KEY ENABLERS

THEME SUMMARY

The ACIC has identified six key enablers for serious and organised crime:

- Money laundering
- Technology
- Professional facilitators
- Identity crime
- Public sector corruption
- Violence and intimidation

Key enablers have a unique role in facilitating serious and organised crime. Activities such as money laundering and identity crime contribute to the effectiveness of other types of organised crime. While not all of the above enablers are present in every illicit market, two or more enablers may be used concurrently within the same criminal enterprise.

Enablers are integral to the business of serious and organised crime groups. Law enforcement, regulatory, legislative or policy actions against enabling activities have the potential to disrupt criminal networks across multiple illicit markets or to severely hinder their activities. For example, increased law enforcement and regulatory capability to identify and prosecute professional facilitators would have a significant impact on all criminal groups relying on the expert advice and knowledge provided by such facilitators to perpetrate or conceal criminal activity. Similarly, reduced ability of crime groups to realise their illicit proceeds or conceal their illicit wealth through targeting of money laundering would be likely to affect future illicit activity by serious and organised crime groups.

MONEY LAUNDERING

Money laundering remains a fundamental enabler of profit-motivated crime, and is a significant, potentially lucrative criminal enterprise in itself. The primary goals of money laundering are to give illicit money the appearance of legitimacy and, through the use of complex methods, to move illicit funds without detection. Illicit funds, laundered for the appearance of legitimacy, are likely to be invested in businesses or schemes that provide the greatest chance of concealing the origins of the money, rather than on the basis of predicted returns.

Money laundering is an extremely diverse activity carried out at all levels of sophistication, and it plays an important role in serious and organised crime. The banking system and money transfer services are common methods used to launder funds, and money launderers continually exploit vulnerabilities in the financial system to circumvent the counter-measures designed to detect them. Bulk cash smuggling also remains a viable and active means to launder the proceeds of crime.

The ACIC's Eligo National Task Force[11] (Eligo) identified the following four key features of money laundering activity in Australia, which can appear separately or jointly:

- intermingling legitimate and illegitimate financial activities through cash-intensive businesses or front companies
- engaging professional expertise/facilitators
- engaging specialist money laundering organisations to provide specific money laundering services to domestic and international crime groups
- 'internationalisation' of the Australian crime environment—international money laundering components for Australian crime groups are common.

CASE STUDY: DISRUPTION OF INTERNATIONAL MONEY LAUNDERING SYNDICATE

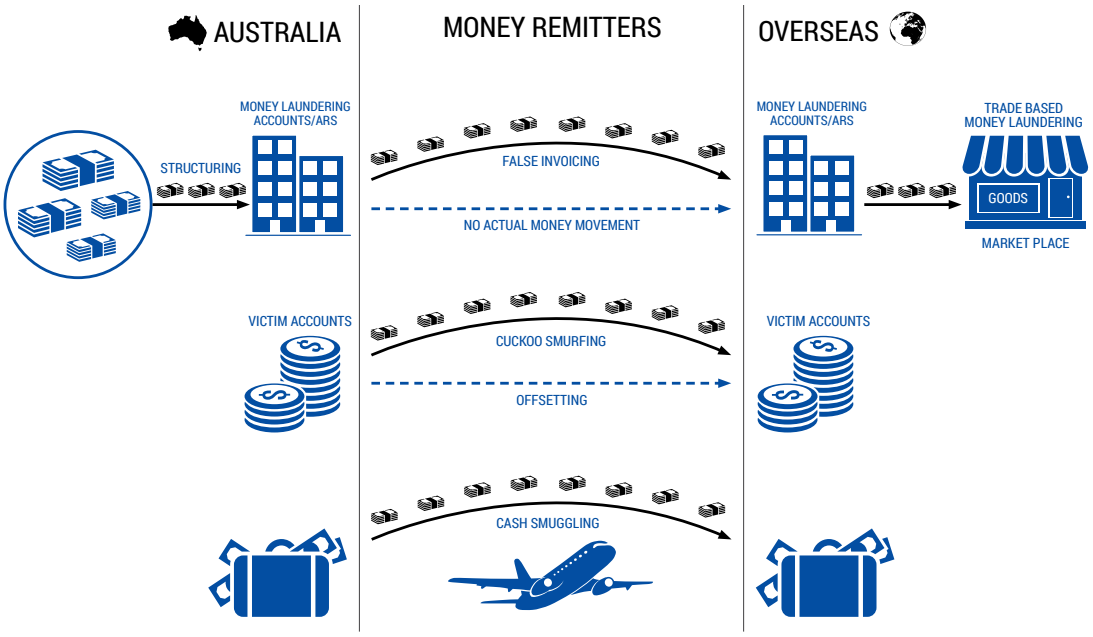
In January 2017, following a lengthy joint investigation, the key figure in an international money laundering syndicate was arrested in Sydney. The foreign national was charged with knowingly directing the activities of a criminal group. Police allege the woman coordinated the group's activities from Vietnam, recruited people to launder money, and directed them on how to acquire, deposit and exchange the funds through financial institutions.

