Appendix B – AUSTRAC case studies involving the use of telecommunication data

The sanitised case studies in this appendix are examples of how AUSTRAC intelligence contributes to investigations into serious crime and terrorism financing.

Each case also exhibits criminal use of telecommunications, including for arranging drug importations, transferring and laundering the illicit proceeds of crime and financing overseas terrorist groups. Access to the evidence trail left by telecommunications would greatly assist AUSTRAC in cases such as these.

Access to telecommunications data is especially important where criminals attempt to exploit the anonymity afforded by unregulated financial channels, such as digital currencies (see Case 1). In cases such as this, where criminals misuse new and/or unregulated channels or products, it creates an information gap for AUSTRAC and its partner agencies – a gap AUSTRAC could resolve through the judicious use of telecommunications data.

Case 1 – Suspect used black market website and digital currencies for drug trafficking

Comment [JM1]: Case summarised

AUSTRAC assisted an investigation which led to the arrest of a suspect who used a digital currency to purchase, import and sell illicit drugs through a black market website.

Australian law enforcement intercepted a number of packages containing cocaine and methylenedioxymethamphetamine (MDMA), sent to from Germany and the Netherlands.

AUSTRAC information identified that the suspect had transferred funds via banks to an online digital currency exchange based overseas, enabling him to purchase an amount of digital currency.

Law enforcement executed a search warrant on the suspect's home computers, **mobile phones** and a number of stun guns.

Analysis of the suspect's mobile phones identified text messages thought to be associated with drug trafficking. The suspect's computers revealed he maintained an online account with a black market website which allowed him to purchase and sell illicit drugs and conduct transactions using a digital currency.

The suspect was sentenced to three years and six months imprisonment. He was also fined AUD1,000 for possessing controlled weapons.

Case 2 - Canadian drug importations hidden in foot spas

Comment [JM2]: Case summarised.

A law enforcement investigation foiled efforts by an Asian organised crime group to import hundreds of kilograms of drugs – cocaine, ecstasy and crystal methamphetamine ('ice') – into Australia. Authorities intercepted several shipping containers from Canada and seized drugs worth more than AUD31 million, hidden in foot spas.

AUSTRAC financial transaction information helped identify the Canadian company believed to have supplied the foot spas and the Australian companies that were to receive the importations.

A Canadian national suspected of being the main organiser of the importations conducted low-value international funds transfers from Australia to Vietnam while

visiting Australia. The associated international funds transfer reports revealed a mobile phone number used by the suspect when undertaking the transactions.

This same phone number was also provided by a second suspect when sending low-value transfers to beneficiaries in Vietnam through a remittance dealer based in Australia. This second suspect was subsequently arrested for overseeing one of the drug importations.

As result of the investigation, three suspects were sentenced to jail terms ranging from five-and-half years to 19 years.

Case 3 - Drug trafficker intercepted with 1.5 kilograms of cocaine

Comment [JM3]: Summarise and include, or not?

A money laundering and drug importation syndicate was dismantled as a result of a joint operation between Australian law enforcement agencies.

An investigation into a suspected money laundering syndicate led law enforcement officers to stop and question a Canadian man at an Australian airport upon his arrival from Hong Kong. The man was searched and allegedly found to be carrying approximately 1.5 kilograms of cocaine strapped to his legs. The law enforcement investigation continued and officers searched two properties and uncovered a significant amount of cash. Two other men were also arrested as a result of the investigation.

Authorities had previously been monitoring the syndicate for suspected money laundering. AUSTRAC's database was used to monitor the syndicate's financial activities, which included numerous international funds transfer instructions (IFTIs) into and out of Australia. The details of these international transfers assisted law enforcement agencies to identify overseas associates of the syndicate.

AUSTRAC information was also used to trace the activities of the syndicate members within Australia and to assist law enforcement officers investigating the syndicate under the *Proceeds of Crime Act 2002*. Information contained in financial transaction reports linked members of the syndicate to each other through their activities, addresses and **mobile phone numbers.**

Following their arrests, the three men faced charges including importing a prohibited substance and attempting to possess a prohibited import. All three were also charged with dealing with proceeds of crime relating to money or property worth AUD50,000 and were remanded in custody.

The syndicate member who attempted to smuggle the cocaine into Australia pleaded guilty and was sentenced to six years with a non-parole period of four years. Another member of the syndicate received a six-month suspended sentence with a two-year good behaviour bond for possession of cash which was reasonably expected to be the proceeds of crime.

As a result of the investigation, authorities also restrained assets worth AUD1.3 million under the Proceeds of Crime Act, including three houses, two vehicles and AUD67,000 cash.

Case 4 - Money laundering remitter jailed after sending false reports to AUSTRAC

Comment [JM4]: Summarise and include, or not?

Law enforcement conducted an investigation into a remittance service provider suspected of falsifying customer information on transaction reports and submitting false information to AUSTRAC to facilitate money laundering.

AUSTRAC information was critical to the law enforcement investigation to help identify that the remitter and his remittance business had assisted a criminal syndicate with laundering the proceeds of identity fraud. The identity fraud involved money fraudulently withdrawn from the bank accounts of innocent third parties. A key element in the laundering of criminal proceeds involved the remitter disguising the funds and concealing the identity of members of the criminal syndicate.

The typical activity undertaken to launder the illicit funds involved:

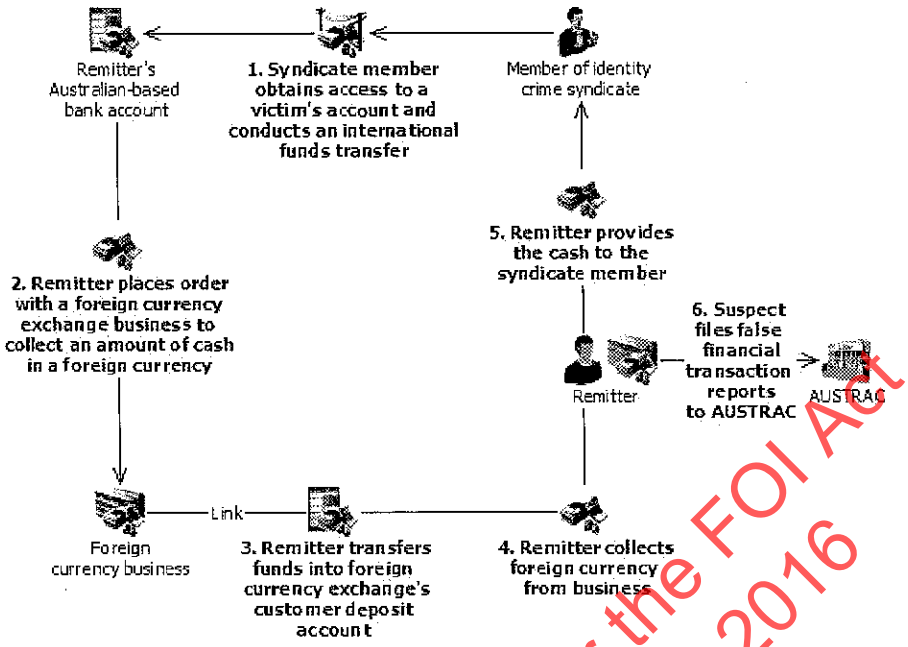
1. A member of the identity crime syndicate would obtain access to a victim's account and arrange for funds from the account to be sent as an international funds transfer instruction (IFTI) into an Australian account operated by the remitter.
2. The remitter would place an order with a foreign currency exchange business to collect an amount of cash in foreign currency equivalent to the value of the stolen funds.
3. Using the stolen money, the remitter would transfer funds into the foreign currency exchange's customer deposit account.
4. The remitter would visit the foreign currency exchange to collect the foreign currency.
5. With the original stolen funds now laundered into foreign currency, the remitter would provide the foreign currency, less a commission, to a member of the criminal syndicate.
6. As a last step in concealing the money trail, the remitter would file a significant cash transaction report (SCTR) with AUSTRAC detailing the payment to the syndicate member, but using false identification details to conceal the recipient's true identity from authorities.

Analysis of financial transaction activity by law enforcement, supported by AUSTRAC analysts, revealed the remitter had reported approximately AUD3.5 million in SCTRs over a two-year period. Further law enforcement investigation found that the majority of recipients recorded in these transaction reports could not be identified or did not exist. Over this same period, 15 foreign exchange transactions were reported to AUSTRAC totalling over AUD1.1 million. The value per transaction ranged between AUD10,000 and AUD 200,000.

AUSTRAC also received suspect transaction reports (SUSTRs) relating to the remitter's financial transactions with other reporting entities. Information within the SUSTRs, combined with further analysis of personal financial transactions undertaken by the remitter, revealed a range of suspicious activity, including:

- the remitter's reluctance to explain the source of funds to bank staff
- the depositing of large amounts of cash into an account followed by an international funds transfer on the same day
- the use of third parties to make international funds transfers on the remitter's behalf.

The law enforcement investigation collected evidence confirming the remitter was involved in money laundering on behalf of third parties. The remitter was charged and convicted on multiple counts of dealing with the proceeds of crime worth more than AUD100,000 contrary to section 400.4 of the *Criminal Code Act 1995*. The remitter was ultimately sentenced to five years and six months imprisonment, with a minimum of three years and seven months. The remitter was also charged and convicted of money laundering offences.



