with the option of taking criminal enforcement action in particular cases. The AFP's role in relation to superannuation fraud is limited to providing support to the lead agencies.
20. Breaches of the Superannuation Industry (Supervision) Act 2003 can be dealt with as criminal matters where there is an additional element of dishonesty/fraud, but only carry a maximum penalty of 5 years imprisonment. Under the Corporations Act 2001 penalties for offences generally range from low fines to up to five years imprisonment. In the financial services context (which includes certain superannuation entities) there are higher penalties for market misconduct and insider trading (10 years imprisonment).
21. Given the risk and the potential involvement of serious and organised crime in superannuation fraud, the Committee may wish to consider whether additional treatment options – such as the introduction of specific, serious offences to be enforced by the AFP – could be added to complement the current approach. Any expansion of the AFP's role in this area, and the need for legislative reform (for example to the Criminal Code) would need to be carefully considered in consultation with AGD and Treasury (and their portfolio agencies).

### Identity Crime

22. Identity crime is often linked to other forms of criminality such as illicit commodity movements, money laundering, fraud against the Commonwealth, people smuggling, and human trafficking. Identity information is stolen by a range of methods including phishing, hacking and malware. The organised theft and sale of stolen identity information is usually for the purposes of manufacturing fraudulent identity documents. In Australia, these documents are typically credit cards, driver licences, Medicare cards and other documentation, which are then used to support subsequent criminal activity.
23. The extent and impact of identity crime in Australia remains difficult to establish definitively. The Australian Bureau of Statistics Personal Fraud Survey for 2010-11 estimated over 700,000 Australians were victims of identity fraud and over 44,000 Australians were the victims of identity theft.
24. Identity crime offences are not usually subject to AFP investigations in isolation. Instead, these offences are considered as part of a wider investigation into other crime types, as identity crime is a key enabler of crime. As a result, the number of AFP investigations categorised as relating to identity crime can appear minimal and not accurately reflect the true extent of the AFP's work in this area.

## UNCLASSIFIED

### **Money Laundering**

25. Money laundering is the process by which proceeds from criminal and illicit activity are disguised to conceal their true origins. Its use incites further criminal activity by allowing OCGs to accumulate wealth, avoid detection and prosecution. Criminals engage in money laundering for three main reasons: to further the interests of the criminal activity by covering operating expenses; to hide the source of their wealth to avoid prosecution; and to shield illicit profits from suspicion and subsequent seizure by law enforcement agencies.

## UNCLASSIFIED

### Financial Crime – Impact of New Technologies

26. Serious and organised criminal activity can cut across a broad spectrum of society and varies from crude to highly sophisticated methods. This may include simple theft of personal information or complex attempts to manipulate stock markets or launder the proceeds of crime. Globalisation and technological advancements have had a significant impact on how financial transactions and business is undertaken.
27. New technologies are enabling OCGs to expand their reach using deception, extortion and social engineering to commit traditional crimes. Rapid advancements in technology are also enabling OCGs to employ sophisticated methods including cybercrime to facilitate their illicit activities. Cybercrime that is undertaken for financial gain is a significant issue for Australia as it is complex, multi-jurisdictional and is generally considered an enabler for financial crime.
28. The Australia and New Zealand Police Advisory Agency (ANZPAA) Protocol on Cybercrime Operations defines cybercrime as:
- Crime directed at computing and communications technologies themselves, such as unauthorised access to, modification or impairment of electronic communications data, and/or
  - Crime where the use of the internet or information technology is integral to the commission of the offence (sometimes referred to as technology-enabled crime), such as online fraud (e.g. internet or email scams), online identity crime, online child exploitation and online intellectual property infringement.
29. Traditionally, the vast majority of cybercrimes have been perpetrated by those wishing to gain fame and/or notoriety by attacking and disabling the computer systems of their victims. These crimes rarely involved a monetary gain or financial aspect (other than the cost of damages incurred). With the exponential growth of the internet over the past 15 years, including a growth in e-commerce and business, this is no longer the case. The majority of cybercrimes are now perpetrated by OCGs with a very clear financial motive.
30. The rise in popularity of crypto/digital currencies such as Bitcoin is already used by criminals to further anonymise their identity when conducting transactions online. Additionally, as there is no governance for these types of currencies, they may be seen as an attractive method to launder proceeds of crime or hide legitimate sources of money in an attempt to avoid paying tax. For example, in Australia, the use of these currencies may circumvent Australian Transaction Reports and Analysis Centre (AUSTRAC) reporting requirements regarding the movement of monies into, and out of, Australia.

