Australian Government
Department of Home Affairs

Joint Submission to the Senate Select Committee on Financial Technology and Regulatory Technology

Department of Home Affairs

The Australian Transaction Reports and Analysis Centre

January 2020

Table of Contents

Preface

The Department of Home Affairs and the Australian Transaction Reports and Analysis Centre (AUSTRAC) (hereafter 'the Portfolio') welcome the opportunity to provide this joint submission to the Senate Select Committee on Financial Technology and Regulatory Technology. The content of this submission is unclassified and suitable for public release.

This submission engages the Terms of Reference of the inquiry, and specifically addresses certain questions posed in Sections One (National Competitiveness) and Two (Specific sectoral issues – FinTech and RegTech in Australia) of the Issues Paper.

Section One: National Competitiveness Issues

Regulation – Anti-Money Laundering / Counter-Terrorism Financing

There are currently more than 15,000 Australian businesses (known as 'reporting entities') who are regulated by AUSTRAC under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the associated AML/CTF Rules and the *Financial Transaction Reports Act 1988* (FTR Act). Reporting entities range from the major banks, the financial services sector and casinos, to single-operator businesses in the money remittance, digital currency exchange and gambling sectors (including pubs and clubs).

The AML/CTF Act obliges reporting entities to take preventative measures to identify, mitigate and manage the risk of their services being used for money laundering or terrorism financing. These AML/CTF Act obligations require reporting entities to:

- enrol with AUSTRAC
- in the case of remitters and digital currency exchanges, register with AUSTRAC
- develop and maintain an AML/CTF program designed to identify, mitigate and manage money laundering or terrorist financing risks
- conduct customer due diligence
- report certain cash transactions, international funds transfers and suspicious matters, and
- keep certain records.

AUSTRAC, as Australia's Financial Intelligence Unit (FIU), collects, analyses and transforms the financial information gathered from reporting entities into actionable intelligence for law enforcement, national security and regulatory partners, as well as for 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.

Financial technology (hereafter FinTech) businesses may offer services that are regulated under Australia's AML/CTF regime. These include:

- lending (for example, Afterpay Pty Ltd and Zip Money Pty Ltd)
- issuing a debit card,
- money remittance and foreign exchange (for example, Finch or TransferWise), and
- digital currency exchange.

AUSTRAC has closely collaborated with FinTech start-ups who are involved in the digital transformation of the financial services and payments sectors in Australia. This engagement has aimed to recognise opportunities for the application of regulatory safeguards in the development of transformative technologies and to ultimately reduce the regulatory burden on current and future regulated businesses.

AUSTRAC also engages with FinTech partners through the Fintel Alliance. AUSTRAC has established an Innovation Hub which allows Fintel Alliance partners to collaborate, co-design and test new and innovative technology solutions. The Innovation Hub is currently:

- developing a secure information-sharing and collaborative analytics environment that supports the flow of information between Fintel Alliance partners, while protecting commercial and privacy obligations, and
- automating alert capabilities – developing a set of integrated capabilities where detection and reporting of intelligence matters moves to real-time.

Since 2015, AUSTRAC, together with other regional FIUs, has hosted an annual CTF Summit, which has engaged both the FinTech and Regulatory Technology (hereafter RegTech) sectors. The most recent CTF Summit, hosted by the Philippines in November 2019, was attended by over 350 representatives including attendees from the FinTech and RegTech sectors.

Equally, the Minister for Home Affairs, the Hon Peter Dutton MP, hosted a global No Money for Terror Conference in Melbourne on 7-8 November 2019. This Conference had more than 65 delegations including 23 Ministers, representatives from 15 international bodies including the United Nations, Financial Action Task Force (FATF) and FATF-Style Regional Bodies, as well as representatives from 28 private sector and not-for-profit organisations. The 2019 Conference built on the important work of the inaugural 'No Money for Terror' Ministerial Conference in 2018, hosted by France. A copy of the outcomes of the Conference are attached to this Submission. This was an example of FinTech and RegTech sectors coming together to work on terrorist financing issues.

Australia's AML/CTF framework is largely supportive of RegTechs, businesses that utilise or create technology to enhance regulatory processes, due to the risk based nature of the AML/CTF Act. However, this framework requires that RegTech solutions be adaptable and tailored for each client. Although this requirement is time consuming and requires more engagement between the RegTech business and the reporting entity to ensure the solution is fit for purpose, AUSTRAC encourages RegTechs to develop better regulatory outcomes and efficiencies for reporting entities in meeting their reporting obligations under the AML/CTF regime.

