Chapter 6

Anti-money laundering and counter-terrorism financing regime

6.1 The Attorney-General's Department is currently conducting a statutory review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) which is considering the emergence of digital currencies and whether they should be brought within Australia's AML/CTF regime.[1]

6.2 In this chapter, the committee considers whether digital currencies should be brought within the AML/CTF regime.

The relationship between digital currency businesses and banking services

6.3 A number of concerns were raised by digital currency businesses about access to banking services. One submitter, whose company was considering relocating its business overseas, in part because digital currencies are not regulated under the AML/CTF Act, noted that Australian banks had 'uniformly turned down any involvement with our company, citing the regulatory restraints imposed by the Australian government'.[2]

6.4 The Bitcoin Foundation and Bitcoin Association of Australia expressed concerns regarding the banking industry's approach to digital currencies. They noted:

> The issue of access to banking services is also key to the growth of a local digital currency industry. Blanket classification of all bitcoin businesses and users as 'high risk' customers is both inappropriate and disproportionate.
>
> Banking institutions should have a risk-based approach that is 'tailored to the nature, size and complexity of their business and proportionate to the level of money laundering and terrorism financing risk'.[3]

6.5 The Melbourne Bitcoin Technology Center noted that its members had indicated that many individuals and businesses had experienced discrimination and refusal of service by Australian banks. It proposed legislation to make it an offence for banks to discriminate against a customer on the basis that they are trading or transacting in Bitcoin.[4]

6.6 mHITs Limited, an Australian-based mobile money service company, was concerned that some banks and payment industry members were overstating the risks and downplaying the opportunities that digital currencies represent.[5] It stated:

---

1 The currently regulatory framework and the statutory review were discussed in chapter 2.

2 Name withheld, *Submission 2*, p. [1].

3 Bitcoin Foundation and Bitcoin Association of Australia, *Submission 13*, p. 20.

4 Melbourne Bitcoin Technology Center, *Submission 36*, p. [2].

5 mHITs Limited, *Submission 48*, p. 12.

> By definition new and emerging fintech startups including mHITs represent a potential threat to the status quo. In our 10 years of operation, we have observed the reluctance of Australian banks to embrace innovation outside the comfort of core business products of lending, cards and insurance.[6]

6.7 ASIC's submission noted that it was 'aware of a number of banks taking steps to cease dealing with Bitcoin related businesses due to concerns that digital currency providers pose an unacceptable level of risk to the banks' business and reputation'. ASIC advised that it 'does not have any power to intervene in decisions made by businesses in relation to digital currencies, and considers that this is a matter for the banks and businesses involved'.[7]

6.8 Mr Bezzi, from the ACCC, advised the committee that he was aware of one case in the ACCC's records where a company involved in digital currency transactions had had its accounts closed by a bank, because the business that the company was involved in was not consistent with the bank's policies. Mr Bezzi noted that the ACCC's view is that 'it is up to banks to determine who they want to have as their customers'. He noted further that the ACCC had no evidence of collusion between banks on the issue of providing banking services to digital currency businesses.[8]

6.9 Mr Miller, Bit Trade Australia, explained why his business complies with regulations that do not currently cover digital currencies:

> We are dependent on our banking relationships. We have worked closely with them to achieve a level of comfort for them because we require the ability to bank in the Australian banking sector. We have mirrored their safe harbour practices. We will require you to provide photo ID. We will require you to provide proof of current residential address and date of birth.[9]

6.10 Dr Carmody, Westpac, was supportive of the approach by ADCCA to develop best practices for digital currency businesses that replicate, as far as they are able, the same sorts of safe-harbour obligations that would apply to a bank or to a foreign exchange broker. In his view, this approach assists banks comply with their obligations. He suggested that perhaps the 'sorts of businesses that have been unable to get access to banking accounts are those that have been unable to demonstrate that they are doing that level of due diligence'.[10] He noted that these best practices were not in place when digital currency businesses were first opening up in Australia. He remarked that in the 'early days' the only thing that a customer may have been required to provide in order to purchase Bitcoin was a Bitcoin wallet address and an email address, which did not necessarily identify the customer. He noted:

---

6 mHITs Limited, *Submission 48*, p. 14.