## UNCLASSIFIED

### AFP Response

31. The AFP Cyber Crime Operations (CCO) teams are comprised of investigators and technical experts dedicated to preventing, mitigating, disrupting, investigating and prosecuting cybercrime. The AFP CCO teams investigate significant computer intrusion offences, collaborating closely with government, public and private sectors to protect the security and stability of Australia's critical systems.
32. As an active partner in the Cyber Security Operations Centre, the AFP continues to implement intelligence-led policing methodologies to identify and mitigate cyber security events through enhanced intelligence-sharing opportunities. The AFP also provides the national law enforcement investigative capability for the Government's Cyber Security Strategy.



## UNCLASSIFIED

### THE ROLE OF THE AFP IN DETECTING, DISRUPTING AND PROSECUTING FINANCIAL RELATED CRIME

33. A key objective for the AFP is to remove the profit from crime and prevent its reinvestment in further criminal activity. This is achieved through the targeting of the financial base of OCGs through anti-money laundering mechanisms and proceeds of crime investigations. In this space, the AFP often works collaboratively through multi-agency taskforces such as the Criminal Assets Confiscation Taskforce (CACT). Taskforces such as these are increasingly playing a key role at the national level in the investigation and prosecution of financial crime matters.

#### **Partnerships**

34. The AFP routinely works in coordination with other agencies to achieve a whole of government approach in the detection, disruption and prosecution of serious and organised financial related crime impacting on the Commonwealth. In order for Australia to combat the ongoing and future effects of serious and organised financial crime it remains paramount that international, Commonwealth, state and territory and industry partnerships are collaborative and flexible.

35. While cooperation across Commonwealth agencies remains effective, the AFP continues to work with partners to identify ways to enhance existing activities. Illustrative of this effort, in March 2013 the AFP and ATO were tasked by the Heads of Commonwealth Law Enforcement Agencies (HOCOLEA) to develop options for cooperative models - based on Project Wickenby - that can respond flexibly to threats from serious and organised crime impacting on the Commonwealth.

36. In accordance with the HOCOLEA task, and with the cessation of Project Wickenby funding in June 2015, the AFP, ATO and Australian Crime Commission (ACC) are working together to identify cooperative multi-agency approaches, within existing resources and frameworks, to enhance the Commonwealth's ability to respond to specific instances of high priority financial crime in a more coordinated and effective manner.

37. The AFP also has strong relationships with state and territory jurisdictions and Australia's industry sector as well as 48 cooperation agreements with foreign law enforcement agencies. The majority of these agreements relate to combating transnational crime, including people smuggling and terrorism, and developing law enforcement cooperation to achieve greater operational outcomes. Many of these agreements have been developed to establish a basic framework of cooperation between the participants in preventing and combating transnational organised crime.

38. These agreements are integral to helping the AFP drive investigations and support bilateral or multi-lateral cooperation; assist with the collection and exchange of criminal intelligence in support of international law enforcement effort; and enhance the

## UNCLASSIFIED

capacity and capability of international law enforcement agencies to combat transnational organised crime. Most of the AFP's international agreements include collaboration and engagement with international partners through the AFP's International Network.

39. Unique industry partnerships contribute to the AFP's ability to prevent and disrupt crime, as well as foster innovation and technological solutions to the benefit of both industry and law enforcement. The Commonwealth Organised Crime Strategic Framework, the OCRP and the National Organised Crime Response Plan have all recognised the importance of government and industry partnerships in combatting serious and organised crime.