Joint task force activity has provided Australian law enforcement with significant insights into the operation of transnational money laundering syndicates and their connections to other serious and organised crime groups. Investigations have strengthened law enforcement's understanding of the range and extent of methods and channels used to launder funds. These include the use of the banking sector, alternative money remitters, informal value transfer systems, casinos, trade-based money laundering, online wagering platforms, high-value commodity trading, complex domestic and international business structures, securities markets, virtual currencies and professional facilitators. Money laundering continues to be a focus of law enforcement with work being undertaken across multiple government agencies and across national and international jurisdictions.

Money laundering remains a key risk to Australia and is the common element in almost all serious and organised crime. Money laundering enables criminals to hide and accumulate wealth, avoid prosecution, evade taxes, increase profits through re-investment, and fund further criminal activity. Money laundering activities also have the potential to undermine the stability of financial institutions and systems, discourage foreign investment and alter international capital flows.

11 Eligo commenced in December 2012 under the then ACC to tackle the high-risk alternative remittance sector and operators of other informal value transfer systems impacting on Australia. Eligo was extended in 2014 under the Eligo 2 National Task Force (Eligo 2) to disrupt high-priority international and domestic money-laundering operators. The task force comprised members of the ACC, AFP and AUSTRAC, with support from Commonwealth, state and territory partners, along with a number of international partners. Eligo 2 ceased on 31 Dec 2016, with work continuing under the Targeting Criminal Wealth Determination.

MONEY LAUNDERING METHODS: MOVEMENT OF FUNDS OVERSEAS



SPORTS BETTING

Several international organised crime groups are direct owners of online bookmakers. Multiple opportunities exist for domestic and international criminals to utilise online bookmakers to launder proceeds of crime and profit from the corruption of sporting and racing events. This includes the capacity to bet large amounts of money anonymously through offshore bookmakers.

Bookmakers operating online wagering platforms are increasingly basing their operations in jurisdictions where regulation and oversight of gambling activities ranges from minimal to completely absent. Online bookmakers offer a vast array of wagering products on sport and racing events to a global customer base, including gamblers in Australia. The capacity of Australian regulatory agencies to effectively monitor gambling through domestic licensing and regulatory arrangements has been significantly impacted by the shift to the online domain.

As at 31 December 2016, there were approximately 25.4 million mobile handset subscribers and 13.5 million internet subscribers in Australia. This is an increase of 4.7 per cent in internet subscribers since the end of December 2015.

TECHNOLOGY

Increasingly, criminal activities are committed with the assistance of technology either via the online environment or through advances in technological capabilities, such as secure communications.[12] The online environment enables crime to be committed remotely and with relative anonymity—characteristics that are attractive to serious and organised crime groups and other motivated individuals, making the identification and prosecution of offenders more difficult. The commercial availability of secure communication platforms and surveillance equipment—such as tracking devices—provides serious and organised crime groups with the means to conceal their criminal activities from law enforcement. Serious and organised crime groups also engage the services of professional facilitators with relevant information and communication technology (ICT) knowledge and skills to assist in the commission of technology enabled crimes.[13]

In 2016, the Australian Cybercrime Online Reporting Network (ACORN) received 46,957 reports. The top three crimes reported related to scams and/or fraud (50 per cent), purchase or sale (20 per cent) and cyberbullying (7.5 per cent), and the top three modes of contact used to conduct these crimes were email, social networking and website advertising.

The majority of serious and organised crime activities are enabled, to some extent, by the use of technology. Technology is attractive to criminals as it can provide anonymity, obfuscate activities and locations, and increase their global reach by connecting them to potential victims and information around the world. Using technology to commit crime is also significantly more efficient and less resource intensive than traditional methods of perpetrating crime.