Case 5 - Australian terror suspects sent funds to Somalia to support terrorist group

Comment [JM5]: We should definitely include this case – Jon to summarise

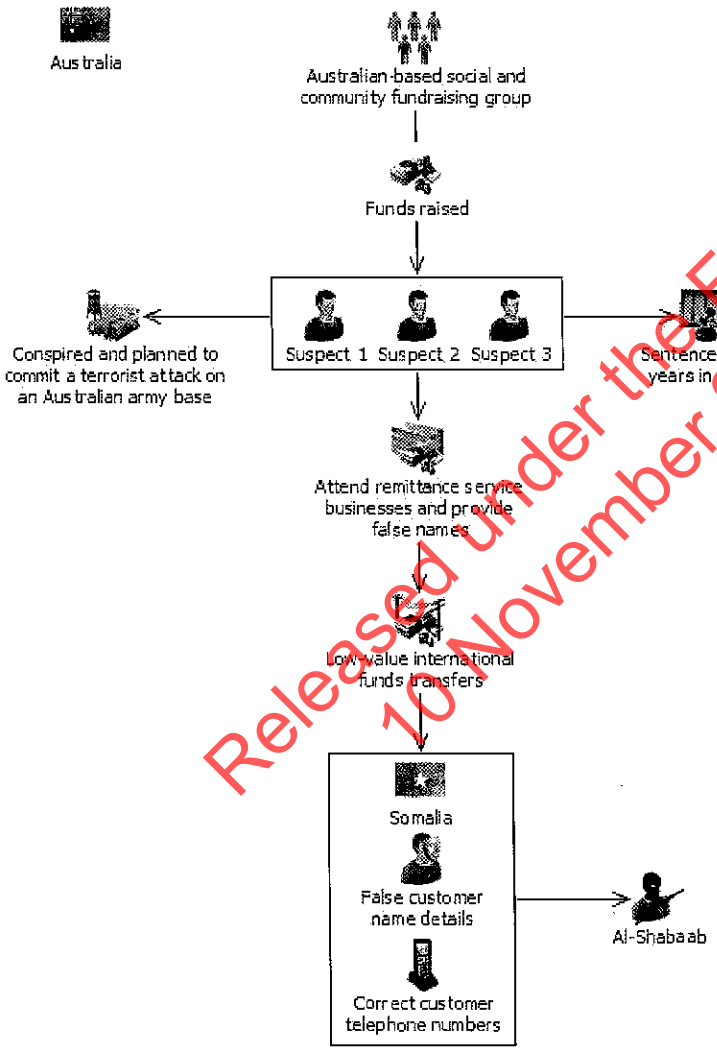
A joint-agency investigation led to the arrest of five suspects on charges of conspiring to commit a terrorist attack on an Australian army base. Investigations revealed the group had sent funds destined for use by the Somalia-based terrorist group, al-Shabaab. The group had also facilitated travel for Australian-based supporters to attend overseas military training camps. Funds remitted offshore by the suspects did not go directly to al-Shabaab but to entities linked to al-Shabaab's activities in Somalia.

Investigating officers, assisted by AUSTRAC information, discovered that the suspects had sent thousands of dollars in low-value IFTIs to Somalia. Authorities suspected these IFTIs were to support the aims of al-Shabaab and associated military training activities overseas.

The suspects sent the funds via remittance service businesses, often using false names for the overseas beneficiary customer to obscure the money trail. However, the **telephone numbers** recorded in the IFTIs for the overseas customers were correct. Investigating officers concluded that the suspects used the customers' correct **phone numbers** to ensure the funds arrived safely and were handed to the correct customer in Somalia. In this case, the information reported in the IFTIs was valuable intelligence for the investigation officers to use to corroborate other information or consider leads in the investigation.

In general, the group members paid for the remittances to Somalia using their own funds. The group also remitted funds that had been raised by Australian-based social and community fundraising groups – a common terrorism-financing method internationally. There was no evidence to suggest that members of the social and community groups involved were aware that the funds being raised were to be remitted to East Africa in support of al-Shabaab.

Three suspects were found guilty of conspiring to plan an Australian-based terrorist attack and sentenced to 18 years jail to serve 13 years and six months. Two of the suspects were found not guilty.



Case 6 - 'Cuckoo smurfing' used in million dollar money laundering scheme

Comment [JM6]: Summarise and include, or not? Might be worth including, as an example of TF Eligo type activity.

AUSTRAC disseminated a suspect transaction report (SUSTR) to a law enforcement partner agency, which sparked an investigation into a widespread money laundering syndicate.

Further investigations revealed that the syndicate, which operated in multiple states across Australia, was using a money laundering technique known as 'cuckoo smurfing'.

The criminal syndicate misused the bank account of a legitimate Australian-based export company in its money laundering scheme. The scheme also exploited legitimate international funds transfers made by a customer of the export company, who was based in Pakistan.

The Pakistan-based customer sent funds, via a remittance business in Pakistan, to the Australian-based export company. The funds transfers were payments for legitimate invoices owing to the Australian company.

However, investigations revealed that the Pakistani remitter used to remit the funds had connections with money laundering crime syndicates in Australia.

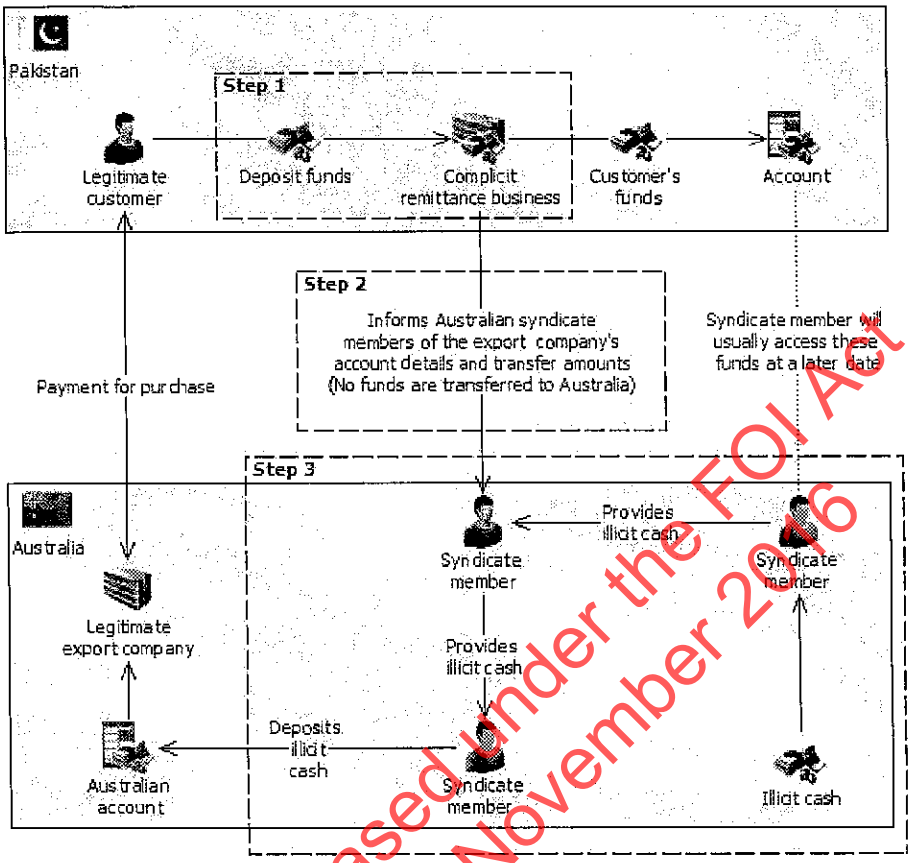
The following steps outline how the illicit funds were laundered:

1. The Pakistani-based customer of the export company attempted to send funds via a Pakistani remittance business to the export company's Australian bank account, for the payment of legitimate invoices.
2. The Pakistani remitter informed the money laundering syndicate in Australia of the export company's bank account details and the amounts required to be deposited into the company's account in Australia.
3. Australian syndicate members made a number of cash deposits into the Australian account of the export company equal in value to the expected payments from Pakistan. The cash deposits were often made in structured amounts, intended to fall below the AUD10,000 cash transaction reporting threshold. These funds were the proceeds of illicit activities undertaken in Australia.
4. Meanwhile, the remitter in Pakistan transferred the funds provided by the customer in Pakistan into another account in Pakistan, to be later accessed by a member of the syndicate.

Over a 15-month period, 13 SUSTRs were reported to AUSTRAC by major banks, identifying multiple structured cash deposits made by third parties into the export company's Australian bank account.

During this period approximately ten syndicate members conducted 217 cash deposits totalling AUD2.1 million into the Australian bank account of the export company. A total of 196 of these cash deposits were structured deposits, totalling AUD1.6 million. The structured deposits were primarily conducted in amounts between AUD8000 and AUD9500 at multiple bank branches throughout Sydney and Melbourne.

The syndicate members were careful to provide the bare minimum of personal information when undertaking the cash deposits. Nevertheless, 18 bank deposit receipts examined by law enforcement revealed identifying characteristics such as **phone numbers**. These identifiers lead to the identification of some of the depositors.



Case 7 - Suspicious transactions revealed Colombian cocaine importations

Comment [JM7]: Summarise and include, or not?

An Australian law enforcement agency arrested and charged two suspects for importing nearly AUD2 million worth of cocaine into Australia from South America. The international investigation involved Australian, German, and New Zealand law enforcement agencies. AUSTRAC information assisted the investigation by linking the suspects to the purchase of the drugs and the methods used to pay for and import the drugs.

- A reporting entity submitted a suspect transaction report (SUSTR) to AUSTRAC highlighting the following activity:
- One of the suspects sent six international funds transfers from five different branches of the same remitter over a one-month period.
- All transfers were for amounts between AUD1,300 and AUD4,200. The total amount transferred was more than AUD20,000.
- The funds were all sent to the same beneficiary in Colombia who collected them from three different locations.

- It appeared as if the suspect may have split the funds transfers into several transactions in attempt to avoid transaction reporting requirements by establishing a number of bank accounts at various banks.