### **Fraud and Corruption**

40. Overseas experiences indicate increasingly concerning trends in fraud and corruption, including the likelihood of the underreporting of matters. Ultimately, this may have significant commensurate impacts on market and public confidence, international reputation, and the loss of public monies. In accordance with Australia's multi-agency approach to combating corruption, a number of Australian Government agencies play a role in combating corruption through promoting accountability, transparency and effective enforcement.
41. The AFP has primary law enforcement responsibility for investigating serious or complex fraud and corruption against the Commonwealth. The AFP is proactively seeking to address global fraud and corruption issues through bolstering efforts on the detection of, and investigation into, these multi-dimensional crimes through increased intelligence, inter-agency liaison, and investigator training.
42. The AFP established the Fraud and Anti-Corruption (FAC) business area in February 2013. FAC enhances the AFP response to serious and complex fraud against the Commonwealth, corruption, foreign bribery and complex identity crime involving the manufacture and abuse of credentials. The FAC has dedicated investigative teams in Canberra, Sydney, Brisbane, Melbourne and Adelaide, as well as an Identity Security Strike Team (ISST) based in Sydney. Further, the AFP can also access additional investigative resources nationwide on an as-required basis, including teams in Perth, Darwin, Hobart and Cairns.
43. Through the FAC business area, the AFP works closely with partner agencies using a multi-agency approach to strengthening the Commonwealth's capacity and response to fraud and corruption law enforcement.
44. This multi-agency approach contributes to the reduction or cessation of activities beyond those targeted by a particular investigation, which results in increased compliance with Commonwealth legislation and provides enhanced revenue and expenditure outcomes for the Commonwealth.

## UNCLASSIFIED

45. Complex fraud and corruption matters are generally protracted, requiring specialised skills and significant resources. The committed FAC teams provide a robust framework to build inter-departmental and industry engagement.
46. Currently, Commonwealth agencies must refer all instances of potential serious or complex fraud offences (including potential corruption of Commonwealth Officials) to the AFP in accordance with the Commonwealth Fraud Control Guidelines, Australian Government Investigation Standards and the AFP referral process except where:
- legislation sets out requirements for referrals of a particular nature or by a particular class of bodies or agencies, such as to the Australian Commission for Law Enforcement Integrity (ACLEI); or
  - where agencies have the capacity and the appropriate skills and resources needed to investigate criminal matters and meet the requirements of the AFP and the Commonwealth Director of Public Prosecutions in gathering evidence and preparing briefs of evidence.
47. The FAC works closely with AFP's partner agencies throughout these investigations and has recently established a FAC Centre within the AFP's national headquarters to facilitate closer working relationships through improved access to the specialised advice and resources available across agencies, increased information and intelligence sharing opportunities and the delivery of whole-of-government investigations training.
48. The FAC also provides a coordination function for the operational activities of relevant AFP out-posted agents within key partner agencies. These initiatives enable the AFP to work with and inform partner agencies to also explore alternative treatments other than protracted investigations, such as prevention and disruption strategies.

### Identity Crime

49. The FAC business area is also responsible for the prevention, disruption and investigation of identity offences that relate primarily to illicit possession, brokering, manufacture or theft of identity material. The FAC incorporates the ISST in Sydney, which investigates identity crimes in partnership with the New South Wales Police Force and with the assistance of the Department of Immigration and Border Protection (DIBP) and the NSW Roads and Maritime Service.
50. The ISST targets the syndicated manufacture, distribution and use of fraudulent identity documents, as well as the compromise of personal information by OCGs. The primary manifestations of identity crime, being use of fraudulent credit cards and driver licences, are typically investigated by state and territory law enforcement.
51. Where identity crime offences are detected against the Commonwealth, such as passport crime and visa fraud, the responsibility for the investigation of these offences

## UNCLASSIFIED

falls primarily to other Commonwealth agencies such as the Department of Foreign Affairs and Trade and DIBP.

52. The FAC also works closely with the Attorney-General's Identity Security Policy section to provide input to the ongoing development of Australian policy in this area. The ISST also engages with international partners as required through the AFP's International Network.