Identity crime, where personal identifying information is stolen and sold online, relies heavily on technology. Virtual currencies are used by criminals for money laundering and in exchange for illicit goods. Alternative banking services that are based online are being exploited by serious and organised crime to launder illicit funds, evade tax obligations and avoid regulatory oversight. Tax fraud has occurred as a result of compromised payroll systems and superannuation platforms have been targeted for fraud and theft. Technology is fundamental to the success of card fraud and facilitates the distribution of child exploitation material worldwide.

The two key enabling technologies currently used to facilitate serious and organised crime are virtual currencies and encryption. Virtual currencies, such as bitcoin, are increasingly being used by serious and organised crime groups as they are a form of currency that can be sold anonymously online, without reliance on a central bank or financial institution to facilitate transactions. Darknet[14] marketplaces such as Silk Road 3.0 and Valhalla

12 Secure communications include but are not limited to communication devices with military grade encryption, remote wipe capabilities, duress passwords and secure cloud-based services.

13 The Australian Cybercrime Online Reporting Network (ACORN) is a national policing initiative of Commonwealth, state and territory governments. It is a national online system that allows the public to securely report instances of cybercrime. It also provides advice to help people recognise and avoid common types of cybercrime.

14 The darknet is a routed allocation of internet protocol address space that is not discoverable by usual means. The term can refer to a single private network or to the collective portion of internet address space that has been configured in that manner. Popular darknets include Tor (the onion router), Freenet and I2P. Such networks are decentralised, routing traffic through a widespread system of servers, making it difficult to trace communications.

Marketplace are used to facilitate the sale and trafficking of illicit drugs, firearms, precursor chemicals and child exploitation materials. Australia's use of darknet marketplaces is expected to grow, given the increasing popularity of online trading and the perceived anonymity such marketplaces provide.

High-end encrypted smartphones continue to be preferred by serious and organised crime groups to reduce visibility of their activities to law enforcement. Multiple OMCGs and other serious and organised crime groups use encrypted communication devices and software applications such as Phantom Secure BlackBerry and Wickr as their primary means of communication, due to the content protection features available on these devices and applications.

Increased availability and ongoing advancement of technology will continue to provide criminals with a diverse range of resources to conduct criminal activity and impede law enforcement investigations.

PROFESSIONAL FACILITATORS

Serious and organised crime groups engage the services of professional facilitators to launder the proceeds of crime, conceal illicit wealth and enhance their criminal activities. Professional facilitators are individuals who possess specialist skills and knowledge and who are used, wittingly or unwittingly, to facilitate criminal activities. The most common professions exploited by organised crime include lawyers, accountants, financial and tax advisers, registered migration agents, stockbrokers, real estate agents and customs brokers. Information and communications technology professionals are also emerging as a key group of professional facilitators.

As seen with the release of the so called Panama Papers in April 2016,[15] criminal groups may employ offshore service providers to conceal their illicit funds. Service providers facilitate the creation of offshore company structures and associated bank accounts, and provide administration services, nominee directors or shareholders. These providers and the activities they undertake can be legal; however, their services can also enable criminals to conceal the beneficial ownership of assets and the transfer of illicit value between jurisdictions.

Professional facilitators possess detailed knowledge of often complex areas of expertise, improving a criminal group's resilience to law enforcement detection and intervention and increasing their opportunity for success. The use of professional facilitators often results in financial gains for criminals through tax evasion, money laundering, superannuation fraud, and phoenixing activities.

IDENTITY CRIME

Identity crime continues to be one of the most common types of crime committed in Australia, and acts as an enabler of significant criminal activities including money laundering, financial crimes, drug trafficking and fraud. The true extent of identity crime is difficult to quantify due to under-reporting, discrepancies in cross-jurisdictional reporting, and instances where identify theft is undetected. There is a growing trend towards the commission of identity crime online through the production and sale of identity documentation and fraudulent use of personal identifying information.

Identity crime commonly occurs through:

- 'phishing' activities where personal information is elicited over the telephone or internet and disclosed to a business-type entity that appears legitimate
- hacking online accounts
- retrieving personal information available on social media
- illegal access of personal information stored on business databases.

The cost of identity crime in Australia is estimated at A$2.2 billion, with prevention and response activities costing a further A$390 million.

