

Parliamentary Joint Committee on Law Enforcement
Inquiry into the impact of new and emerging ICT

SUBMISSION BY AUSTRAC

January 2018

The Australian Transaction Reports and Analysis Centre (AUSTRAC) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into the impact of new and emerging information and communications technology (ICT), with particular reference to:

- a) Challenges facing Australian law enforcement agencies arising from new and emerging ICT;
- b) The ICT capabilities of Australian law enforcement agencies;
- c) Engagement by Australian law enforcement agencies in our region;
- d) The role and use of the dark web;
- e) The role and use of encryption, encryption services and encrypted devices; and
- f) Other relevant matters.

This submission responds specifically to criteria a), b) and c) above by providing examples that reflect some of the key challenges AUSTRAC faces, the ICT capabilities that have been developed and the significant relationships forged with domestic and regional partners.

By collaborating with the fintech and regtech industries in particular, AUSTRAC has gained greater insight into the transformation of the financial sector through digitisation, leading to a strong understanding of the risks, threats and vulnerabilities in this environment.¹ This collaborative approach has ensured that AUSTRAC is well positioned to understand and respond to new and emerging ICT, particularly where it is exploited to facilitate money laundering and terrorism financing (ML/TF).

We also acknowledge the opportunities and benefits that can be achieved through innovation and new and emerging ICT as evidenced by the Fintel Alliance public-private partnership (see 'Capabilities' section below for detail).

We note that the Attorney-General's Department has also made a submission in relation to this inquiry, to which AUSTRAC has contributed.

About AUSTRAC

Financial intelligence unit

As Australia's financial intelligence unit (FIU) and anti-money laundering and counter-terrorism financing (AML/CTF) regulator, AUSTRAC'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.

In its FIU role, AUSTRAC collects, analyses and transforms financial information into actionable intelligence for our partners in law enforcement, national security and intelligence, regulatory and border protection roles; and for our international counterpart FIUs. This financial intelligence assists with investigating, disrupting and prosecuting serious criminal activity, including money laundering, terrorism financing, organised crime and tax evasion.

¹ For more information on the fintech and regtech industries, please see <https://fintechaustralia.org.au/learn/> and <https://www.thewealthadvisor.com/article/what-regtech>

AML/CTF supervisory role

As AML/CTF regulator, AUSTRAC supervises more than 14,000 Australian businesses with their compliance and transaction reporting obligations under 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). These businesses range from major banks, the financial services sector and casinos, to single-operator businesses in the money remittance and gambling (that is, pubs and clubs) sectors.

In some circumstances, AUSTRAC seeks to enforce compliance with these Acts through mechanisms that are more formal. Recent enforcement action initiated by AUSTRAC includes Tabcorp² and the Commonwealth Bank of Australia.³

The role and value of AUSTRAC financial intelligence

A key obligation imposed on regulated businesses (also known as 'reporting entities') is the collection and reporting to AUSTRAC of financial transaction and suspicious matter reports. The AML/CTF Act provides that the following must be reported to AUSTRAC:

- threshold transaction reports (TTRs): reporting entities must report transactions involving the transfer of physical currency or e-currency of \$10,000 or more
- international funds transfer instruction (IFTI) reports: reporting entities must report the details of an instruction to or from a foreign country to transfer money or property
- suspicious matter reports (SMRs): for example, where in the provision of a service to a customer, the reporting entity suspects on reasonable grounds that information provided may relate to an offence against the Commonwealth, state or territory, or may relate to money laundering, terrorism financing or proceeds of crime
- cross-border movement (CBM) reports: travellers must declare cross-border movement of physical currency of AUD10,000 or more (or foreign currency equivalent) and, on request, cross-border movement of bearer negotiable instruments of any amount.

AUSTRAC has entered into written memoranda of understanding on the dissemination of financial intelligence with 45 domestic partner agencies and 89 international counterpart FIUs. Each year AUSTRAC disseminates thousands of pieces of actionable intelligence to its partners, including suspicious matter reports and detailed analysis reports, for use in their investigations and operations.

The actionable financial intelligence disseminated by AUSTRAC contributes to hundreds of investigations and related seizures of criminal proceeds and revenue by law enforcement, national security, revenue authorities, border protection and other agencies in Australia and overseas.

As evidence of this key role, during the period 2016-17, AUSTRAC received a total of 112,533,536 transaction reports and SMRs, which represents an increase of 11 per cent on the previous year. This increase in the number of reports, and analysis of same, supports AUSTRAC and its partners to meet intelligence outputs. To complement the 2.7 million searches of the AUSTRAC database by partner agencies, AUSTRAC also disseminated a total of 783 intelligence products to its law enforcement and national intelligence partners to assist in identifying new and emerging risks and threats.