## UNCLASSIFIED

### Identity Crime Strategies

#### *National Identity Security Strategy*

53. The AFP is part of the Commonwealth Reference Group on Identity Security and continues to support the development and implementation of the identity crime measurements framework as outlined by the 2012 National Identity Security Strategy (NISS).
54. The NISS aims to develop the conditions required so that Australians may confidently enjoy the benefits of a secure and protected identity. The scope of the NISS is shaped by the need to strengthen national security, prevent crime and enable the benefits of the digital economy. Commonwealth, state and territory Governments are working together to enhance national consistency, interoperability and opportunities (including for government service delivery) through nationally consistent processes for enrolling, securing, verifying and authenticating identities and identity credentials.<sup>7</sup>
55. Through close collaboration with partner agencies and the Attorney General's Department, the AFP continues to support and contribute to the implementation of the NISS.

#### *Australian Identity Crime Policing Strategy 2011-2014*

56. In 2011 the AFP took the lead in the development of the Australian Identity Crime Policing Strategy 2011-2014 (the Strategy) after agreement was reached by all jurisdictions at the ANZPAA Crime Forum. Consultation was undertaken with the heads of jurisdictional police fraud departments, as well as with Commonwealth agencies including the Attorney-General's Department, the Australian Transaction Reports and Analysis Centre (AUSTRAC), ACC, and the Department of Foreign Affairs and Trade. The Strategy was endorsed by the ANZPAA Board in October 2012.
57. The Strategy directly supports both the objectives of the NISS and the Organised Crime Strategic Framework, as well as contributing to the Government's law enforcement, integrity and crime prevention outcomes. The Strategy aims to facilitate a cooperative and collegiate approach to the prevention, investigation and reduction of identity crime by Australian law enforcement agencies, ensuring the provision of assistance to the victims of identity crime.

---

<sup>7</sup> Attorney-General's Department 2013, 'National Identity Security Strategy',

<<http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/National%20Identity%20Security%20Strategy%202012.PDF>>

## UNCLASSIFIED

### Identity Crime Case Studies

58. AFP Operations LINO, SAXTON, PULSE and ZULU demonstrate how OCGs can attack both individuals and the public and private sectors to steal large sums of money from the Australian community.

#### Operation LINO

Operation LINO focused upon a series of breaches of independent retail stores' Electronic Funds Transfer Point of Sale (EFTPOS) terminals, each of which possessed a common vulnerability (this vulnerability was present across a large spectrum of the market). The purpose of the breach was to collect and steal credit card credentials which had been used to make purchases at the individual businesses. The perpetrators of the crime conservatively cost the credit card issuers in excess of AU\$30m (based on banking industry figures). The overall exposure of the financial sector was in the vicinity of AU\$1bn.

The AFP investigation exposed vulnerabilities in both the banking infrastructure which facilitated the use of credit cards at the merchant (including the EFTPOS terminals), in addition to the computer systems of the individual merchants that were affected.

In this case, the OCG which perpetrated the intrusions and sale of the credit card data was based in Romania, and the AFP worked closely with the Romanian National Police to affect the arrest and prosecution of the groups' members.

#### Operation SAXTON

The SAXTON investigation focused on a malware campaign whereby individuals who made use of online banking services had malware installed on their personal computers by an eastern European OCG. This resulted in their banking credentials being stolen and later used to conduct unauthorised transactions on their accounts. These unauthorised transactions took the form of transfers of monies to the accounts of a third party (who are often unaware of the genuine source of the funds) who then removed the stolen funds from the banking system and sent them to the offshore cybercrime group.

Despite a total Australian exposure of approximately AU\$580m (based on banking industry estimates), detection and early intervention by the AFP mitigated the extent of loss with an actual industry loss of AU\$1.5m.

Operation LINO and Operation SAXTON demonstrate how attacks of this scale can have a major impact on the national economy and public confidence in the digital economy and highlight the covert and adaptive nature of organised crime. In a number of cases, the first time the victims or financial institutions become aware of illegal financial transactions are when the AFP approaches them, having detected the original intrusions through regular investigations.