The suspects, originally from New Zealand, flew to Australia to organise the cocaine importation. They transferred funds to Colombia to pay for the cocaine which was hidden in industrial equipment to be shipped to Australia. They also spent over AUD4,000 on arrangements with couriers, **mobile phone**s and apartments, to avoid detection.

German and Australian law enforcement agencies cooperated to intercept the packages in Germany and confirm the presence of the cocaine. Listening devices were attached to the packages which were monitored by Australian law enforcement until they **were** delivered to the suspects' address in Australia. **Telephone calls** made by the suspects were also tapped and they were heard discussing the drug shipments.

Both suspects were arrested at their Australian hide-out and charged with attempting to possess a marketable quantity of an unlawfully imported border control drug. The suspects were each sentenced to 11 years imprisonment, with one to be deported to New Zealand upon release.

Case 8 – Drug importation through the postal system

Comment [JM8]: Summarise and include, or not?

Case study summary

A law enforcement investigation identified a suspect based in Australia who was in receipt of drugs imported into Australia through the postal system. AUSTRAC information showed a correlation between international funds transfers coinciding with drug importations. The suspect was sentenced to 10-and-a-half years imprisonment for attempting to possess or possessing a border controlled drug contrary and recklessly dealing in the proceeds of crime.

The case study involves an established method of structuring international funds transfers to be below the perceived reporting threshold.

Investigation outline

A suspect used false identification to lease multiple privately owned mailboxes. The drugs were imported into Australia in letters and packages addressed to the various false identities based in Sydney. The suspect used multiple aliases to transfer funds overseas via a remittance service provider in various locations.

Law enforcement enquiries revealed the packages containing drugs were sent from Brazil, Laos and France. One package from Brazil included a greeting card and two plastic bags which contained pure cocaine with a street value of between AUD3,000 and AUD7,500. Another package sent from Laos contained cocaine with an estimated street value between AUD73,000 and AUD101,000.

The suspect drove to Brisbane where he obtained a package from an individual. Upon his return to Sydney, law enforcement officers stopped his vehicle and a search revealed a backpack hidden in the tyre well of the boot. The backpack contained pellets made up of pure heroin with an estimated street value of between AUD121,680 and AUD162,240.

During a search of the suspect's residential property, law enforcement officers located cash totalling AUD61,150, and numerous **mobile phones** and money transfer documents.

Analysis of the **mobile phone** SIM cards revealed the suspect had been in frequent contact with individuals in Nigeria, Brazil, Ghana and Suriname. Documents were located which indicated the suspect had transferred money overseas in various names.

Industry contribution

Suspicious matter reporting (SMRs) submitted by remittance service providers identified the following suspicious activity:

- a higher than normal volume and frequency of international funds transfer instructions (IFTIs)
- all outgoing IFTIs were paid for in cash, in structured amounts below the AUD10,000 cash reporting threshold
- the recording of multiple address details and **telephone numbers**
- addresses slightly altered or completely different to previous transactions.

AUSTRAC contribution

Analysis of AUSTRAC information identified the overseas beneficiary customers, and identified other aliases and identities suspected to be involved. AUSTRAC monitored the aliases used by the suspect.

AUSTRAC data further assisted in showing a correlation between the transfers of funds overseas coinciding with the importation of drugs. The importation of drugs was usually followed by the transfer of funds to countries including Laos, Brazil and Nigeria.

AUSTRAC information identified that all outgoing IFTIs were conducted via remittance service providers in various locations. The IFTIs were paid for in cash amounts below AUD10,000, and multiple transactions were conducted in one day.

AUSTRAC financial transaction activity linked an alias to a drivers licence number, which was linked to an additional six aliases of the suspect. The additional identities used the drivers licence as a form of identification. Over an eight-month period, 11 SMRs were submitted by remittance service providers which mentioned the drivers licence number.

Outcome

The suspect possessed or attempted to possess a total commercial quantity of two kilograms of cocaine and heroin with a total estimated street value of between AUD322,180 and AUD493,240.

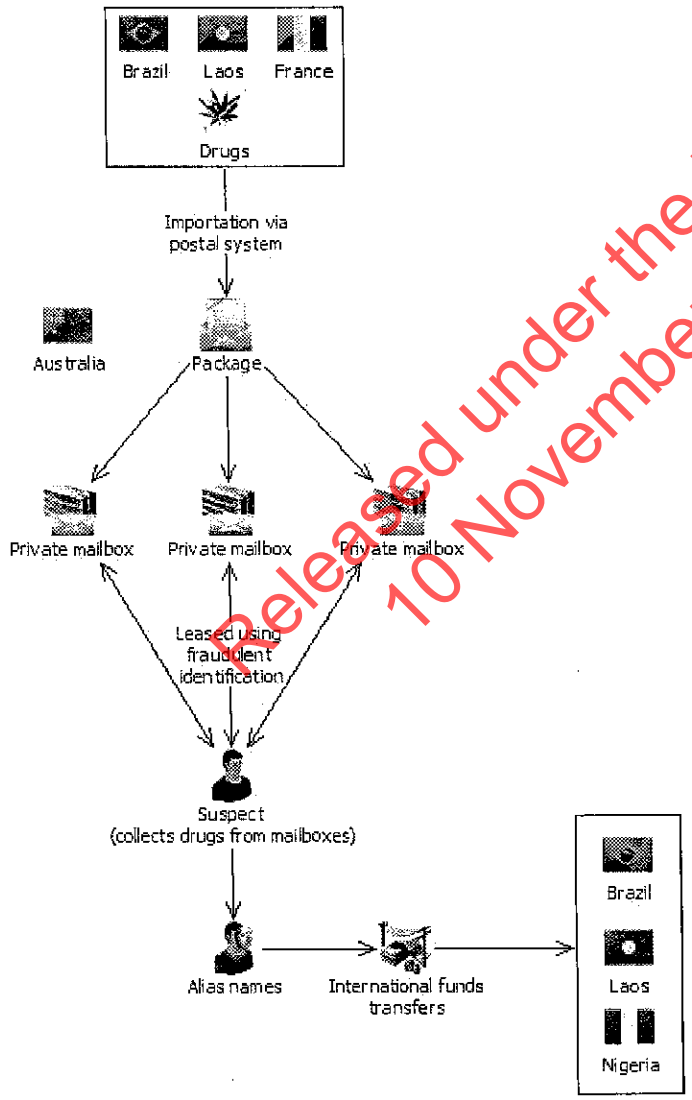
On appeal, the suspect was convicted of the following offences:

- three counts of attempting to possess marketable quantities of unlawfully imported border controlled drugs contrary to section 307.6(1) of the Criminal Code Act 1995

- one count of possessing a marketable quantity of a boarder controlled drug reasonably suspected to have been imported contrary to section 307.9(1) of the Criminal Code Act
- one count of recklessly dealing in the proceeds of crime, greater than $50,000 contrary to section 400.5(2) of the Criminal Code Act 1995.

The suspect was sentenced to 10-and-a-half years imprisonment with a total non-parole period of six years and 10 months.

Figure 1 – False identities used to import drugs into Australia



Document 2

TOPICAL ISSUE BRIEF

ISSUE: ACCESS TO TELECOMMUNICATION INTERCEPTION MATERIAL

Talking points:

- AUSTRAC having access to metadata substantially increases our capability to fight terrorism and provide stronger and more diverse intelligence to partner law enforcement agencies.
- This new capability would strengthen the future capability of NFIC.
- Other law enforcement agencies rely on AUSTRAC for its expertise to identify suspect transactions and new financial crime trends, this access would further enrich that expertise.
- The ACCC, which addresses consumer issues, has access to this data, through their agency status, yet AUSTRAC which is mandated to fight terrorism and money laundering does not.
- AUSTRAC has assumed a global leadership role and is influencing globally to maximise financial intelligence sharing with a present emphasis on terrorism financing.
- AUSTRAC would like to further discuss the options available to provide it with this essential capability.

KEY ISSUES:

- On 9 February 2016, the Attorney-General's Department (AGD) orally advised that the Attorney-General had declined AUSTRAC's request to be prescribed as a ***criminal law-***

enforcement agency under Section 110A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

- This decision appears to overlook AUSTRAC's mandated role in combating serious and organised crime, money laundering and the financing of terrorism.
- Given AUSTRAC's role, the decision appears further inconsistent when comparing with the designation of ASIC and the ACCC, that although playing a significant role in the protection of Australia's financial markets and consumer interests, do not address similar national security harms.
- The sentiment on the value of financial intelligence was expressed through comments made by the French Finance Minister following the terrorist attacks in Paris in November 2015: *'The struggle against terrorism . . . is first and foremost [for us] a struggle against its financing'.*
- The decision reinforces the urgency of a key recommendation in the report of the statutory review to simplify the framework at Part 11 (Secrecy and Access) of the AML/CTF Act to enhance the sharing of AUSTRAC information.
- This Review recommendation is a critical element to the success of the NFIC and it is important that any necessary feedback from the Minister's Office is conveyed to AGD to ensure finalisation and formal consideration before Ministerial tabling in Parliament.
- Following the Attorney-General's decision, AGD has suggested AUSTRAC consider alternative options for accessing

telecommunications data;

section 47E

- AUSTRAC's submission in June 2015 highlighted the nexus between AUSTRAC's operations and the additional intelligence value telecommunications data would provide.
- Since this time global terrorist events have further heightened the importance of building a comprehensive intelligence picture.
- The financial system is rapidly being transformed by digital disruption, a process in which telecommunications technologies will play an increasingly major role.
- AUSTRAC's inability to access telecommunications data will severely restrict the agency's ability to keep pace with technology and respond to 21st century challenges.
- Since AUSTRAC's original submission in mid-2015, the agency has continued to evolve to maximise prevention, detection and disruption into the future. In particular, AUSTRAC has worked with government and industry partners to develop the concept of the centre for excellence in financial intelligence – the National Financial Intelligence Centre.
- Furthermore, AUSTRAC has assumed a global leadership role and is influencing globally to maximise financial intelligence sharing with a present emphasis on terrorism financing.