² <http://austrac.gov.au/media/media-releases/record-45-million-civil-penalty-ordered-against-tabcorp>

³ <http://austrac.gov.au/media/media-releases/austrac-expands-civil-penalty-case-against-cba>

AUSTRAC works closely with law enforcement and national security intelligence agencies, primarily on counter-terrorism and counter-terrorism financing matters, as well as other national security priorities. AUSTRAC's intelligence has played an important role in identifying new suspects linked to terrorism in Australia and overseas, and has improved Australia's understanding of high-risk funds flows to Syria, Iraq and surrounding countries.

a) Challenges facing Australian law enforcement agencies arising from new and emerging ICT

Digital currencies, digital identities and cybercrime are three key challenges AUSTRAC faces in relation to new and emerging ICT. This section outlines some of the work AUSTRAC undertakes in response to these challenges.

Digital currencies (for example, bitcoin)

The rise of digital currencies provides a challenge for AUSTRAC, both as a regulator and FIU, and for our partners. As defined by the Financial Action Taskforce (FATF)⁴ a 'digital currency' is:

[A] digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the digital currency.⁵

While digital currencies offer the potential for cheaper, more efficient and faster payments, the associated ML/TF risks are well documented. Key risks include:

- greater anonymity compared with traditional non-cash payment methods
- limited transparency because transactions are made on a peer-to-peer basis, generally outside the regulated financial system
- different components of a digital currency system may be located in many countries and subject to varying degrees of AML/CTF oversight.

With the risks in mind, digital currencies provide an attractive way to facilitate payments relating to illicit activities such as money laundering, tax avoidance, and purchasing illicit goods and services.

In response to these risks, on 7 December 2017 the Australian Parliament passed the [Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017](#) (Amendment Act), which includes the first phase of reforms to Australia's AML/CTF framework. This is in response to the recommendations of the [Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations](#) (the Report). On 29 April 2016 the former Minister for Justice, the Hon Michael Keenan MP, tabled the Report in the Parliament.

In accordance with a recommendation in the Report, the Amendment Act introduced reforms to the AML/CTF Act to close a regulatory gap (and indeed respond to a new and emerging technology) by regulating digital currency exchange providers.

It is important to note that the Report also recommended that the AML/CTF Act be amended to ensure that digital wallets are comprehensively captured by AML/CTF regulation. Despite the foregoing, it was subsequently found that it was neither feasible nor practical to regulate digital

⁴ The FATF is the lead inter-governmental body that develops and promotes the implementation of international anti-money laundering and counter-terrorism financing (AML/CTF) standards – refer to the following link: <http://www.fatf-gafi.org/home/>

⁵ Financial Action Task Force, *FATF Report: Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, 2014, p. 4, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (accessed 13/12/2017).

wallets at this time. AUSTRAC in conjunction with the Department of Home Affairs is closely monitoring other AML/CTF jurisdictions to ascertain how this matter will be addressed because at this time there is no AML/CTF regulation of digital wallets for digital currencies.

The Amendment Act received Royal Assent on 13 December 2017. The AML/CTF compliance and reporting obligations will come into effect for digital currency exchange service providers from the date of Proclamation, which is expected to be 3 April 2018. Digital currency exchange providers will be required to:

- enrol and register on the Digital Currency Exchange Register maintained by AUSTRAC, and provide prescribed registration details
- adopt and maintain an AML/CTF program to identify, mitigate and manage the ML/TF risks they may face
- identify and verify the identities of their customers
- report suspicious matters and transactions involving physical currency that exceed \$10,000 or more (or foreign equivalent) to AUSTRAC
- keep certain records related to transactions, customer identification and their AML/CTF program, for seven years.

AUSTRAC has been working collaboratively with digital currency exchange providers to gain greater insight into the operation of the sector and assist in preparation for the implementation of the regulatory reforms. To facilitate the introduction of the regulatory reforms, AUSTRAC has formed several joint working groups with the sector, based on the following themes:

- *Education and Sector Specific Guidance:* The focus of this working group is to develop a broad education strategy targeting the sector on AML/CTF compliance and reporting obligations. The working group is also jointly developing complementary guidance using a question and answer approach, combined with worked examples to explain and outline the nature, detail and context of the AML/CTF obligations.
- *Transaction and Suspicious Matter Reporting:* The limited transparency of transactions involving digital currency poses a range of challenges in identifying and managing ML/TF risk. This working group is examining options to strengthen and expand the identifying information that can assist AUSTRAC's partner agencies. For example, the inclusion of common identifiers that are accepted by digital currency service providers, which are not used by other components of AUSTRAC's regulated population.
- *Digitisation and Interoperability:* Given the online nature of digital currencies, this working group is exploring opportunities for better reporting and interaction in identifying, managing and mitigating ML/TF risk.