AFP Operations LINO and SAXTON successfully identified and prevented access to an estimated \$1.5 billion of potential fraudulent activity against the Australian financial sector.

## UNCLASSIFIED

### Operation PULSE

Operation PULSE was an ISST investigation into the manufacture and distribution of fraudulent identity documents by criminal networks operating domestically and internationally. Investigations identified offenders engaging in supplying materials used to manufacture false identity documents, creating and distributing documents, and coordinating subsequent criminal use.

Stolen identity information is believed to have been skimmed or intercepted from a range of sources, including intercepted commercial transactions and from compromised taxi services. Stolen data was then provided to syndicates operating within Australia via SMS, and loaded onto blank card stock sourced primarily from China. Within 24 hours, Australian-based syndicates produced fraudulent identity bundles containing credit cards, driver licences', and Medicare card which were distributed to 'shoppers'. Fraudulent credit cards were then used to purchase small, high-value items for on-sale, with other documents 'legitimising' the name appearing on the card. The syndicate then laundered proceeds offshore.

To date Operation PULSE has resulted in several arrests, the seizure of over 15 000 false credit cards, and a restraint in excess of AUD\$1.1 million in assets. Several persons of interest identified during the investigation have been convicted of previous identity crime offences, suggesting the criminal perceived financial benefit outweighs deterrent measures.

### Operation ZULU

In 2010 the AFP received a referral to investigate the theft and use of stolen identity information for the purpose of defrauding the ATO and other Commonwealth agencies. Investigations revealed that since at least 2005, two primary offenders had acquired identity information through means including break-and-enters of business premises in Queensland and South Australia, and advertising bogus employment opportunities to elicit tax files numbers and other details. This resulted in the theft of over 370 victims' details used to create fraudulent identity documents, utility records and other supporting documents.

These documents were used to establish 85 'front' companies and sole trader businesses, which were then used to defraud the ATO of Goods and Services Tax refunds and individual tax returns. Compromised tax file numbers were also used to complete fraudulent superannuation claims. After extended multi-agency investigations, in mid-2013 both primary offenders in Operation ZULU were sentenced to six year and five year imprisonment respectively.

## UNCLASSIFIED

### Money Laundering

59. Targeting the criminal economy is crucial to understanding organised criminal activity and developing strategies to disrupt it. A key objective of the AFP is to remove the profit from crime and prevent its reinvestment in further criminal activity. Through the CACT, Project Wickenby, and a money laundering strategy involving the Money Laundering Short Term Teams (MLSTT), Operations ZANELLA and ELIGO, the AFP has enhanced its focus on following the money.

60. It is commonly held that there are three steps in the money laundering process:

- *Placement* – locating the proceeds of crime in a legitimate context and away from direct association with the crime;
- *Layering* – disguising the true origins and ownership through a series of transactions; and
- *Integration* – incorporating the proceeds of crime into the legitimate economy by investing in lawful activities.<sup>8</sup>

61. Some commonly used money laundering strategies include moving money and creating complex money trails, breaking up large amounts of cash and depositing smaller sums in different bank accounts, and trade-based money laundering.

62. In Australia and around the globe, criminal entities are becoming increasingly determined to evade law enforcement efforts by using sophisticated techniques to launder money through the Australian and international economy. Typically these techniques involve the use of the regulated finance sector and through the use of identity crime to deposit and transfer funds domestically and internationally. OCGs may also seek the assistance of professional advisors. Globalisation and the integration of capital and technology across borders enables criminals to launder their criminal proceeds faster, farther and cheaper than ever before.

#### *Money Laundering Short Term Teams*

63. The assessment and analysis of money laundering activity is now a major component of any AFP investigation and the AFP has dedicated money laundering investigation teams in Sydney and Melbourne to proactively target syndicates involved in laundering illicit funds on behalf of organised crime.

64. The money laundering investigation teams work with partner agencies, including the ACC, ATO and AUSTRAC to gain an understanding of the operations of money laundering syndicates. Results from money laundering operations for the 2012–13 reporting period include cash seizures of approximately \$14.7 million and money laundering offence charges against 25 persons.