BACKGROUND:

In response to a written invitation, AUSTRAC made a submission to the Attorney-General on 17 June 2015, to be prescribed as a ***criminal law-enforcement agency*** under Section 110A of the *Telecommunication (Interception and Access) Act 1979* (TIA Act).

On 9 February 2016, the Department orally advised that the Attorney-General had declined AUSTRAC's request to be prescribed. The Department has explained that the Attorney-General has resolved not to prescribe any new agencies under section 110A of the TIA Act, and that this position is unlikely to alter in the immediate future.

AGD has not as yet provided AUSTRAC with a written explanation behind the rationale for why certain agencies were prescribed under the TIA Act (for example, the ACCC and ASIC), while AUSTRAC was not.

AUSTRAC's Role as an Enforcement Agency

All agencies currently listed under section 110A of the TIA Act are responsible for investigating and prosecuting (enforcing) breaches of the criminal law, independent of other agencies. AUSTRAC as an FIU and AML regulator currently has limited powers and provisions to investigate and prosecute breaches of the criminal law under the AML/CTF Act. The absence of a clear mandate to investigate and enforce criminal law may have been a reason that weakened the effectiveness of AUSTRAC's submission. This issue has been identified and is being addressed in the Statutory Review of the AML/CTF Act through recommendations to amend the objects of the Act.

The guidance provided by the Department defines "enforcement of the criminal law" to include the gathering of intelligence about crime to support the investigating and prosecuting functions of law enforcement agencies. It is considered AUSTRAC's role as Australia's financial intelligence unit directly meets this requirement.

AUSTRAC's direct role in intelligence collection and analysis related to combating serious and organised crime, transnational crime and terrorism is far reaching and is of critical value domestically and internationally. AUSTRAC's contribution to major national security and law enforcement investigations should be given full weight in any assessment of its role in gathering actionable intelligence.

AUSTRAC intelligence analysts are experts in their field. While AUSTRAC's partner agencies utilise AUSTRAC information in their investigations, AUSTRAC's capability to conduct specialist financial intelligence analysis is not currently replicated by other agencies.

Telecommunications information provides valuable contextual information to financial transaction data. It enhances financial intelligence to enable the

identification and understanding of the intent behind suspicious financial transactions. With the rapid uptake of digital based transactions the linkage between telecommunications and financial activity will become increasingly interwoven. When identifying terrorism financing threats, which are often low-value and innocuous in appearance, as seen in recent terrorist attacks overseas, this linkage will be of increasing benefit for intelligence and investigators.

Future Opportunities

The Report of the Statutory Review of the AML/CTF Act includes several key recommendations which will provide opportunities to further pursue our requirement to be prescribed as a law enforcement agency under the TIA Act. In particular, the report recommends that the objects and general principles of the AML/CTF Act should be amended to more clearly articulate AUSTRAC's role in discovering, understanding, and responding to money laundering and terrorism financing threats, and that the functions of the CEO should be expanded.

It is considered that the development and implementation of these key recommendations, and the establishment of a National Financial Intelligence Centre, add substantial weight to AUSTRAC's compelling case for access to telecommunications data.

AGD's suggested alternative options to access telecommunications data

AGD has provided several altemative options for AUSTRAC to consider in relation to obtaining access to telecommunications data:

1. In the context of a joint investigation or taskforce where AUSTRAC is involved with another agency which has been prescribed as a law enforcement agency for the purposes of the TIA Act – for example, the AFP, ACC, ACCC or ASIC etc; or

2. AUSTRAC consider whether it can use a formal Notice Power under the AML/CTF Act (e.g. section 49) which can be used in conjunction with section 280 of the *Telecommunications Act 1997* and which could be served on a telecommunications company requesting that they provide information as specified in the Notice.

section 42

AUTHORISED:
Bradley Brown
A/g National Manager
Strategic Intelligence and Policy
02 9950 0085

CONTACT:
Richard Bunting
Director
Policy and Guidance
03 8636 0587

23 February 2016

Attachment A: Definition of Enforcement Agency

Definition of enforcement agency BEFORE Data Retention Bill	Definition of criminal law-enforcement agency AFTER Data Retention Bill
the Australian Federal Police	the Australian Federal Police
a Police Force of a State	a Police Force of a State
the Australian Commission for Law Enforcement Integrity	the Australian Commission for Law Enforcement Integrity
the ACC	the ACC
the Immigration and Border Protection Department	the Immigration and Border Protection Department, only in connection with the investigation by that Department of a contravention of: • the Customs Act 1901; or • the Crimes Act 1914; or • the Criminal Code; or • the Environment Protection and Biodiversity Conservation Act 1999; or • Part 6 of the Australian Border Force Act 2015; or • an Act prescribed in a legislative instrument made by the Minister for the purposes of this paragraph; or • a provision of an Act, being a provision prescribed in a legislative instrument made by the Minister for the purposes of this paragraph.
the Crime Commission	the Crime Commission
the Independent Commission Against Corruption	the Independent Commission Against Corruption
the Police Integrity Commission	the Police Integrity Commission
the IBAC	the IBAC
the Crime and Misconduct Commission	the Crime and Corruption Commission
the Corruption and Crime Commission	the Corruption and Crime Commission
the Independent Commissioner Against Corruption	the Independent Commissioner Against Corruption
an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph	subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.
a body or organisation responsible to the Ministerial Council for Police and Emergency Management - Police	**REMOVED**
the CrimTrac Agency	**REMOVED**
any body whose functions include: • administering a law imposing a pecuniary penalty; or • administering a law relating to the protection of the public revenue.	**REMOVED**
	ADDED - the Australian Securities and Investments Commission
	ADDED - the Australian Competition and Consumer Commission

Document 3

Australian Government

Australian Transaction Reports and Analysis Centre

Submission – Enforcement agency access to telecommunications data

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015

Australian Transaction Reports and Analysis Centre

Contents

AUSTRAC Contact officer

Richard Bunting, Director, Domestic Policy

Tel: 03 8636 0587 Mobile: 0439 416 795

E-mail: richard.bunting@austrac.gov.au

Introduction

1. AUSTRAC's critical role as Australia's financial intelligence unit has evolved in recent years, in parallel with increased whole-of-government emphasis on collaboration between agencies and greater recognition of the benefits of sharing intelligence. AUSTRAC's expanded role reflects the reality that criminals and terrorism financiers do not respect national or international borders, and that tackling serious and organised crime requires coordinated responses and information sharing across government.
2. This trend is reflected in the *2015–18 National Organised Crime Response Plan*, under Initiative Six, 'Reducing barriers to information sharing between agencies'. This includes enhancing legislative arrangements for sharing information between Commonwealth agencies and enhancing arrangements with the Australian Taxation Office (ATO), Centrelink and AUSTRAC to improve information sharing in unexplained wealth investigations and litigation.
3. AUSTRAC has experienced increased demand from its partner agencies for access to its financial intelligence data and for more sophisticated analysis. AUSTRAC's total number of Commonwealth, state and territory designated partner agencies has grown to 40 as of June 2015.[1] Similarly, AUSTRAC has expanded its international network of counterpart financial intelligence units – in 2008–09 AUSTRAC had 55 agreements in place for the international exchange of financial intelligence; by March 2015 this number had grown to 75.
4. In recognition of this increased use and application of AUSTRAC data, successive governments have also increased investment in AUSTRAC's intelligence functions and systems, including a $24 million investment in the 2010 budget to enhance AUSTRAC's analytical capability and $20 million over four years in 2014 for AUSTRAC to improve the detection and disruption of terrorism financing.
5. In the 2015 Budget, the Government announced additional funding of $21.1 million over four years to finance a revenue protection initiative between AUSTRAC and the Department of Human Services (DHS), aimed at protecting the integrity of taxpayer dollars and reducing the risk of erroneous or fraudulent welfare payments.
6. AUSTRAC requires access to telecommunications data to fully capitalise on the recent investment in the agency's enhanced systems. Combining financial intelligence with associated communications data will provide AUSTRAC and its partners with a greater degree of insight, not just into criminal financial activity itself, but the underlying reasons for the activity – this will address a key information gap in financial intelligence – the intended end use of the funds. This information will create efficiencies in the intelligence value chain and will enable AUSTRAC to continue providing the Australian law enforcement, intelligence and national security community with timely, high-quality actionable intelligence.
7. Access to telecommunications data is also crucial for the agency to keep pace with rapid evolutions in technology and new payment methods. Customers, both legitimate and criminal, have embraced mobile and internet banking and new payment models, including online money transfer platforms. AUSTRAC requires access to telecommunications data to complement and enhance its traditional transaction reporting data and shed light on potentially illicit transfers conducted using these new payment methods.

[1] Correspondingly, the number of partner agency users with online access to AUSTRAC information increased from 3,081 on 30 June 2010 to 3,406 on 30 June 2014. Source: *AUSTRAC annual report 2013–14*

AUSTRAC's functions

8. As Australia's financial intelligence unit (FIU) and anti-money laundering and counter-terrorism financing (AML/CTF) regulator, AUSTRAC's purpose and functions complement those of the wider Australian law enforcement and intelligence community.

9. The agency's purpose is to protect the integrity of Australia's financial system and contribute to the administration of justice through its expertise in countering money laundering and the financing of terrorism.

10. In its FIU role, AUSTRAC collects analyses and transforms financial information into 'actionable intelligence' for its Australian law enforcement partners. This intelligence is used to investigate and prosecute serious criminal activity, including money laundering, terrorism financing, organised crime and tax evasion.