AUSTRAC conducts comprehensive engagement with the RegTech sector to ensure that RegTechs are developing products which meet the compliance needs of reporting entities. This engagement allows AUSTRAC to provide guidance to the sector on common compliance issues and risks that could benefit from technical solutions. AUSTRAC engages with the RegTech sector through collaborative events and one-on-one sessions with individual RegTech businesses.

RegTechs appear to be alive to the opportunities for growth in the Australian market (such as the recently introduced Consumer Data Right), and are increasingly adopting blockchain technologies in their solutions (for example, Identitii). There is also an active awareness of privacy obligations and emerging consumer concerns.

Sharing of Know Your Customer Checks

Reporting entities must obtain a range of independent and reliable information from customers to ensure they meet the general obligation to 'Know-Your-Customer' in the AML/CTF Act. They are also required to keep up to date information on their customers so they know if there has been any change in circumstances or business activities. These obligations enable reporting entities to better understand their

customers and their financial dealings so that they can determine the ML/TF risk posed by each customer and efficiently manage this risk.

Given the intensive and ongoing nature of these obligations, customer due diligence represents a major component of AML/CTF compliance costs. The Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019 (the Bill), which is currently before the Parliament, is aiming to reduce these costs with reforms to customer due diligence reliance.

Reliance is currently only available in limited circumstances; however, if passed by Parliament, the Bill would expand the provisions to allow reliance on customer due diligence procedures undertaken by a broader range of Australian and foreign entities. These reforms are in line with The Open Banking Review, which recommended that the outcomes of a customer due diligence procedure required by the AML/CTF Act should be shared as part of the new framework.

International Funds Transfer Instructions

There are two types of IFTIs under the AML/CTF Act which require different reportable details.

An IFTI-E is a type of electronic funds transfer instruction (EFTI) for transferring money on behalf of a customer which is sent to or received from another country. In an IFTI-E, the transfer instruction is carried out or passed on electronically, and is within the same financial institution or between financial institutions, such as banks, building societies or credit unions.

An IFTI-DRA is an instruction to transfer money or property to or from another country under a designated remittance arrangement (DRA) where either the entity accepting the instruction from the customer or the entity making the money or property available is not a financial institution.

To conduct their business, financial institutions exchange substantial amounts of information with their customers and among themselves. Such exchanges only work if the sender and receiver of a message have a common understanding of how to interpret this information. SWIFT (Society for Worldwide Interbank Financial Telecommunication) is the standard for messaging in correspondent banking, foreign exchange and documentary credits. Over 11,000 financial institutions around the world use this standard to exchange millions of messages per day over the SWIFT network.

In 2019, SWIFT announced that it is migrating to a revised messaging framework under ISO 20022 (a global, free and open standard that can be used by anyone and implemented on any network) to take effect from November 2021. Accordingly, AUSTRAC is currently working with SWIFT, the Reserve Bank of Australia and the banking sector to ensure there is a smooth transition to ISO 20022 for the Australian payments system while maintaining a workable solution for IFTI reporting to AUSTRAC.

The Portfolio understands that many FinTech businesses utilise ISO 20022 for IFTIs and some use blockchain technology applications, whereby smart contracts are used to transfer funds internationally. The Portfolio is interested in hearing about other message formats and business models used by FinTech businesses to see how it can best support the sector and reduce regulatory burden while enhancing efforts to combat and disrupt money laundering and terrorism financing.

Section Two: Specific Sectoral Issues

Regulatory Settings in Australia

Do current regulatory settings support the growth of local FinTech and RegTech companies in Australia?

The Portfolio supports the development of technology-based solutions and opportunities driven by the agility and pace of change of the FinTech and RegTech sectors. A key driver of this activity is the technological and competitive neutrality of the portfolio's legislation, such as the AML/CTF Act. As a result of these guiding principles, reporting entities of all sizes are adopting cost effective technological solutions and exploring open data, digital identity and artificial intelligence. The value of these technological developments is underpinned by the willingness of industry partners to support collaborative efforts to drive innovation and change how we protect against, detect and deter financial crime across the financial system.

How should Australia take a prominent role in supporting and developing international blockchain standards?