7 ASIC, Submission 44, p. 16.

8 Mr Marcus Bezzi, ACCC, *Committee Hansard*, 7 April 2015, p. 40.

9 Mr Jonathon Miller, Bit Trade Australia, *Committee Hansard*, 7 April 2015, pp. 15–16.

10 Dr Sean Carmody, Westpac, *Committee Hansard*, 7 April 2015, p. 26.

> In that scenario, it is fair to say that there is not a whole lot of know-your-customer going on. A business operating like that would present a real challenge for a bank to provide banking services to because they cannot get satisfied that the underlying business is understood. I think there has been a lot of work from a number of businesses to try and move well beyond that and do the appropriate level of due diligence, which is something we would certainly support.[11]

6.11 Dr Carmody further explained that he supported digital currency businesses coming under the AML/CTF regime. He noted:

> From the point of view of a bank that is providing banking services, if we cannot satisfy ourselves that we can do all the things that we have to do under the legislation to understand the nature of the transactions and what is going on there, it puts us in a very difficult position to be able to provide those banking services. The issues are particularly intense when it comes to moving payments internationally, because obviously we have counterpart banks to deal with globally and they have got their own anti-money-laundering, counter-terrorism-finance obligations, and they will expect us to understand the nature of the payments as well.[12]

6.12 PayPal explained that it had chosen to partner with BitPay, Coinbase and GoCoin as all three companies had taken steps to develop anti-money laundering programs and to ensure they know their customers. PayPal noted that it was proceeding gradually in its approach to digital currencies, so it could ensure that while embracing innovation it remained committed to making payments safer and more reliable for customers. PayPal noted that while all users of PayPal were linked to a specific named PayPal account, with consumer protection for buyers, these standards were not currently required for payments using Bitcoin.[13]

6.13 The ABA noted that banks and other participants that operate within the regulated payments systems have made significant investments in processes and technologies in order to meet their requirements under the AML/CTF regime. As digital currency does not currently come under this regime they are not required to meet these standards and operational requirements.[14] MasterCard maintained that any regulation should include 'obligations to perform KYC [know your customer], maintain an Anti-Money-Laundering and Counter Terrorist Financing program, file suspicious activity reports, and address cybersecurity.[15]

6.14 Dr Carmody, Westpac, noted that digital currency intermediaries are providing similar services to businesses that are regulated under the AML/CTF regime. He observed:

---

11 Dr Sean Carmody, Westpac, *Committee Hansard*, 7 April 2015, p. 26.

12 Dr Sean Carmody, Westpac, *Committee Hansard*, 7 April 2015, p. 22.

13 PayPal, *Submission 45*, p. 6.

14 Australian Bankers' Association, *Submission 14*, p. 3.

15 MasterCard, *Submission 18*, p. 3.

> I would see a very close analogy between the business a foreign exchange broker is carrying on, and a company that is in the business of buying and selling Bitcoin for cash. It is just that under the definitions of the current AML framework foreign currency broking is included as a designated service but Bitcoin broking is not.[16]

6.15 In its submission the Attorney-General's Department noted that the ABA and the Australian Financial Conference (AFC) had made submissions to the statutory review of the AML/CTF Act. Both the ABA and the AFC expressed concern that financial institutions were being placed in a vulnerable position when offering designated services to digital currency businesses, and recommended that trading in digital currencies should be listed as a designated service under the AML/CTF Act.[17] The ABA also recommended that the statutory review consider whether all digital currency payments mechanisms should be brought under the AML/CTF regime.[18]

Know your customer programs

6.16 Under the AML/CTF regime, businesses must ensure that they know their customers and understand their customers' financial activities. Under the AML/CTF business must monitor transactions and collect and verify customer identification information—for example, documents, data or other information obtained from a reliable and independent source. The 'know your customer' (KYC) and customer due diligence processes increase the ability of businesses to better identify and mitigate money laundering and terrorism financing risks in the conduct of their transactions.[19]

6.17 Dr Carmody explained the advantages of digital currencies coming under the AML/CTF regime, in relation to know your customer requirements:

> There was an example given about a bitcoin broker who might have had a bank account with the Commonwealth Bank. If a cash payment came in then the bank would know, presumably, with the purchase of bitcoin. That is about all we would know. That is why there are a lot of advantages in the know-your-customer and due-diligence obligations also sitting with the broker, because the broker who has facilitated that purchase for the customer would also know, for example the wallet address that the customer used. Where they received that bitcoin that is not something the bank would know. If that did prove to be associated with suspicious activity, that would then be something that could be provided under requests from law-enforcement authorities.
>
> I think the phrase that has been used in some of the previous inquiries is on-ramps and off-ramps. It is very much that. If you are relying on trying to get visibility of the on-ramps and off-ramps only, through the bank part of the

16 Dr Sean Carmody, Westpac, *Committee Hansard*, 7 April 2015, p. 24.

17 Attorney-General's Department, *Submission 42*, p. 16.

18 Australian Bankers' Association, Submission 14, p. 3.

19 AUSTRAC, 'Part B of an AML/CTF program (customer due diligence procedures)' http://www.austrac.gov.au/part-b-amlctf-program-customer-due-diligence-procedures#dvs (access 21 May 2015).

> transaction, you do not really see that linkage to the bitcoin wallet. I know Bit Trade and others like them are endeavouring to put that same sort of know-your-customer monitoring within their activities as well. That makes a lot of sense.[20]

Document Verification Service

6.18 Veda expressed concern that the current lack of regulatory certainty meant that digital currency businesses have limited access to identity verification services. Veda noted that access to the best identity verification sources—the electoral roll, Document Verification Service (DVS), and credit reporting information— is restricted to those entities verifying identity for an AML/CTF purpose.[21]

6.19 The Attorney-General's Department manages the DVS. It is a secure, real-time on-line, electronic document verification system. Identity documents that can be verified using the DVS include: birth, marriage and change of name certificates; citizenship certificates; drivers' licences; Medicare cards; passports; and visas.[22] In order to access the DVS, organisations must meet strict eligibility criteria and abide by the terms and conditions of use, including having an approved reason for using the DVS, obtaining client consent and information and communications technology security.[23] The current access rules for the DVS require an applicant to cite a Commonwealth legislated requirement, such as the AML/CTF Act.[24]

6.20 Mr Miller, Bit Trade Australia, advised the committee that as they do not have access to the DVS at this point in time, in order to verify documents his business has to 'go to each of the individual document providers—for example, driver's licence from each state'.[25] He explained that they currently use a service provider to verify identities. However, without access to the DVS, 'the information is patchy' and when information cannot be verified electronically his business has to verify it manually. Mr Miller stated that as his business is already paying for access to a service which is suboptimal, it would happy to pay for access to the DVS.[26]

6.21 ADCCA maintained that digital currency businesses should be given access to the DVS in order to better facilitate KYC practices.[27]

---

20 Dr Sean Carmody, Westpac, *Committee Hansard*, 7 April 2015, pp. 23–24.

21 Veda, *Submission 20*, pp. [1]–[2].

22 Attorney-General's Department, 'Document Verification Service', https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/DocumentVerificationService.aspx (accessed 18 May 2015).

23 Document Verification Service, 'Businesses', http://www.dvs.gov.au/users/Pages/Businesses.aspx (accessed 10 June 2015).

24 Veda, *Submission 20*, p. [2].

25 Mr Jonathon Miller, Bit Trade Australia, *Committee Hansard*, 7 April 2015, p. 16.

26 Mr Jonathon Miller, Bit Trade Australia, *Committee Hansard*, 7 April 2015, p. 16.

27 Australian Digital Currency Commerce Association, *Submission 15*, p. 4.

The AML/CTF regime

6.22 Mr Mossop, Attorney-General's Department, noted that when the AML/CTF regime came into force in 2006, e-currency was covered as it was backed by bullion or backed by fiat currency, but digital currencies are backed by mathematically based formulas. He stated:

> First and foremost, digital currency and cryptocurrencies have evolved in a way that is not currently covered by Australia's anti-money-laundering regime. That is an issue for us in that, at the time the act was drafted, we did not really think about these types of currencies.[28]

6.23 Mr Mossop noted one of the difficulties with digital currencies is peer-to-peer transfers as it means transactions using digital currencies can be made directly to people anywhere in the world. He explained that this creates a particular challenge when working out how to regulate digital currencies:

> While we might have some visibility of the on-ramps and off-ramps in the places where they intersect directly with the financial sector, short of having everybody who has a bitcoin and makes a transaction report to AUSTRAC, it is going to be very difficult to find a point where all those transactions are co-located in a way they can be reported.
>
> So that is a big challenge for us, because we are going to lose visibility of how these bitcoins move around once they are inside the bitcoin system. We can see people buying them, we can see people selling them to a large extent, but we lose visibility of what happens within the system.[29]

