Australian Government
Department of Home Affairs

Joint Submission of the Department of Home Affairs and the Australian Transaction Reports and Analysis Centre (AUSTRAC) on the third issues paper

Senate Select Committee on Australia as a Technology and Financial Centre

30 June 2021

Table of Contents

Home Affairs and AUSTRAC joint submission on third issues paper 3

- Introduction 3
- The Regulation of Cryptocurrencies and Digital Assets 3
- Issues relating to ‘de-banking’ of Australian Fintechs 5
- Regulation of neobanks 5
- Preventing the misuse of payment features on social media and other platforms by terrorists and violent extremist figures. 6

Home Affairs and AUSTRAC joint submission on third issues paper

Introduction

The Department of Home Affairs thanks the Senate Select Committee on Australia as a Technology and Financial Centre for the opportunity to make a submission on the third issues paper. This submission has been developed by Home Affairs and the Australian Transaction Reports and Analysis Centre. The Australian Federal Police and the Australian Criminal Intelligence Commission were consulted on this submission.

The remit of the Department on the issues raised in the third issues paper is limited. The Department is responsible for administering the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (**AML/CTF Act**), which includes regulation of digital currency exchanges and and a range of other financial services providers, bullion dealers and gambling businesses, some of which may be considered fintechs. The AML/CTF Act is focussed on mitigating money laundering and terrorist financing (**ML/TF**) risks and is therefore one part of Australia's regulatory framework. Consistent with global best practice, as reflected in the inter-governmental Financial Action Task Force (**FATF**) standards, the AML/CTF Act applies a risk-based approach to combating financial crime. The risk-based approach extends to new technologies, for which regulated businesses must understand and mitigate any ML/TF risks prior to adopting them. The risk-based approach represents a balanced approach to new technologies, that minimises restrictions on innovation while also helping to ensure that associated risks are understood and addressed before they can be exploited by criminals.

The Regulation of Cryptocurrencies and Digital Assets

The AML/CTF Act provides a framework to detect and deter ML/TF and provide valuable financial intelligence to revenue, law enforcement and national security agencies.

On 3 April 2018 the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* entered into force, extending the AML/CTF Act to regulate digital currency exchanges (**DCEs**), i.e. businesses that exchange fiat currency for digital currency and vice versa, as these business represent the 'on-ramps' and 'off-ramps' to digital currency. These businesses have a significant role to play in mitigating financial crime risks. The principal obligations for digital currency exchanges are clearly set out in the AML/CTF Act and are supported by AUSTRAC guidance co-developed with industry.

The regulatory obligations imposed on DCEs under the AML/CTF Act are in line with guidance developed by the FATF in 2015. The Act does not regulate cryptocurrency or digital assets, just as it does not regulate fiat currency, such as the Australian dollar. However, following the 2018 amendments, businesses offering DCE services between fiat currency and digital currency (i.e. cryptocurrency), and vice versa are regulated for AML/CTF purposes only. It does not regulate transaction exchanges from digital currency to digital currency.

Cryptocurrencies and Digitial Assets - Risk

The main ML/TF risks associated with digital currencies are:

- greater anonymity or, in some cases, complete anonymity, compared with traditional payment methods
- transfers of digital currency are unconstrained by national borders and difficult to tie to any particular geographic location
- transactions can be made on a peer-to-peer basis, generally outside the regulated financial systems, and
- different components of a digital currency system may be located in different countries and subject to varying degrees of regulatory oversight which can lead to regulatory arbitrage or the use of digital currency moving underground

Current regulation

In response to these risks, the Parliament passed legislation to regulate DCEs and provide law enforcement with vital financial intelligence to combat the criminal exploitation of digital currencies with amendments to the AML/CTF Act coming into force in April 2018.

DCE providers are now required to:

- enrol and register their business with AUSTRAC
- adopt and maintain an AML/CTF program to identify, mitigate and manage the ML and TF risks they may face
- collect information and verify the identities of their customers and undertake ongoing customer due diligence
- report suspicious matters and transactions involving physical currency that exceed $10,000 or more to AUSTRAC, and
- keep records relating to customer identification, transactions, and their AML/CTF program and its adoption.

The registration requirement brings with it powers for the AUSTRAC CEO to refuse an application for registration (thereby preventing a digital currency exchange from operating) or to tailor a business' registration according to its ML, TF or other serious crime risk. The AUSTRAC CEO must consider whether such registration would involve significant risks. As part of this process a number of factors will be taken into account, such as whether the person applying for registration has a criminal history, the kinds of services they will be providing, the legal and beneficial owner and control of the applicant, and the compliance or non compliance of the applicant with the AML/CTF Act or any other law.

The AUSTRAC CEO also has powers to suspend or cancel the registration of a digital currency exchange on similar grounds.

AUSTRAC's remit on regulating digital currency exchanges does not extend to areas outside AUSTRAC's mandate, such as prudential, competition or consumer protection regulation.

The information registered, reported and kept by DCEs is not only beneficial to AUSTRAC, but also to partner law enforcement and regulatory agencies internationally and across the Commonwealth, States and Territories. The data assists agencies to conduct trends and typologies analysis, map transaction histories, track activity with potential links to Darknet marketplaces and determine the risk levels of particular digital currencies. This ultimately supports efforts to prevent the criminal exploitation of cryptocurrencies.

There are more than 455 registered DCE providers in Australia. Since regulations commenced, six businesses have had their registration cancelled and three businesses have been refused registration.