Digital identities

Customer identification requirements are the cornerstone of the AML/CTF framework. If implemented well by businesses, this can have a profound impact on mitigating risks of identity fraud, or aid in its detection and disruption.

AUSTRAC is aware that not only organised criminal groups, but also terrorists, exploit and abuse personal and corporate identity requirements to disguise the true ownership and control of funds. This provides challenges for both businesses and law enforcement. Following from the inclusion of digital currency providers under the AML/CTF framework, AUSTRAC is exploring unique identifiers

(for example, IP addresses) that can be used for 'know your customer' (KYC) purposes and provide subsequent intelligence value.

Fraudulent identities have been used to commit criminal activity such as: welfare, tax and other fraud against government agencies; gaining unauthorised access to sensitive information or facilities; and concealing other criminal and terrorism financing activities including the commissioning of terrorist acts. The costs associated with detected identity crime incidents can be substantial. For example, the Attorney-General's Department's *Identity Crime and Misuse in Australia* 2016 report estimates that identity crime costs Australia \$2.2 billion annually.⁶

AUSTRAC is supportive of a whole-of-government approach to revisit identity and identity verification with a strategic view to understand the environment for government, industry and individuals. This comes in the wake of substantial technological developments and innovation including digital identities, biometrics, privacy preserving computing, distributed ledger technologies, artificial intelligence and big data analytics. It is considered that there may be significant benefits that could flow to individual consumers, regulated businesses, national security and law enforcement agencies in protecting the Australian community and economy by better mitigating identity related abuses.

Cybercrime

AUSTRAC established a Cyber Operations team in August 2016 to focus on discovering the financial aspects of cybercrime. The team is assisting partner agencies to combat the cybercrime threat to Australia's financial sector.

Through this team, AUSTRAC focuses on the investigation into cyber threats to the financial sector, the financials of cyber-enabled crime and cyber terrorism financing threats. New technologies, such as distributed ledger technology (that is, blockchain) analysis tools, and more effective partnerships, are helping AUSTRAC stay abreast of developments and providing opportunities for new investigative methods.

Fintel Alliance (explained in more detail below) is providing support to law enforcement operations targeting money mule activity, and collaborating with industry to enrich knowledge of financial indicators. For example, in 2016-17 the Fintel Alliance identified two previously undetected, suspected money mule controllers. AUSTRAC referred intelligence to law enforcement partners, recommending they be assessed for proceeds of crime action.

Fintel Alliance joint operational projects explored the Australian Cyber Online Reporting Network (ACORN) dataset. This was matched against Fintel Alliance partner data holdings to identify leads, financial methodologies and trends, and the financial footprint of Australian cybercrime. Fintel Alliance partners promptly acted upon the financial intelligence produced from this activity. This boosted collective efforts to harden the financial system and improve capability to detect, deter, investigate and prevent financial-related crime and terrorism.

Future considerations

Maintaining pace with emerging and existing technologies remains the key challenge for regulators and law enforcement. AUSTRAC is committed to keeping abreast of new and emerging technologies, particularly around online payment systems, and methods that include communication applications to facilitate financial transactions. There are increasing challenges for regulatory reach and

⁶ See AGD website <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Trends-in-Identity-Crime.aspx>

community/individual protection when these businesses are domiciled off-shore yet service the Australian community. The emergence of illegal offshore wagering is an example.

In addition to understanding technologies used for nefarious purposes, AUSTRAC is dedicated to ensuring the regulatory framework, including relevant legislation, is contemporary and assists businesses to keep pace with changes in technology, while ensuring AML/CTF obligations are met. For example, changes to reporting requirements and information collection can reduce the regulatory burden for businesses, while maximising the intelligence value for law enforcement efforts.

b) The ICT capabilities of Australian law enforcement agencies

In recent years, AUSTRAC has developed and implemented several unique initiatives to advance the ICT capabilities of not only itself as an FIU and regulator, but also of its partners in their day-to-day operations. Fintel Alliance, the Business Research and Innovation Initiative (BRII), and the Innovation Hub are three examples of ICT capabilities that have changed the way AUSTRAC and its partners respond to the challenges faced and embrace the opportunities that new and emerging ICT bring to the AML/CTF space.