---

<sup>8</sup> A Goldsmith 2012, 'Crimes Across Border', in Marmo, de Lint, Palmer, Crime and Justice: A Guide to Criminology, 3rd ed, ch 13.



## UNCLASSIFIED

### Operation ZANELLA

Under Operation ZANELLA, the AFP works closely with domestic and international partners to actively target transnational money laundering networks that provide remittance services to transnational OCGs impacting Australia. The targeting work of this operation has identified significant predicate offending, in particular narcotic importations.

In the last 12 months, Operation ZANELLA activity has led to the arrest of seven persons for drug and money laundering offences and the seizure of approximately \$2 million, 5000 Euro, 716kg cocaine, 1kg cannabis, a false passport and jewellery with an approximate value of \$150,000 AUD.

### Operation ELIGO

The ELIGO National Task Force was established in 2012 as an ACC led special investigation into the use and exploitation of alternative remittance and informal value transfer systems by serious and organised crime groups.

As at January 2014, the Task Force had seized more than \$580 million worth of drugs and assets, including \$26 million in cash.

The MLSTTs work closely with both Operation ZANELLA and Operation ELIGO in targeting money laundering activity.

### Criminal Assets Confiscation Taskforce (CACT)

65. The AFP also plays a key role in the investigation and prosecution of proceeds of crime matters through the CACT. This further demonstrates the AFP's commitment to removing the incentive and reward for serious and organised crime in Australia.
66. The CACT is an AFP-led, multi-agency taskforce with primary responsibility for the investigation and litigation of Commonwealth proceeds of crime matters. It aims to enhance the identification and pursuit of criminal wealth where there is a link to a Commonwealth offence.
67. A key focus of the CACT is to maximise the impact of law enforcement resources by targeting the unexplained wealth and identified proceeds of crime from domestic and transnational criminal enterprises, with the combined efforts of investigation and litigation undertaken by the AFP. The CACT also works in partnership with other relevant law enforcement and regulatory agencies in order to identify, investigate, and litigate appropriate asset confiscation matters at the Commonwealth level.
68. A wide variety of assets have been subject to Commonwealth confiscation action in recent years including, but not limited to: cash, real estate and commercial property, share portfolios, luxury cars, jewellery, motorcycles, light planes, jet-skis, sail and motor boats, artwork and other collectibles. In the current financial year (2013/14), the CACT has restrained more than \$120 million.

## UNCLASSIFIED

### **Project Wickenby**

Project Wickenby is an ongoing joint taskforce led by the ATO, which brings together resources from the AFP, ACC, the Australian Securities and Investments Commission, AUSTRAC and the CDPP.

The Project Wickenby cross-agency taskforce was formally established in 2006 to tackle the abusive use of secrecy jurisdictions which pose a serious threat to the integrity of Australia's financial, taxation, regulatory and criminal law systems. ;'

The AFP has conducted 17 investigations in support of Project Wickenby. As at 31 March 2014, the AFP had laid charges against 55 people, and the ACC had charged 18 individuals as a result of these investigations. Of those charged by the AFP, 47 people have been committed for trial, and 44 individuals have been convicted of indictable offences. Many of the offences targeted by the Project Wickenby taskforce relate to serious fraud, money laundering and defrauding the Commonwealth.

There have been a number of significant achievements as part of Project Wickenby, including the dismantling of a \$63 million tax evasion and money laundering scheme in 2012. This is the largest tax fraud investigation since Project Wickenby was launched, and was an outcome of a seven month joint investigation between the AFP and the ATO.

The ATO, as lead agency, has primary carriage of reporting to Government on Project Wickenby's overall progress. The AFP understands that the ATO will address Project Wickenby more comprehensively in their submission to the Committee.