11. The requirement to develop and enrich its financial intelligence guides AUSTRAC's use of regulatory powers and its engagement with its regulated population. AUSTRAC regulates industry compliance with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules), and the *Financial Transaction Reports Act 1988* (FTR Act). In addition, the following regulations have been made:

    - the *Anti-Money Laundering and Counter-Terrorism Financing (Iran Countermeasures) Regulation 2014*, and
    - the *Financial Transaction Reports Regulations 1990*.

12. Among AUSTRAC's functions are those described at section 176A(3B) of the Data Retention Act:

    - enforcement of the criminal law
    - administering a law imposing a pecuniary penalty
    - administering a law relating to the protection of the public revenue.

    These functions are described in more detail below.

Enforcing criminal law

13. AUSTRAC performs a unique and pivotal role in gathering, analysing and enhancing financial intelligence used in the detection and investigation of criminal activity.

14. AUSTRAC disseminates intelligence to 40 domestic partner agencies and exchanges financial intelligence with 75 counterpart international FIUs.

15. AUSTRAC establishes investigative links by connecting money to crime. By investigating and analysing the financial transactions associated with a suspected criminal activity, AUSTRAC supports its partner agencies to identify new criminal targets, locate hidden proceeds of crime and provide the supporting information necessary for law enforcement agencies to obtain warrants and secure prosecutions.

16. AUSTRAC's role in enforcing criminal law is evidenced by the agency's participation and contribution to a number of high-profile joint task forces led by its law enforcement and other partner agencies. The table below gives examples of AUSTRAC's participation and involvement in cross-agency government task forces and forums designed to combat Australia's most serious criminal threats, including organised crime.

Table 1: Examples of AUSTRAC's contribution to cross-agency task forces and forums

Examples of **groups/forums and other initiatives**:
• Australian Criminal Intelligence Forum
• Australian Crime Commission Board member
• Various forums under organised crime national framework – Joint Management Groups (JMG), Joint Analyst Groups (JAGs) Operations Coordination Group (OCG)
• New South Wales Crime Commission/NSW Police – Organised Crime Squad
• National Border Targeting Centre
• Border Management Group
• National Criminal Intelligence Fusion Capability (led by the Australian Crime Commission)
• Fraud and Anticorruption Centre (led by the AFP)
Examples of **task forces**:
• Project Wickenby
• Eligo National Task Force
• Western Australian Joint Organised Crime Taskforce
• Trade Union Corruption Taskforce
• Waterfront task forces – Jericho, Trident, Polaris
• Serious Financial Crime Taskforce (AFP/ATO)

17. In 2013–14 AUSTRAC intelligence supported:
    - 20,931 Australian Taxation Office (ATO) cases, resulting in $358.3 million in tax assessments raised
    - 321 Department of Human Services (Centrelink program) reviews achieving total annualised savings of $5.7 million
    - 260 significant investigations undertaken by AUSTRAC's other law enforcement, intelligence, human services, regulatory and revenue partner agencies.
18. More recently, AUSTRAC:
    - completed 813 intelligence disseminations to partner agencies, including 532 suspected terrorism financing matters to partners in the national intelligence community (for the period 1 July 2014 to 31 March 2015)
    - undertook 703 financial intelligence exchanges with overseas FIU (for the period 1 July 2014 to 28 April 2015).
19. Examples of the types of investigations AUSTRAC information is currently assisting include:
    - counter-terrorism
    - significant drug trafficking
    - transnational organised crime
    - money laundering and proceeds of crime

- illegal tobacco
- child exploitation offences
- tax evasion
- internet romance scams
- boiler room scams.

20. Access to telecommunications data is critical in ensuring that AUSTRAC can continue to produce relevant and effective financial intelligence. This access will also drive efficiencies and improved use and allocation of resources across law enforcement agencies, as it will allow AUSTRAC to more effectively provide its partner agencies with complete, comprehensive and timely financial intelligence.
21. **Appendix B** to this report includes example case studies where AUSTRAC intelligence has contributed to investigations into serious crime. Each case also exhibits criminal use of telecommunications channels.

Administering a law imposing a pecuniary penalty

22. AUSTRAC has a total regulatory population of more than 14,250 entities enrolled on the Reporting Entities Roll spanning the finance, gambling and alternative remittance sectors. These entities have a range of AML/CTF compliance and transaction reporting obligations.
23. The AML/CTF Act includes a suite of enforcement powers which include administrative, civil penalty and criminal sanctions where a reporting entity's breach is systemic and impacts on the overall AML/CTF compliance systems of the reporting entity or on the objectives of the AML/CTF regime.
24. These powers include the ability for the AUSTRAC CEO to issue infringement notices and apply to the Federal Court for injunctions or civil penalty orders. Under the AML/CTF Act, the maximum civil penalty for a body corporate is $17 million and the maximum for an individual is $3.4 million. Criminal sanctions can also apply for non-compliance and criminal matters detected by AUSTRAC can be referred to the AFP or Commonwealth Director of Public Prosecutions.
25. Since 2013 AUSTRAC has issued four infringement notices to reporting entities for serious contraventions of the AML/CTF Act:
    - 29 April 2015 – MoneyGram Payment Systems Inc. – $336,600
    - 9 December 2014 – ClassicBet Pty Ltd – $10,200
    - 19 December 2014 – MoneyGram Payment Systems Inc. – $122,400
    - 19 November 2013 – Ria Financial Services Australia Pty Ltd – $225,600.
26. In addition to the infringement actions, AUSTRAC has also taken a range of other enforcement actions against entities relating to contraventions of AML/CTF requirements including:
    - issuing ten (10) enforceable undertakings
    - giving two remedial directions
    - giving one notice requiring the appointment of an external auditor to assess compliance
    - refusing seven applications for registration on the Remittance Sector Register (RSR)
    - imposing conditions on the registration of 17 persons on the RSR

- suspending the registration on the RSR of two persons
- cancelling the registration on the RSR of nine persons
- issuing 3163 remedial requirements (since July 2010) for breaches of AML/CTF Act.

27. AUSTRAC's financial intelligence also supports the operations and objectives of a range of Commonwealth, state and territory partner agencies which administer laws that impose monetary or financial penalties. A list of AUSTRAC's designated partner agencies is at **Appendix A**.

Administering a law relating to the protection of the public revenue

28. AUSTRAC performs a critical role in the protection of public revenue and this function has been strengthened through recent initiatives. In the 2014 Budget, the Australian Government announced that it would replace the cost recovery arrangements previously administered by AUSTRAC (known as the AUSTRAC Supervisory Levy) with an industry contribution to fund AUSTRAC's regulatory and intelligence functions.
29. The AUSTRAC industry contribution is a charge on reporting entities that will recover the costs of AUSTRAC's functions as AML/CTF regulator and FIU. The industry contribution arrangements commenced in the 2014–15 financial year onwards.
30. Legislation to enable AUSTRAC to recover the costs of its activities from its regulated entities is set out in two Acts:
    - *Australian Transaction Reports and Analysis Centre Industry Contribution Act 2011*
    - *Australian Transaction Reports and Analysis Centre Industry Contribution (Collection) Act 2011.*
31. The levy and any late payment penalties are debts owing to the Commonwealth of Australia and can be recovered by the AUSTRAC CEO.
32. AUSTRAC also supports important revenue protection measures by its partner agencies, as demonstrated by its role in two recent Federal Budget initiatives.
33. The 2015 Budget included a $21 million initiative, to be funded over four years, between AUSTRAC and the Department of Human Services (DHS), aimed at protecting the integrity of Australian taxpayer dollars and reducing the risk of erroneous or fraudulent welfare payments.

section 47E

35. The 2013 Federal Budget included an investment of $77.8 million over four years to the Australian Taxation Office (ATO) to improve individual and micro enterprise taxation compliance by expanding data matching with third-party information. A component of this funding was to strengthen AUSTRAC's reporting systems to provide enhanced reporting to the ATO revenue collection outcomes.
36. Overall, this measure is estimated to have a gain to revenue of $610.2 million over the forward estimates period. In underlying cash terms, the estimated increase in receipts is $431.7 million.

Matters for consideration by the Attorney-General

Telecommunications data assisting AUSTRAC to perform its functions

37. The AML/CTF Act imposes ongoing transaction reporting obligations on reporting entities, and requires individuals to report cross-border movements of physical currency and bearer negotiable instruments.

38. The AML/CTF Rules prescribe the details that reporting entities must report to AUSTRAC for each transaction type, which generally include the following information

- the business details of the reporting entity
- the customer of the designated service
- the individual conducting the transaction (if different from the customer)
- the recipient of the proceeds of the transaction (if different from the customer)
- details of the transaction, including cash and other components.

39. It is common for reporting entities to include a customer's contact details, such as phone number or email address, in the information provided to AUSTRAC, particularly where other prescribed customer information is absent.

section 47E

43. Similarly, telecommunications data would support AUSTRAC in detecting and investigating fraud and other criminal activity facilitated using false names.

44. Historically, and under the Data Retention Act, AUSTRAC has not only been prohibited from accessing telecommunications data, but also from receiving this data from its partner agencies which have and will continue to have access to this information.

45. The prohibition from receiving telecommunications data has had negative impacts on AUSTRAC's operations, particularly when seeking to enhance the quality and utility of the financial intelligence it provides to its partners and in regulating the alternative remittance sector.

46. AUSTRAC's work as Australia's specialist FIU will be impacted if it does not have the same access to telecommunications information as its counterpart law enforcement and national security agencies, 22 of whom are classified as 'criminal law enforcement agencies' under the Data Retention Act.

Compliance with the Australian Privacy Principles

47. As an Australian Government Agency, AUSTRAC is bound by the Australian Privacy Principles (APPs) in the *Privacy Act 1988*, which regulate how agencies collect, use, disclose, and store personal information, including sensitive information, and how an individual may access and correct records containing their personal information.