Access to and the use of telecommunications data as a ‘criminal enforcement agency’ under the *Telecommunications (Interception and Access) Act 1979* is one ICT capability that AUSTRAC considers would provide additional value to its financial intelligence unit operations—particularly having the ability to link financial transactions temporally with communications activity. AUSTRAC understands well the importance of privacy and security, through its protection of collected personal and commercially sensitive financial information. AUSTRAC would apply this same rigour should consideration be given to its use and protection of metadata. Additional safeguards will arise through the Government’s endorsement of Recommendations in the 2017 Independent Intelligence Review to expand oversight of agencies that comprise the National Intelligence Community.

Fintel Alliance

A key development in AUSTRAC’s capabilities was establishing Fintel Alliance—a public-private partnership through a national centre of excellence for financial intelligence. Fintel Alliance was officially launched on 3 March 2017. It brings together government, industry, and international partners in a collaborative approach to countering ML/TF through enhanced information and intelligence-sharing arrangements across participants.

Since it commenced operations, Fintel Alliance has strengthened its operational base. It currently comprises private and public partners including AUSTRAC, the Australian Federal Police, the Department of Home Affairs, NSW Police, Australian Taxation Office, Australian banks (ANZ, Commonwealth Bank, Macquarie Bank, National Australia Bank and Westpac), HSBC, Western Union and PayPal. The UK National Crime Agency has also joined Fintel Alliance, and AUSTRAC is in discussions with other potential international partners.

An Operations Hub was established where government and industry intelligence analysts work side-by-side in joint operational projects, and share information in near real-time. Three projects were undertaken to establish operations: examining the Mossack Fonseca matter (Panama Papers), identifying and profiling online money mules, and enhancing the use of ACORN data.

Fintel Alliance applies risk modelling across the financial data contained in more than 100 million transaction reports that AUSTRAC receives from industry each year. This produces valuable financial

intelligence to help identify and investigate serious crimes affecting Australia. An 'Alerting Initiative' is also underway to enable the discovery of financial crime risks through joining disparate and distributed data silos in a privacy-preserving manner.

Fintel Alliance also provides the opportunity for experts across national and international authorities, industry, academia and technology stakeholders, to collaborate and learn from one another to better inform and strengthen Australia's responses to ML/TF risks.

Business Research and Innovation Initiative

One of the unique partnerships for AUSTRAC arose through BRII, conducted by the Department of Industry, Innovation and Science. BRII encourages the development of innovative solutions for government policy and service delivery challenges.⁷

In 2017, AUSTRAC and the Australian Criminal Intelligence Commission were the joint winners, responding to the challenge 'tracking the effect and value of information products'. Work is underway to produce proof of concepts over the next 12 months.

Innovation Hub

AUSTRAC broadened its engagement and collaboration efforts to include academic and private industry to explore, experiment and share knowledge around new technologies. For example, current partnerships are progressing privacy-preserving data analytics, data lake and automated data integration, open source and visual analytics, blockchain smart contracts, platform as a service, and data visualisation tools.

AUSTRAC is also exploring open-source tools to promote the culture of sharing and collaboration in a real-time environment. This allows consistency in technology development through co-design and source code transparency, speed in deployment and most importantly, scalability and quick experimentation with new technology. The focus on scalable architecture allows AUSTRAC to use several tools and platforms to improve both financial intelligence and regulatory functions, while exercising fiscal responsibility.

Big data experimentation and enterprise analytics are also enabling: real-time tracking of ML/TF transactions across borders and institutions; matching of identities across many deliberate or incidental variations; ability to spot outliers from the norm and find networks; and matching of transactions to typologies. The creation of data lakes, while retaining appropriate security and privacy sensitivities, can bring broad data sets to the desktops of analysts.⁸ For example, through its data-matching capability, AUSTRAC has assisted the Department of Human Services to generate savings from detected instances of welfare fraud of AUD17.25 million.⁹

AUSTRAC is developing a proof of concept for a smart contract¹⁰ for KYC obligations on the blockchain, for IFTI reports and TTRs. The changing nature of technology and potential uptake of

⁷ More information on BRII: <http://www.innovation.gov.au/page/business-research-and-innovation-initiative>

⁸ For more information on 'data lakes' see <https://www.datamation.com/big-data/data-lake.html>

⁹ Australian Government, AUSTRAC Annual Report 2016 – 17, p.11

¹⁰ A smart contract is an innovation independent of distributed ledger technology (DLT), but can be utilised by the distributed nodes of a DLT system and are considered particularly relevant to the technology given the anti-tampering features of DLT. It enables the automated execution of logic based on events, alerts, or value or state of a parameter external (but accessible) to the ledger and is a contract written in computer code rather than legal language, which are executed when certain code observable criteria are satisfied.