## UNCLASSIFIED

### LEGISLATIVE FRAMEWORK

69. The AFP has primary responsibility for investigating offences against the *Criminal Code Act 1995 (Cth)*. The Criminal Code sets out offences that relate to money laundering, identity crime, financial information, as well as offences against the proper administration of the Government including fraud and corruption.
70. The AFP continues to work with partner agencies on legislative reform for issues such as Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF), proceeds of crime and unexplained wealth. Specifically, the AFP is currently contributing to the AGD led statutory review of the AML/CTF Act 2006, including making a submission to the Inquiry into this matter.
71. Further, the Financial Action Taskforce (FATF) is currently conducting a review of Australia's AML/CTF regime, which will consist of an evaluation of Australia's technical and effective compliance with international obligations and the FATF Standards. As part of this, the AFP will provide input to the FATF mutual evaluation. FATF's Report is expected to be completed by February 2015, with any recommendations considered in the statutory review of the AML/CTF Act.
72. The following outlines the key Commonwealth legislation relating to financial crime investigated by the AFP.

#### **Offences against the proper administration of the Government**

73. There are a range of financial-related offences contained in Chapter 7 of the Criminal Code. In particular, these offences criminalise fraudulent conduct committed against the Commonwealth (Part 7.3), making false or misleading statements (in applications to Government) or giving false or misleading information to Commonwealth officials (Part 7.4), bribery of Commonwealth officials (Part 7.6) and forgery in relation to dealing with the Government (Part 7.7).
74. These offences were inserted into the Criminal Code in 2000 by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000 (Cth)*.

#### *Fraudulent conduct*

75. Section 135.1 contains four offences: dishonestly obtaining a gain from the Commonwealth; dishonestly causing an intentional loss to the Commonwealth or being reckless as to causing that loss; and dishonestly influencing a Commonwealth official. All of these offences carry a maximum penalty of five years imprisonment.
76. Section 135.4 contains four offences relating to conspiracy to defraud the Commonwealth. These offences cover conspiring with another to dishonestly: obtain a gain from the Commonwealth, intentionally or recklessly cause a loss to the Commonwealth, or influence a Commonwealth official. All of these offences carry a maximum penalty of 10 years imprisonment.

## UNCLASSIFIED

### Identity crime offences

77. Specifically Commonwealth offences relating to identity crime are set out in Part 9.5 of the Criminal Code. These offences were implemented as part of the Model Criminal Law Officers' project and complement state and territory offences.
78. Commonwealth identity crime offences and a regime of identity crime victim support measures were introduced in 2011 through the *Law and Justice (Identity Crimes and Other Measures) Act 2011 (Cth)*. These offences (contained in Division 372 of the Criminal Code) are directed at dealing in identification information, possessing identification information and possessing equipment to make identification documentation.
79. In 2012, the *Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Act 2012 (Cth)* expanded the existing offences to capture the use of identity information to commit foreign indictable crimes (in addition to indictable Commonwealth offences), and created a new offence of using a carriage service (such as the Internet or mobile phone) to obtain and/or deal in identification information where a person intends to commit, or facilitate the commission of, a Commonwealth, state, territory or foreign indictable offence. These amendments were directed at ensuring that the Commonwealth's laws could address the transnational and multi-jurisdictional nature of identity crime (to the extent permitted by the Constitutional limitations on the Commonwealth legislative power).
80. All of the identification information offences (sections 372.1, subsection 372.1A(1) and (3)) make it an offence to deal with, obtain, or possess identification information intending that the identification information will be used to commit or facilitate the commission of a serious offence. These offences all carry a maximum penalty of five years imprisonment.
81. Section 372.2 makes it an offence to possess identification information, intending it to be used to commit an offence against section 372.1 or subsections 372.1A (1) or (3). Section 372.3 makes it an offence to possess equipment used to make identification documentation, intending that the identification documentation will be used to commit an offence against section 372.1 or subsections 372.1A(1) or (3). Both offences carry a maximum penalty of three years imprisonment.

### Financial information offences

82. Part 10.8 of the Criminal Code sets out a range of financial information offences. These offences were inserted into the Criminal Code in 2004 by the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004 (Cth)*. In 2004, as part of the Model Criminal Law Officers project, a gap in relation to credit

## UNCLASSIFIED

card skimming offences was identified in Federal, state and territory laws. The Act addressed that gap at the Commonwealth level.