48. AUSTRAC recognises the importance of protecting privacy and personal information, respects individuals' rights to privacy and complies with all Privacy Act requirements on the collection and management of personal information.

49. In addition to the Privacy Act, the AML/CTF Act has extensive provisions supporting privacy. The Act imposes:

    - requirements on reporting entities regarding their disclosure of certain classes of information – for example, there are strict limitations on disclosure of information related to suspicious matter reports (SMRs)
    - a criminal offence regime on all AUSTRAC and designated agency staff for unauthorised disclosure of AUSTRAC information
    - requirements that all non-Commonwealth designated agencies agree to comply with the APPs as a condition of their access to AUSTRAC information, and this requirement is backed up by written agreements entered into by AUSTRAC as part of the authorisation process
    - requirements that the AUSTRAC CEO be satisfied that foreign countries who receive AUSTRAC information have appropriate arrangements to protect the confidentiality of the information, and appropriate controls on use of the information
    - requirements on the AUSTRAC CEO to have regard to privacy in carrying out his functions and to consult with the Information Commissioner in relation to privacy functions.

50. AUSTRAC established the AUSTRAC Privacy Consultative Committee to provide advice to the AUSTRAC CEO. The Privacy Consultative Committee comprises representatives of the following:

    - Australian Privacy Foundation
    - Victorian Council of Civil Liberties (Liberty Victoria)
    - Australian Consumers' Association
    - Australian Taxation Office (ATO)
    - Australian Crime Commission
    - Australian Federal Police
    - Attorney-General's Department (AGD)
    - the Office of the Australian Information Commissioner.

51. AUSTRAC has memorandums of understanding (MOUs) in place with its designated partner agencies which provide a comprehensive framework governing their access to, and use of, AUSTRAC information.

52. AUSTRAC also negotiates a written exchange instrument with foreign FIUs or regulators with which it shares information. Each exchange instrument consists of a comprehensive framework and parameters for information exchange with that particular foreign jurisdiction.

53. Access to stored communications will assist with AUSTRAC's privacy compliance by:

- enhancing the AUSTRAC CEO's ability to confirm the identity of a subject where multiple individuals have the same name, thus eliminating 'false positives'
- ensuring the quality of personal information used by AUSTRAC is in accordance with APP10 – Quality of personal information.

54. Access to stored communications would improve the quality of AUSTRAC's information both domestically and internationally, for the purpose of protecting the integrity of Australia's financial system and contributing to the administration of justice.

AUSTRAC's processes and practices

section 47E

57. AUSTRAC operates under the secrecy and access provisions of Part 11 of the AML/CTF Act, which regulate access to, and the disclosure of, AUSTRAC information. These provisions are designed to ensure that the sensitive information under AUSTRAC's control is secure and protected from unauthorised disclosure and generally provide for:
    - the circumstances under which an AUSTRAC official is permitted to disclose information or documents obtained under the AML/CTF Act
    - the controls around the access and use of AUSTRAC information by prescribed government agencies. For example, AUSTRAC can restrict access to certain types of data (e.g. telecommunications information) so that it is only accessed by authorised partner agencies and authorised personnel.
    - the sharing of AUSTRAC information with the government of a foreign country and with foreign law enforcement and intelligence agencies.

    Part 11 also prohibits the use or disclosure of AUSTRAC information under most circumstances in court or tribunal proceedings.

58. The *Law Enforcement Integrity Commissioner Act 2006* was amended in 2012 to extend the jurisdiction of the Australian Commission for Law Enforcement and Integrity to include AUSTRAC. This oversight is complemented by AUSTRAC's own comprehensive integrity framework, which includes a Fraud and Corruption Control Plan and associated training for staff.

Public interest

59. AUSTRAC's intelligence contributes directly to public interest considerations including:
    - national security
    - the prevention and detection of crime and fraud
    - the economic wellbeing of Australia..

[2] Including more than 415 million financial transaction and suspicious matter reports as of January 2015. In the year 2014, AUSTRAC received more than 91 million financial transaction reports from its regulated population.

Access to stored communications would enhance AUSTRAC's ability to perform its functions in support of the public interest.

National security

60. AUSTRAC provides unique financial intelligence – including intelligence sourced from international counterparts – to assist Commonwealth, state and territory partners to better understand, identify, investigate and disrupt the financing of terrorism. AUSTRAC also makes targeted use of its regulatory and enforcement powers as part of counter-terrorism investigation strategies. The *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* has enabled the sharing of sensitive AUSTRAC information as part of broader financial intelligence operations.

61. As detailed in its 2015 Portfolio Budget Statements, AUSTRAC will continue improving its counter-terrorism capability to conduct complex financial intelligence analysis to:

- provide national intelligence community partners with a better understanding of the financial enablers of terrorism
- support counter-terrorism investigations and help prevent the funding of terrorism, including Australian foreign fighters.

62. To support these objectives, AUSTRAC will develop new financial data collection, matching and transformation capabilities to significantly enhance its capacity to process the information it receives from reporting entities.

section 47E

66. In September 2014, as part of whole-of-government measures to respond to the threat of terrorism, including threats posed by Australians involved in foreign conflicts, the

Australian Government announced additional funding of $20 million for AUSTRAC to invest in new business processes and systems to improve AUSTRAC's capacity to undertake complex financial intelligence analysis.

67. The overarching objective of this initiative is to better understand the financial enablers of terrorism and to build a new data capture and transformation system. This system will develop AUSTRAC's analysis of financial data by utilising the enhanced customer identifier information (including metadata) included in reports of international funds transfers submitted by reporting entities.

68. Enabling AUSTRAC to access telecommunications data will further the objectives of this Budget initiative.

Protection and detection of crime and fraud – money remittance sector

69. Access to stored communications would assist AUSTRAC to investigate serious contraventions of the law and assist in the prevention and detection of crime and fraud. An example is AUSTRAC's regulatory and intelligence oversight of the regulated money transfer/remittance sector.

70. The remittance sector has been identified by both domestic law enforcement and international AML/CTF bodies as a high-risk for money laundering and terrorism financing activity. This is reflected in its classification as a 'high-risk' sector in the National Threat Assessment on Money Laundering conducted in 2011.

71. The sector is the target of the Eligo National Task Force, established by the Australian Crime Commission in December 2012. Under Eligo, the ACC and AUSTRAC partner with other law enforcement bodies to 'take coordinated collective action against high-risk alternative remittance and IVTS (informal value transfer systems) operators to reduce their adverse impact on Australia and its national well-being'. Further, the task force seeks to professionalise the remittance sector and make it an unattractive target for misuse by serious and organised crime.

72. Eligo has disrupted several global money laundering and drug networks and achieved significant outcomes including (as of 31 March 2015):

    - seizures of more than $65.9 million cash, and illicit drugs and precursors with a combined estimated street value of more than $925.7 million
    - restraint of more than $46 million worth of assets
    - arrest of 289 people on 673 charges
    - disruption of 49 serious and organised criminal groups/networks
    - identification of more than 285 targets previously unknown to law enforcement
    - the referral to the ATO of 139 serious and organised crime targets, which has resulted in 35 reviews/audits with total of $48.5 million in liabilities being raised.

73. Access to telecommunications data by AUSTRAC would assist AUSTRAC and its Eligo partners to uncover complicit operators in the remittance sector undertaking money laundering and other serious crimes.

74. Complicit remitters use telephone, fax, text message or email to facilitate 'underground' international funds transfers. These underground transfers bypass the formal banking system and transaction reporting requirements and are therefore invisible to AUSTRAC and other authorities. This includes where transfers of illicit funds are commingled with legitimate transfers being undertaken by commercial money transfer businesses.

Economic wellbeing of the country

75. To complement the work of the multi-agency task force Project Wickenby, which concludes June 2015, the Government announced in its 2015 Budget the establishment of the Serious Financial Crime Taskforce to lead a Commonwealth operational response to high-priority serious financial crimes. The taskforce will comprise officers from AUSTRAC, the Australian Taxation Office, the AFP, Australian Crime Commission, Commonwealth Director of Public Prosecutions, and the Australian Securities and Investments Commission. The task force agencies will receive $127 million over four years to combat high-priority financial crimes.

76. AUSTRAC will provide support to partner agency investigations and prosecutions, primarily though intelligence and data sharing and analytical and intelligence support. For example, AUSTRAC will analyse funds flows relating to serious financial crime to provide a taskforce effectiveness measure and detect financial service providers enabling serious financial crime.

77. AUSTRAC has been a key partner of Project Wickenby's efforts preventing people from promoting and participating in the misuse of secrecy jurisdictions and an integral partner in the fight against tax evasion, tax avoidance and crime.

78. At 31 March 2015, Project Wickenby has recouped $946.53 million, including:

- $372.60 million in improved voluntary compliance
- $571.18 million in cash collections
- $2.75 million in other money recouped under proceeds of crime
- 76 people charged with indictable offences and 46 convictions.

79. AUSTRAC's objectives and functions support national priorities to protect Australia's security, apprehend criminals, protect the integrity of our financial markets and maximise revenue collection. The capacity to access and use telecommunications data is essential in AUSTRAC fulfilling its objectives and supporting these national priorities. Enhancing financial intelligence with telecommunications data ensures that the agency retains its frontline role in working with its partner agencies protecting the integrity and standing of Australia's financial system and economy.

Appendix A – AUSTRAC designated agencies (June 2015)

In working to combat money laundering and terrorism financing, it is vital for AUSTRAC to develop and maintain effective relationships with its designated partner agencies.