blockchain applications and platforms across the financial services sector, present significant opportunities for AUSTRAC in collaboration with reporting entities, research institutes and law firms, to lead the way in understanding the use of smart contracts for automating AML/CTF KYC obligations. This work will also strengthen AUSTRAC's understanding and ability to consider smarter regulatory options as recommended in the statutory review of the AML/CTF Act, Rules and regulations. In addition, it has the potential to provide a number of benefits to AUSTRAC and its regulated population, which include:

- increased cost savings to industry by embedding a large proportion of the KYC and transactional reporting requirements in code
- increasing the speed of KYC processes
- developing a rules-based process for transaction reporting
- reducing regulatory burden

c) Engagement by Australian law enforcement agencies in our region

In addition to the Fintel Alliance capability mentioned above, AUSTRAC is actively involved in domestic and international engagement to enhance resilience to money laundering, terrorism financing and serious crime, with ICT being a key component.

International Community of Experts

AUSTRAC is a leading member of the International Community of Experts (ICE) Forum, joining heads of technology and innovation from Indonesia, Malaysia, Philippines, Brunei, Thailand and Singapore. The forum aims to identify and analyse emerging trends, understand current and future challenges in identifying and solving financial crime, and develop methodologies, viable solutions and algorithms to enhance AML/CTF detection and response in our region.

The ICE Forum officially formed after the inaugural Counter-Terrorism Financing (CTF) Summit in Sydney in 2015, hosted by AUSTRAC. To date, the Forum has focused on developing a real-time information-sharing model, and development of an 'Open FIU' that will set standards and best practices for its members.

Codeathons

AUSTRAC has facilitated and contributed to several codeathons to promote innovation in the development of policy solutions. For example, in the lead-up to the 2017 CTF Summit in Malaysia, AUSTRAC hosted a codeathon bringing together 69 participants from 11 different countries. Participants ranged from FIUs, fintech and regtech communities, financial institutions and private individuals (such as software developers, programmers, analysts, designers, engineers and students).

The participants were brought together to solve common challenges: 'Where is the money?'; 'Who are you?'; and 'Help your community'. Initiatives such as these not only provide the avenue for policy collaboration, but bring together disparate sectors to produce innovative solutions including prototypes.

Fintel Alliance Smarter Regulation program

To complement AUSTRAC's engagement strategies, a smarter regulation program is underway where all aspects of AUSTRAC's regulatory model are being co-designed by industry and AUSTRAC.

This high level of collaboration aims to bring about efficiencies and reduce the regulatory burden experienced by some entities. This is done by developing and implementing a modern, innovative, collaborative and sustainable regulatory model that is capable of delivering the necessary AML/CTF outcomes.

Of particular interest is ongoing and timely review of the operating context to ensure readiness for future AML/CTF risks and threats to Australian industry and community. This forms the driver for AUSTRAC's compliance and enforcement activities. As part of this process, AUSTRAC is refining its risk model in consultation with the regulated population, which will become the foundation of its enhanced supervision model. Compliance operations have been realigned to ensure compliance and supervisory activities are commensurate with: the level of identified ML/TF risk, and the nature, size and complexity of the businesses or corporate groups and AUSTRAC's supervisory priorities.

Fintechs and regtechs

Since late 2015, AUSTRAC has been actively engaging private sector entities operating in the innovation and financial technology spaces. AUSTRAC has a dedicated web page that enables fintechs and other start-ups to engage directly and understand the compliance and reporting obligations under the AML/CTF regime. The web page has received more than 70 enquiries since its introduction in late 2016. To complement the fintech web page, in 2017 AUSTRAC established a compliance team solely focused on understanding and engaging with third-party regtech developers and AML service providers.

Engagement with these sectors has assisted AUSTRAC to generate regulatory intelligence and maximise regulatory efficiencies, through improved communication with, and education of, reporting entities. The early and direct engagement strategies AUSTRAC is undertaking with these industries are easing the regulatory burden. For example, following direct engagement with AUSTRAC, one business decided not to proceed with its e-commerce platform until it had reached a maturity to cope with compliance activities.

There have also been many opportunities for AUSTRAC through this direct engagement, including:

- better understanding new technologies and business models used by the regulated population
- improved engagement and capturing of information via the customer identification and compliance reporting framework
- more accurate and regular provision of actionable intelligence to our law enforcement partners.