The Portfolio is of the view that blockchain technologies have the potential to significantly reduce the costs of compliance and regulation imposed on reporting entities. This technology can ensure that sensitive financial data used for intelligence purposes remains secure, transparent and protected through the use and application of encryption. AUSTRAC participates in Standards Australia's Technical Working Committee on Blockchain and Distributed Ledgers, and actively engages with members of that committee including Blockchain Australia on issues related to blockchain technologies and digital currencies.

The Portfolio has also actively participated in the development of international standards that relate to Virtual Asset Service Providers (similar to digital currency exchange providers in the Australian context) through its membership of the Financial Action Task Force (FATF). The FATF is an intergovernmental organisation that sets international standards to combat money laundering and the financing of terrorism and proliferation. Australia is a founding member of the FATF and its engagement with the organisation feeds directly into our domestic regime. Following the new international standards being adopted, the Portfolio is also part of a FATF sub-group that is working hand-in-hand with industry to ensure that the new obligations can be effectively implemented.

Since 2016, the FATF has engaged in constructive dialogue with the FinTech and RegTech sectors, with the overall objective of supporting innovation in financial services, whilst addressing the regulatory and supervisory challenges posed by emerging technologies. One of the FATF's current products being developed in the FinTech space is guidance which will help governments, financial institutions and other relevant entities apply a risk-based approach to the use of digital identity for CDD purposes.

How can public sector data be made more accessible and useful for FinTech and RegTech companies seeking to deliver innovative products and services?

The Portfolio supports the private sector by providing technology services to enable CDD checks and prevent identity crime, such as fraud against financial institutions. These identity matching services assist entities in verifying their customers' identities and if applicable meeting their obligations under the AML/CTF Act. The services are provided through secure, online systems that operate 24 hours a day, seven days a week.

Document Verification Service

The Document Verification Service (DVS) checks whether the biographic information on an individual's provided identity document matches the original, as recorded on government databases. The DVS is currently used by more than 120 Commonwealth, state and territory agencies and more than 1100 private sector organisations. The financial sector are already key users.

Face Verification Service

The Commonwealth, with the States and Territories, is developing the Face Verification Service (FVS) as a means to address known vulnerabilities in name-based checking systems like the DVS. The FVS compares an individual's face against the image used on their identity documents. In service delivery contexts, this would be done with the individual's consent.

The *Identity-matching Services Bill 2019*, which is currently before Parliament, seeks to implement the 2017 Intergovernmental Agreement on Identity Matching Services (IGA) and operationalize the FVS.

Global Comparisons and Investment

Should Australia seek more formal international FinTech agreements? Are there particular countries that Australia should look to for partnership?

The Portfolio supports international collaboration at multiple levels, including industry and government, and harnessing international fora to build mutual understanding and capability amongst countries in relation to FinTech.

AUSTRAC has established memorandums of understanding with five international regulatory agencies across three countries for the exchange of information to support the regulation and supervision of reporting entities. AUSTRAC also has posted officers located in six countries who engage closely with regulatory and financial intelligence partners to share information on emerging risks, challenges and opportunities. These information sharing mechanisms allow AUSTRAC to share information on regulated FinTechs and RegTechs operating transnationally within partner jurisdictions, and to better understand the FinTech and RegTech space.

Under the UK-Australia FinTech Bridge, referenced in the Committee's Issues Paper, AUSTRAC successfully seconded an officer to the UK's Financial Conduct Authority (FCA). The 6-month secondment allowed AUSTRAC to gain insights into the business processes and operations of a sophisticated regulator, which is leading the way in risk-based AML/CTF supervision, and paved the way for further collaboration with other UK authorities.

Through the secondment, AUSTRAC attended and contributed to roundtable discussions and international conferences on terrorism financing and the sharing of financial intelligence through public-private partnerships, helping to develop links between AUSTRAC and UK agencies and other organisations working on combating financial crime.

In addition, the Department and AUSTRAC engaged with UK authorities on the regulation of digital currencies for AML/CTF purposes, sharing Australia's experience to assist the UK to develop a regulatory model to implement the EU Fifth Money Laundering Directive.

The Department and AUSTRAC also facilitated a visit by the then-Minister for Law Enforcement and Cyber Security to the FCA to discuss approaches to digital currency regulation, innovation in the FinTech sector and the opportunities to reduce costs of AML/CTF compliance presented by RegTech.