AUSTRAC's designated agencies under the AML/CTF Act are listed below:

Australian Government agencies

- Australian Commission for Law Enforcement Integrity
- Australian Competition and Consumer Commission
- Australian Crime Commission
- Australian Customs and Border Protection Service
- Australian Federal Police
- Australian Prudential Regulation Authority
- Australian Secret Intelligence Service
- Australian Securities and Investments Commission
- Australian Security Intelligence Organisation
- Australian Taxation Office
- Department of Human Services
- Defence Imagery and Geospatial Organisation
- Defence Intelligence Organisation
- Defence Signals Directorate
- Department of Foreign Affairs and Trade
- Department of Immigration and Citizenship
- Foreign Investment and Trade Policy Division, Department of Treasury
- Inspector-General of Intelligence and Security
- Office of National Assessments

State and territory agencies

- ACT Revenue Office
- Corruption and Crime Commission (WA)
- Crime and Misconduct Commission (Queensland)
- Independent Commission Against Corruption (NSW)
- New South Wales Crime Commission
- Northern Territory Police
- NSW Office of State Revenue
- NSW Police Force
- Office of State Revenue (Queensland)
- Office of State Revenue (WA)
- Police Integrity Commission (NSW)
- Queensland Police Service
- Revenue SA
- South Australia Police
- State Revenue Office (Tasmania)
- State Revenue Office (Victoria)
- Tasmania Police

- Territory Revenue Office (NT)
- Victoria Police
- Victorian Independent Broad-based Anti-Corruption Commission (IBAC)
- Western Australia Police

Appendix B – AUSTRAC case studies involving the use of telecommunications

The sanitised case studies in this appendix are examples of how AUSTRAC intelligence contributes to investigations into serious crime and terrorism financing.

Each case exhibits criminal use of telecommunications, including for arranging drug importations, laundering proceeds of crime and financing overseas terrorist groups. Access to the evidence trail left by telecommunications would greatly assist AUSTRAC in cases such as these.

Access to telecommunications data is especially important where criminals attempt to exploit the anonymity afforded by unregulated financial channels, such as digital currencies (see Case 1). In cases such as this, where criminals misuse new and/or unregulated channels or products, it creates an information gap for AUSTRAC and its partner agencies – a gap AUSTRAC could resolve through the judicious use of telecommunications data.

Case 1 – Suspect used black market website and digital currencies for drug trafficking

AUSTRAC assisted an investigation which led to the arrest of a suspect who used a digital currency to purchase, import and sell illicit drugs through a black market website.

Australian law enforcement intercepted a number of packages containing cocaine and methylenedioxymethamphetamine (MDMA), sent to from Germany and the Netherlands.

AUSTRAC information identified that the suspect had transferred funds via banks to an online digital currency exchange based overseas, enabling him to purchase an amount of digital currency.

Law enforcement executed a search warrant on the suspect's home computers, mobile phones and a number of stun guns.

Analysis of the suspect's mobile phones identified text messages thought to be associated with drug trafficking. The suspect's computers revealed he maintained an online account with a black market website which allowed him to purchase and sell illicit drugs and conduct transactions using a digital currency.

The suspect was sentenced to three years and six months imprisonment. He was also fined AUD1,000 for possessing controlled weapons.

Case 2 – Australian terror suspects sent funds to Somalia to support terrorist group

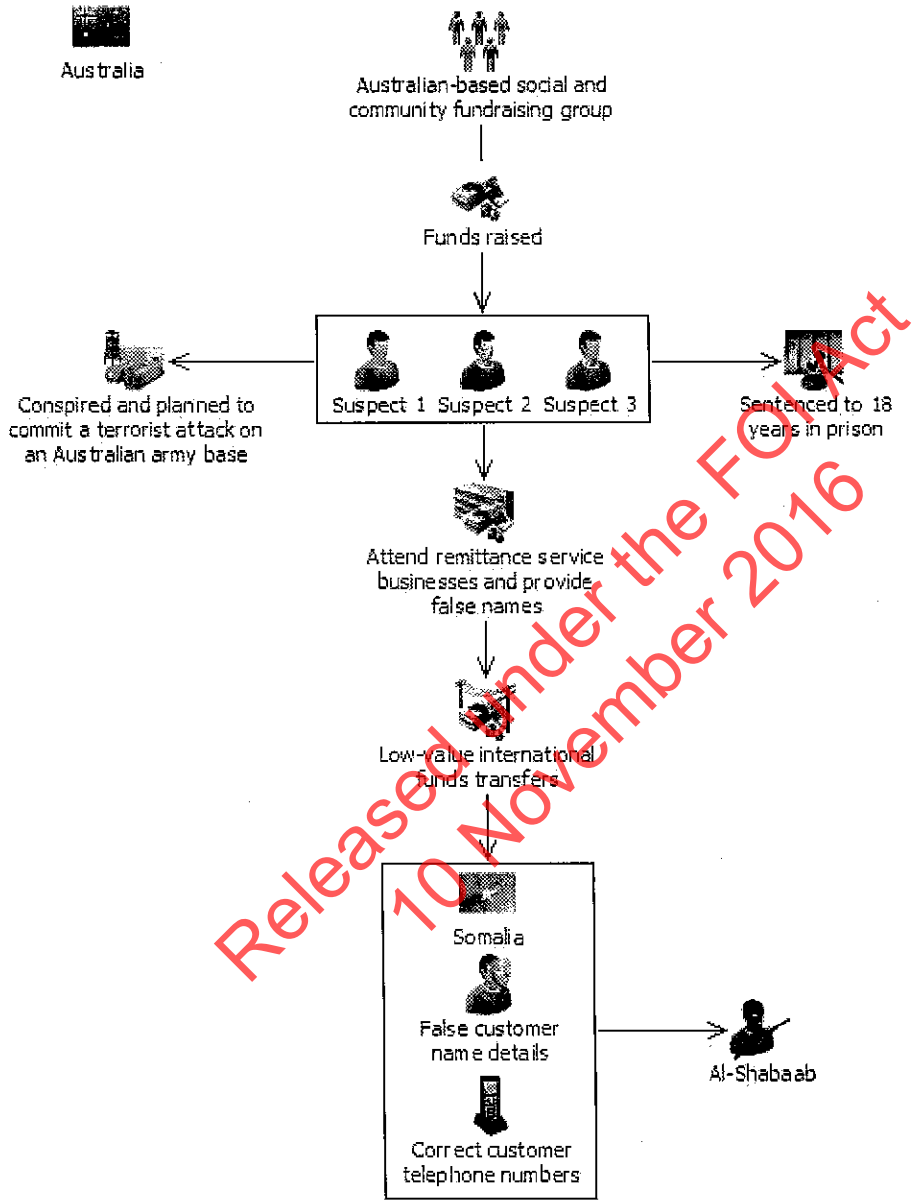
A joint-agency investigation led to the arrest of five suspects on charges of conspiring to commit a terrorist attack on an Australian army base. Investigations revealed the group had sent funds destined for use by the Somalia-based terrorist group, al-Shabaab. The group had also facilitated travel for Australian-based supporters to attend overseas military training camps. Funds remitted offshore by the suspects did not go directly to al-Shabaab but to entities linked to al-Shabaab's activities in Somalia.

The suspects sent the funds via remittance service businesses, often giving false names for the overseas beneficiary customer to obscure the money trail. However, the suspects used the correct telephone numbers for the overseas customers, and these numbers were recorded in the international funds transfer instruction (IFTI) reports submitted to AUSTRAC by the remitter. Investigating officers concluded that the suspects were careful to use the

customers' correct phone numbers to ensure the funds arrived safely in Somalia. In this case, the IFTI reports provided valuable intelligence to corroborate other information or consider leads in the investigation.

Three of the suspects were found guilty of conspiring to plan an Australian-based terrorist attack and sentenced to 18 years jail to serve 13 years and six months.

Figure 2 – Australian terror suspects sent funds to Somalia to support terrorist group



Case 3 – 'Cuckoo smurfing' used in million dollar money laundering scheme

AUSTRAC disseminated information to a law enforcement partner agency, which sparked an investigation into a widespread money laundering syndicate. The syndicate, which operated in multiple states across Australia, used a sophisticated money laundering technique known as 'cuckoo smurfing'.

The syndicate misused the bank account of a legitimate export company based in Australia and international funds transfers sent from a Pakistani customer to the export company.

Over a 15-month period members of the syndicate conducted 217 cash deposits totalling AUD2.1 million into the Australian bank account of the export company. A total of 196 of these cash deposits were 'structured' deposits, primarily in amounts between AUD8000 and AUD9500, conducted at bank branches throughout Sydney and Melbourne.

The syndicate members were careful to provide the bare minimum of personal information when undertaking deposits. Nevertheless, 18 bank deposit receipts examined by law enforcement revealed identifying characteristics such as phone numbers. These identifiers lead to the identification of some of the depositors.

Case 4 – Canadian drug importations hidden in foot spas

A law enforcement investigation foiled efforts by an Asian organised crime group to import hundreds of kilograms of drugs – cocaine, ecstasy and crystal methamphetamine ('ice') – into Australia. Authorities intercepted several shipping containers from Canada and seized drugs worth more than AUD31 million, hidden in foot spas.

AUSTRAC financial transaction information helped identify the Canadian company believed to have supplied the foot spas and the Australian companies that were to receive the importations.

A Canadian national suspected of being the main organiser of the importations conducted low-value international funds transfers from Australia to Vietnam while visiting Australia. The associated international funds transfer reports revealed a mobile phone number used by the suspect when undertaking the transactions.

This same phone number was also provided by a second suspect when sending low-value transfers to beneficiaries in Vietnam through a remittance dealer based in Australia. This second suspect was subsequently arrested for overseeing one of the drug importations.

As result of the investigation, three suspects were sentenced to jail terms ranging from five-and-half years to 19 years.

Case 5 – Suspicious transactions revealed Colombian cocaine importations

Australian authorities arrested and charged two suspects for importing nearly AUD2 million worth of cocaine into Australia from South America. The international investigation involved Australian, German and New Zealand law enforcement agencies. AUSTRAC information assisted the investigation by linking the suspects to the purchase of the drugs and the methods used to pay for and import the drugs.