The incidence of identity crime continues to exceed that of other personal and household thefts. 2016 AIC survey data indicates approximately 8.5 per cent of respondents had experienced misuse of their personal information and 5 per cent of all respondents reported a financial loss as a result of this misuse. Data breaches increased by approximately 5 per cent in 2015–16, with 123 voluntary and mandatory notifications reported.[16] Timely disclosure of data breaches is critical, as identity misuse typically occurs within 72 hours following the breach.

15 In April 2016, 11.5 million documents were leaked from the Panamanian law firm, Mossack Fonseca, exposing how secretive offshore tax regimes can be exploited to hide money and evade tax. See *Revenue and taxation fraud* for further information.

16 A voluntary data breach notification scheme allows businesses and agencies to self-report possible privacy breaches. Mandatory data breach notifications specifically refer to breaches of the *My Health Records Act 2012.*

Identity credentials, whether stolen or fraudulent, command high prices. Australian passports reportedly cost up to A$5,200 on the illicit online market; drivers licences and Medicare cards—the most frequently used credentials in identity crime—can be purchased for A$400 and A$250 respectively.

Compromise of one type of identity credential can often enable further compromise of other credentials. For example, unauthorised mobile phone porting—where mobile numbers are transferred to another carrier without the owner's consent—is likely to involve an earlier compromise of an identity credential such as a drivers licence.

The financial impact of identity misuse on the individual varies; however, the process of restoring identity can be both time-consuming and complex. The minor financial loss contributes to under-reporting of incidents: victims commonly report identity misuse to financial institutions, for reimbursement purposes, but not to law enforcement. Collaborative work between government, business and community sectors will help mitigate the risk of identity crime. Increasing uptake of the Document Verification Service,[17] particularly in the private sector, and use of biometric identification will strengthen identity protection.

The Document Verification Service uses name-based checks to help prevent the use of fictitious identities. It is not designed to detect instances where criminals steal information used on legitimately issued evidence-of-identity documents and substitute their own photos. To address this risk, the Australian Government is implementing the Face Verification Service, which uses photos on evidence-of-identity documents to help verify a person's identity.

It is expected the threat of identity crime will continue to evolve, particularly as the amount of personal information posted online through social, business and consumer platforms continues to grow.

PUBLIC SECTOR CORRUPTION

Public sector corruption is the misuse of public power or position for personal and/or third-party gain or advantage. Exploitation of the public sector by serious and organised crime weakens the instruments of government and strengthens criminal networks, undermining public confidence in government and public office. There is currently limited evidence of serious and organised crime involvement in public sector corruption in Australia. Areas of the public sector considered most at risk of corruption by serious and organised crime include procurement across all levels of government, frontline agencies, and new agencies without established anti-corruption practices.

While Australia is viewed as one of the least corrupt countries, the Transparency International *Corruption Perceptions Index* has rated Australia 13th in 2016, after rating Australia 7th in 2012. Various reasons for the decline in Australia's perception ranking have been cited, including a number of well-publicised instances of corruption in sport as well as publicity generated by several recent anti-corruption agency and royal commission investigations into criminality and workplace misconduct.

17 The Document Verification Service is one of the key initiatives of the Council of Australian Governments' *National Identity Security Strategy*. It is a national online system that allows organisations to use information taken from a person's identity document, with their consent, and compare this against the corresponding records of the document issuing agency.

VIOLENCE AND INTIMIDATION

Violence and intimidation continues to enable serious and organised criminal activity in Australia. The majority of violence involving organised crime occurs between criminal groups, rather than being directed at members of the general public. Serious and organised criminals will often use violence and intimidation to extort significant financial gain from individuals and their businesses, or to coerce them into facilitating and/or undertaking criminal activities on behalf of the organised crime group. Violence may also be used as a means to control drug networks and settle disputes with the intention of causing serious injury or death. The threat of violence posed by serious and organised crime groups is realised across all jurisdictions. For example, in 2016 a series of execution-style shootings left eight people dead in New South Wales, including a significant underworld figure who was shot multiple times on a residential street in Earlwood in Sydney.

Victims of violence and intimidation at the hands of individuals associated with serious and organised crime groups may be reluctant to report their experiences to police or health professionals for fear of retribution. Under-reporting creates challenges for determining the exact nature and extent of harm caused through the use of violence and intimidation tactics by serious and organised crime.