Attachment A

Chair's Statement, 2019 'No Money for Terror' Ministerial Conference on Counter-Terrorism Financing

More than 65 delegations including 23 Ministers, representatives from 15 international bodies including the United Nations, Financial Action Task Force (FATF) and FATF-Style Regional Bodies, as well as representatives from 28 private sector and not-for-profit organisations met in Melbourne, Australia, on 7–8 November 2019 for the 'No Money for Terror' Ministerial Conference on Counter-Terrorism Financing. The 2019 Conference built on the important work of the inaugural 'No Money for Terror' Ministerial Conference in 2018, hosted by France, and its Paris Agenda.

The 2019 Conference assessed the evolving global and Indo-Pacific threat environment; built understanding of the key terrorism financing risks, trends and methods; and highlighted best practice from across the globe, between regions and across the public and private sector.

Consistent with United Nations Security Council Resolution 2462 (2019) and the global standards set by the FATF, participants agreed to promote international and regional cooperation and improve capacity to combat the financing of terrorism.

In their discussions, participants addressed and reinforced their commitment to the five key themes of the Conference as follows:

1. *The evolving terrorist threat*
    - Noted that the evolving and significant threat posed by terrorism is global in nature, and the agility and adaptability of terrorists and terrorist organisations to take advantage of emerging situations and weaknesses in counter-terrorism frameworks.
    - Recognised that terrorist organisations rely on funding to sustain their activities and disrupting and preventing financial flows to terrorist is one of the most effective ways to fight terrorism.
    - Recognised that despite the territorial defeat of Daesh (ISIL) in Syria and Iraq, its capacity, including hundreds of millions of dollars generated over that time, to radicalise, recruit and carry violent acts remains a significant threat.
    - Recognised that strategies to counter the evolving terrorist threat need to be holistic and based on mutual cooperation between governments, the private sector and civil society.

2. *Global responses to kidnap for ransom and terrorism financing*
    - Noted that the transnational nature of terrorism and its financing requires a strong and coordinated global response supported by the work of multilateral forums such as the United Nations and the FATF, and underpinned by regional and bilateral partnerships.
    - Recognised that hostage-taking by terrorists to raise funds is a significant source of income for terrorist groups that supports their recruitment and operational capability, and is an incentive for groups to undertake further kidnappings for increased ransoms.
    - Considered international approaches to addressing hostage-taking and underlined the need for information sharing and international cooperation to break the terrorists' business model.
    - Reaffirmed support for international efforts to prevent terrorist and violent extremist exploitation of the Internet, including through the Christchurch Call to Action.

- Agreed to seek further opportunities to provide mutual support to address terrorism financing, including through exchange of information and intelligence, and capability building

3. *Emerging technologies and terrorism financing risks*
   - Noted the positive opportunities for developing countries offered by emerging financial technologies, such as financial inclusion and access to markets.
   - Noted that the opportunities brought by technology may also appeal to terrorists seeking platforms for propaganda, recruitment and raising funds to support malicious activities.
   - Acknowledged the importance of engagement between governments and the private sector to build a shared responsibility to safeguard against abuse by terrorists.
   - Recognised the need to identify emerging risks from new technology platforms and implement effective mitigation measures before widespread use by terrorist actors.
   - Reaffirmed their commitment to implementing the FATF standards and other international requirements in relation to new technologies and virtual assets.

4. *Enhancing public-private partnerships to fight terrorism financing*
   - Recognised the critical role played by the private sector to detect and prevent misuse of financial systems by terrorists.
   - Highlighted the opportunities offered by partnerships between government and the private sector to share and harness existing information and resources to develop strategies combating terrorism financing and other financial crimes.

5. *Preventing the exploitation of not-for-profit organisations for terrorism purposes*
   - Recognised the important role of not-for-profit organisations in providing activities and services that aim to improve the lives of individuals and societies.
   - Noted that terrorist organisations seek the same logistical capabilities as not-for-profit organisations, which makes them potentially vulnerable to abuse by terrorists and terrorist networks.
   - Discussed strategies for strengthening not-for-profit sectors against abuse by terrorists, including through conducting regional and national risk assessments, education and outreach.

Participants warmly welcomed the offer of India to host the next No Money for Terror conference in 2020 and to continue this important work combating terrorism financing.