83. All of the offences in Part 10.8 relate to personal financial information which is defined to mean information relating to a person that may be used (whether alone or in conjunction with other information) to access funds, credit or other financial benefits.
84. Section 480.4 criminalises dishonestly obtaining or dealing in personal financial information without the consent of the person to whom the information relates. This offence carries a maximum penalty of five years imprisonment.

### Money laundering offences

85. Investigations undertaken by the AFP in relation to money laundering in Australia are primarily conducted under the *Financial Transactions Reports Act 1988 (Cth)*, the *Proceeds of Crime Act 2002 (Cth)* and the *Criminal Code Act 1995 (Cth)*. The AFP uses a risk based assessment and prioritisation model to ensure that resources are directed to high priority investigations, including those involving a money laundering offence.
86. The money laundering offences are contained in Division 400 of the Criminal Code. These offences meet Australia's international obligations under the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* and the *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*. Australia has fulfilled its international obligations by developing and implementing a money laundering enforcement strategy through four main measures: criminalising money laundering at a Federal, state and territory level; establishing and developing advanced technological systems to track cash and other forms of transferable value; a strong legislative framework to strip criminals of their proceeds of crime; and allowing international engagement with partner agencies through mutual assistance.<sup>9</sup>
87. Sections 400.3 to 400.8 of the Criminal Code set out a matrix of 18 offences, graded both in terms of the fault (mental) element required to be established, and the value of the money or property involved.
88. The six provisions set out offences of similar terms. In essence, these offences criminalise dealing with money or property that is proceeds of crime (e.g. money or property derived from the commission of a crime) or intended to become an instrument of crime (e.g. money or property used to commit an offence). The key difference between the provisions is the value of the money or property involved. Each provision includes three offences with different thresholds of criminal culpability: intent,

---

<sup>9</sup> Commonwealth Proceeds of Crime Act 1987, Financial Transactions Reports Act, 1988 and Mutual Assistance in Criminal Matters Act 1987.

## UNCLASSIFIED

recklessness or negligence. The higher the value of money or property involved, and the higher the fault element, the higher the maximum penalty applies.

89. For example, subsection 400.4(1) makes it an offence to deal with money/property that is (and the person believes it to be) proceeds of crime, and at the time of dealing, the value of the money/property is \$100,000 or more. The maximum penalty is 20 years imprisonment, a 1200 penalty unit fine, or both.
90. Subsection 400.6(2) makes it an offence to deal with money/property that is proceeds of crime, the person is reckless as to the fact that the money/property is proceeds of crime, and at the time of dealing, the value of the money/property is \$10,000 or more. The maximum penalty is five years imprisonment, a 300 penalty unit fine, or both.
91. Section 400.9 sets out two offences of dealing with money or property reasonably suspected of being proceeds of crime. A maximum penalty of three years imprisonment or a 180 penalty unit fine (or both) applies where the value of the money/property is \$100,000 or more. Where the value of the money/property is less than \$100,000, the maximum penalty is two years imprisonment or a 120 penalty unit fine (or both).
92. The money laundering offences in Division 400 were further strengthened in 2010, by the *Crimes Legislation Amendment (Serious and Organised Crime) Act (No.2) 2010 (Cth)*. Specifically, the amendments addressed several impediments to the investigation and prosecution of the offences as identified by the AFP and the Commonwealth Director of Public Prosecutions. In particular, the amendments extended the geographical jurisdiction of those offences and removed limitations on the scope of the offences to enable them to apply to the full extent of the Commonwealth's constitutional power in this area.
93. Money laundering may also be prosecuted under some offences contained in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* including:
- sections 142-143 – structuring offences;
  - sections 53, 55 – the movement of physical currency both in and out of Australia;
  - sections 136-138 – opening of bank accounts using false customer identification documents;
  - sections 139-141 – use of bank accounts in false names or failing to disclose the use of 2 or more names.