The suspects, originally from New Zealand, flew to Australia to organise the cocaine importation. They transferred funds to Colombia to pay for the cocaine which was hidden in industrial equipment to be shipped to Australia. They also spent over AUD4,000 on arrangements with couriers, mobile phones and apartments, to avoid detection.

German and Australian law enforcement agencies cooperated to intercept the packages in Germany. Listening devices were attached to the packages which were monitored by Australian law enforcement until they were delivered to the suspects in Australia. Telephone calls made by the suspects were also intercepted in which they were heard discussing the drug shipments.

The suspects were arrested at their Australian hide-out and charged with attempting to possess a marketable quantity of an unlawfully imported border control drug. The suspects

were each sentenced to 11 years imprisonment, with one to be deported to New Zealand upon release.

GUIDE TO ENFORCEMENT AGENCY STATUS

1. From 13 October 2015 any agencies wanting ongoing access to historical telecommunications data must be listed as an 'enforcement agency', unless already listed as a 'criminal law enforcement agency' in section 110A of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.*

2. The Attorney-General's Department is seeking advice from agencies that consider they require direct access to telecommunications data to fulfil their functions.

3. This guide is designed to assist organisations seeking to be included as an enforcement agency. It is not intended as legal advice or determinative of legal rights or obligations.

Changes introduced by the Data Retention Act

4. Prior to passage of the Data Retention Act, any authority or body with functions involving enforcing the criminal law, enforcing a law imposing a pecuniary penalty or a law protecting the public revenue was deemed to be an 'enforcement agency'. Those authorities and bodies could authorise access to historical telecommunications data.

5. The law has now changed to ensure that access to historical telecommunications data is limited to agencies with a clear operational need and appropriate privacy safeguards.

6. Section 110A of the Act lists specific *criminal law enforcement agencies* that are also deemed to be enforcement agencies.

7. Section 176A of the Data Retention Act provides that the Attorney-General may declare a body or authority to be an enforcement agency if satisfied on reasonable grounds that its functions include:

   (a) enforcement of the criminal law; or

   (b) administering a law imposing a pecuniary penalty; or

   (c) administering a law relating to the protection of the public revenue.

8. When doing so, the Attorney-General must have regard to:

   (a) whether the ability to access data under authorisations would be reasonably likely to assist the authority or body in performing those functions

   (b) whether the authority or body is required to comply with the Australian Privacy Principles, an equivalent binding scheme or has agreed in writing to do so

   (c) whether the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of an enforcement agency, and

(d) whether the declaration would be in the public interest.

Next steps

9. If your organisation has in interest in enforcement agency status, you will need to write to the Attorney-General's Department by **12 June 2015**. Emails to ESPB@ag.gov.au are preferred.

10. While there is no prescribed form, all requests should be in writing. The information you provide should be accurate, credible and relevant.

11. You will need to provide sufficient detail in your request to address each of the factors in section 176A of the Data Retention Act.

12. Your request should also:

    (a) include references to the legislation underpinning relevant powers exercised by your organisation

    (b) demonstrate why your organisation cannot perform its functions using alternative information sources (i.e. without access to telecommunications data)

    (c) include evidence and examples of past use of historical telecommunications data, and

    (d) include details of a nominated contact officer.

13. The Attorney-General's Department will contact your organisation's nominated officer to confirm receipt of your request.

14. Any organisations not listed in the legislation as 'criminal law enforcement agencies' or temporarily declared to be an enforcement agency may wish to engage with law enforcement about being able to continue to be able to access this data for its investigative or operational purposes.

Guidance on the factors in section 176A of the Data Retention Act

What is a 'body' or 'authority'

15. A *body* is any identifiable group of persons (whether a body corporate or not). An *authority* is an organisation (generally public or quasi-public) that controls a subject matter area, zone or certain activities. This can include Commonwealth, State and Territory Departments, local government bodies, statutory authorities or quasi-government organisations

When will an organisation have a function of 'administering a law'?

16. 'Administering a law' may involve managing processes associated with its application or having charge of, or being involved in, its execution.

17. An organisation will generally have a 'function' of 'administering a law' where a body or authority is:

    (a) responsible for carrying legislation into effect (implementing a law or series of laws or provisions under a statute)

    (b) involved in activities supporting the ongoing application of legislation or key aspects of legislation, or

    (c) monitoring and ensuring compliance with the administrative requirements associated with the application of a law.

18. Examples include:

    (a) ensuring that obligations imposed by the legislation are performed by officials within the organisation or by members of the public, and

    (b) setting up and operating any associated administrative processes and mechanisms for ensuring the objects of the legislation are carried out. For example, a Commonwealth Department described in the Administrative Arrangement Order as the Department responsible for administering a statute would have the function of administering that statute.

19. Administering a law may also include where a body's sole function in respect of a law is to investigate possible breaches.

What is meant by 'enforcement of the criminal law'?

What is meant by 'enforcement'?

20. 'Enforcement' can extend not only to the apprehension of persons who commit an offence, but also to activities directed at investigating whether an offence has been committed (i.e. detection/investigative activities). It includes:

    (a) the process of investigating crime and prosecuting criminals, or

    (b) gathering intelligence about crime to support the investigating and prosecuting functions of law enforcement agencies.

What is the 'criminal law'?

21. Criminal law extends to laws that make certain conduct an offence punishable by fine or imprisonment such that criminal proceedings (i.e. proceedings prosecuted by Crown prosecutors and heard in criminal courts) can be taken. Criminal law can be State, Territory or Commonwealth-based.

What is meant by a 'pecuniary penalty'?

22. A 'pecuniary penalty' simply means a monetary or financial penalty designed to deter a person and others or an entity from breaching the law. For example:

    (a) the penalty payable in respect of an infringement notice or

    (b) the penalty payable in respect of civil contraventions of relevant provisions.

23. Pecuniary penalties generally include penalties for breaches of Commonwealth or State/Territory laws that are not criminal or that impose a penalty which is an administrative alternative to prosecution (they are often referred to as civil or administrative penalty provisions and are usually accompanied by a penalty unit payable).

24. Pecuniary penalties are generally paid to a Commonwealth, State/Territory body instrumentality (rather than the victim/affected party) and are imposed by civil (non-criminal) courts following a civil trial. They are designed to punish and deter unlawful behaviour, rather than compensate those directly affected by that behaviour.

25. Notably, the Explanatory Memorandum to the Data Retention Act provides that pecuniary penalties for the purposes of the statutory test in s 176A are not intended to encompass small-scale administrative fines, like minor library late-return fines.

What is meant by 'protection of the public revenue'?

26. The concept of 'public revenue' includes State and Territory revenue in addition to Commonwealth revenue. Lawful obligations charged on a regular basis such as taxes, levies, rates and royalties involve the protection of the public revenue. Occasional charges, such as fines, do not.

27. Protecting the public revenue would also include the activities of agencies and bodies undertaken to ensure that those lawful obligations are met; for example routine collection, audits, investigatory and debt recovery actions.

28. Protecting the public revenue would not include activities aimed at identifying and eliminating inefficient but lawful spending of public monies.

29. The term 'revenue' is not intended to be limited to incoming monies from taxation but could also extend to monies to which a Commonwealth, State or Territory government instrumentality has a right, or monies which are due to it.

Privacy

30. An enforcement agency must either comply with the Australian Privacy Principles, comply with a comparable framework or agree in writing to be bound to such a scheme.

Does your organisation comply with the Australian Privacy Principles?

31. The Australian Privacy Principles in the *Privacy Act 1988* include obligations relating to the:

(a) management of personal information (APP 1 and APP 2)

(b) collection of personal information (APP 3 – APP 5)

(c) use or disclosure of personal information (APP 6)

(d) security standards for retained information (APP 11)

(e) access to personal information (APP 12)

32. Guidelines and fact sheets are available via the Office of the Australian Information Commissioner. See:

(a) http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

(b) http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf

33. For organisations bound the *Privacy Act 1988*, your response should indicate how its processes and procedures are compliant with those principles.

Does your organisation comply with a privacy framework comparable to the APPs?

34. Your response should outline:

(a) how the binding scheme (for example, the State or Territory equivalent privacy legislation) under which your organisation operates provides protections commensurate with those which apply under the Australian Privacy Principles,

(b) identify the mechanism(s) that scheme provides to monitor privacy protections; and

(c) the provisions under which individuals can seek recourse for any alleged misuse of their personal information.

Does your organisation propose to agree in writing to comply with a privacy scheme?

35. If your organisation proposes to undertake to comply with other arrangements to provide similar or equivalent levels of privacy protection, then:

(a) the CEO or a senior officer within your organisation should provide a written undertaking affirming your organisation's compliance with a privacy protection scheme, and

(b) the undertaking should specify the scheme of arrangement to which the undertaking relates and its key privacy protection features, specifically the protection it confers in relation to personal information disclosed to carriers and how this is consistent with the Australian Privacy Principles or State/Territory equivalent privacy principles.

Public interest

36. Your response should identify the public interest considerations which weigh in favour of your organisation being given access to telecommunications data. Rather, the meaning of 'public interest' derives its content from the subject matter and the overarching context.

37. Some matters which may engage public interest considerations include, but are not limited to:

(a) public health and safety;

(b) national security;

(c) the prevention and detection of crime and fraud; and

(d) the economic wellbeing of the country.

Further information

39. The full text of the Data Retention Act is at: http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r5375_third-reps/toc_pdf/14242b01.pdf;fileType=application%2Fpdf

40. The Explanatory Memorandum to the Data Retention Act is available at http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001/upload_pdf/14242b01EM.pdf;fileType=application%2Fpdf