International AML/CTF framework

In June 2019, the FATF set international standards for the AML/CTF regulation of cryptocurrency/digital asset services. These standards built on the 2015 guidance and require AML/CTF regulation beyond the exchange of fiat currency for cryptocurrency or vice versa to also include regulation of:

- exchanges between one or more forms of cryptocurrency
- transfers of cryptocurrency on behalf of customers
- safekeeping or administration of cryptocurrency or instruments enabling control of cryptocurrency (e.g. custodial wallet providers), and
- participation in and provision of financial services related to an issuer's offer and/or sale of cryptocurrency (e.g. Initial Coin Offerings or ICOs).

Businesses providing these services are referred to globally as 'virtual asset service providers' (**VASPs**) and cryptocurrency or digital assets are referred to as 'virtual assets' (**VAs**).

The FATF also includes VASPs under the 'travel rule', which requires financial institutions to include verified information about the originator (payer) and information about the beneficiary (payee) for wire transfers and other value transfers throughout the payment chain. However, technological solutions to enable VASPs to comply with the 'travel rule' are still under development and only beginning to be rolled out globally.

Issues relating to 'de-banking' of Australian Fintechs

The Department is aware that Australian banks, when concerned about the ML, TF and sanctions risks posed by particular customers, sometimes choose to 'de-bank' these customers by withdrawing the provision of financial services. A decision to 'de-bank' a particular customer sits with the relevant financial institution, and the AML/CTF Act does not mandate this practice. The blanket de-banking of whole industry sectors and classes of customers goes beyond the risk-based approach to AML/CTF regulation, which is premised on a customer-by-customer assessment of risk and appropriate mitigation measures, rather than the complete disengagement from risk. At the same time, the AML/CTF Act does not require any financial institution to provide services to particular customers—this would go well beyond the scope of AML/CTF regulation.

As noted above, Australia's AML/CTF regime implements a risk-based approach to regulation. Under this framework, the AML/CTF Act sets out the principal obligations that regulated businesses must meet, such as requirements to identify and verify the identity of their customers and monitor transactions and report suspicious activities. However, it is the responsibility of each business to determine how it can best meet these obligations in line with the AML/CTF Act and Rules.

This approach recognises that each individual business is in the best position to assess the ML/TF risks it faces in relation to the customers, products, and services it offers, and ensure that the procedures and policies put in place are proportionate to those risks.

This approach also recognises that the drivers of de-banking are complex and go beyond ML or TF concerns. A range of additional factors may lead to a customer being de-banked, e.g. commercial considerations; reputational risk; uncertainty associated with new business models; expectations of overseas correspondent banks; and a range of other regulatory requirements relevant to the financial sector.

Regulation of neobanks

Neobanks are financial technology firms that offer online financial services and may not have physical offices or outlets for customer facing interactions. The AML/CTF Act regulates a wide range of financial services under table 1 of section 6 of the Act, including services typically provided by neobanks, such as opening accounts and accepting or transferring money between accounts.

The AML/CTF Act only applies to 'designated services' that satisfy the geographical link test under subsection 6(6) of the Act, such as 'authorised deposit-taking institutions' (ADIs). The geographical link test requires that for an entity that provides a designated service to be regulated under the AML/CTF Act it must be domiciled in Australia. This has posed challenges for the effective regulation of neobanks as they are often based offshore, and their digital nature means they do not require a physical office in Australia in order to provide their services here.

To ensure neobanks are appropriately regulated, the Australian Prudential Regulation Authority (APRA) can designate neobanks as ADIs under the *Banking Act 1959*. This brings these neobanks on-shore, satisfying the geographical link test, and ensuring that they are regulated as ADIs under the AML/CTF Act.

Authorised deposit-taking institutions must:

- enrol with AUSTRAC
- adopt and maintain an AML/CTF program to identify, mitigate and manage the ML/TF risks they may face

- collect information and verify the identities of their customers and undertake ongoing customer due diligence
- report suspicious matters, transactions involving physical currency that exceed $10,000 or more and international funds transfer instructionsto AUSTRAC, and
- keep records relating to customer identification, transactions, and their AML/CTF program and its adoption.

Preventing the misuse of payment features on social media and other platforms by terrorists and violent extremist figures.

Social media and other platforms, both mainstream and alternative, offer payment options that continue to be exploited by violent extremist actors as a means of financing. For example, violent extremists are able to exploit YouTube's "Super Chat" feature, which gives users the ability to receive funds under the pretext of supporters paying to ask questions. The use of this system by violent extremist actors has been observed in the UK and Australia. Patreon and other crowdfunding platforms have been used by violent extremist actors as a means of revenue raising in the US and Australia. E-commerce platforms like Amazon and Redbubble have also been exploited by violent extremists seeking to sell manifestos, t-shirts, and other merchandise.

The majority of platforms already prohibit categories such as 'hate speech' and 'incitement to violence' in their terms of service. Therefore, requiring platforms to prohibit this conduct is unlikely to produce an outcome more beneficial than the status quo. An alternative is to introduce safeguards to the financial models of these platforms to prevent exploitation by terrorists and violent extremists. YouTube introduced one such safeguard by demonetising videos on 'sensitive topics' (removing the ability for those posting these kinds of videos to earn money from the videos and live streams). Following the 2019 Christchurch terrorist attack several platforms introduced livestream safeguards that indirectly limit the use of livestreaming tools for funding.

For consistent and effective safeguarding measures, any safeguard must be adopted as industry best practice.