6.24 Mr Mossop explained that there was still work to do to determine exactly which digital currency businesses should be brought under the AML/CTF regime.[30] Internationally, countries such as Canada, Singapore and the UK have decided to bring digital currency exchanges under their equivalent AML/CTF regimes. Mr Mossop noted that one of the considerations in the statutory review is how to define digital currency exchanges, and whether they should be defined as businesses that buy and sell digital currency, or if the definition should also include businesses that facilitate peer-to-peer exchanges, such as Bitcoin ATMs.[31]

Finding the right balance

6.25 Mr Mossop explained that an additional challenge was figuring out how to regulate digital currencies without stifling the growth of the industry. Regulators need to find a balance between trying to mitigate risks while allowing the more positive uses of digital currency to develop.[32]

---

28 Mr Daniel Mossop, Attorney-General's Department, *Committee Hansard*, 4 March 2015, p. 8.

29 Mr Daniel Mossop, Attorney-General's Department, *Committee Hansard*, 4 March 2015, p. 8.

30 Mr Daniel Mossop, Attorney-General's Department, *Committee Hansard*, 4 March 2015, p. 13.

31 Mr Daniel Mossop, Attorney-General's Department, *Committee Hansard*, 4 March 2015, p. 13.

32 Mr Daniel Mossop, Attorney General's Department, *Committee Hansard*, 4 March 2015, pp. 8–9.

6.26 DFAT was concerned about the application of AML/CTF regulations worldwide on small-value transactions that are predominantly made by people in poverty. Ms Rebecca Bryant, DFAT, explained that these small-value transaction are being made by:

> …itinerant workers who want to send money across specific corridors home to family and friends. In many instances they are unable to do that because they cannot show adequate identification. It is worse than that in a sense, because even people with identification today are having trouble transferring money across corridors that are considered risky.[33]

6.27 Ms Bryant, raised concerns that this would lead to people using black-market providers, outside the regulatory framework:

> And that is the danger: the more money you push into those corridors the less transparency you have. You do not know how much it is. You do not know who it is being transferred from and to. So, if money is pushed out of the formal system—I am not suggesting that it is excessive regulation—you will not see it. You cannot see it; you do not know where it is going. And that is the real concern.[34]

6.28 The Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church of Australia supported the regulation of digital currencies under the AML/CTF regime to ensure they are not used for serious criminal activities. It also noted potential benefits for financial inclusion. It noted that the FATF is an intergovernmental body that develops and promotes policies to protect the global financial system against money laundering and terrorism financing. In particular, the FATF aims to support countries and financial institutions in designing AML/CFT measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime. It noted that:

> FATF has stated that it recognises that applying an overly cautious response to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the financial system, thereby compelling them to use services that are not subject to regulatory and supervisory oversight. They argue the AML/CFT controls must not inhibit access to formal financial services for financially excluded and unbanked persons. The FATF recognises that financial exclusion could undermine the effectiveness [of] an AML/CFT regime. Hence, financial inclusion and AML/CFT should be seen as serving complementary objectives.[35]

---

33 Ms Rebecca Bryant, Department of Foreign Affairs and Trade, *Committee Hansard*, 7 April 2015, p. 29.

34 Ms Rebecca Bryant, Department of Foreign Affairs and Trade, *Committee Hansard*, 7 April 2015, p. 29.

35 Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church of Australia, *Submission 30*, p. 3.

Legislative changes

6.29 AUSTRAC advised that in order to cover digital currency in the AML/CTF regime, it would be necessary to change the Act not just the regulations.[36] Ms Jane Atkins, AUSTRAC, explained that although designated services can be added to the AML/CTF Act by regulation there would be other more complex consequential changes to be made if the decision was made to cover digital currencies. 'Obviously, the [statutory] review is the logical place to be looking at that and looking at what needs to be done'.[37]

6.30 AUSTRAC recognised that digital currency may pose a potential risk in the future, noting 'but right now we are not seeing that there is the sort of risk that has us saying to government, "It is imperative that you give us sight over this"'.[38] Ms Atkins, AUSTRAC, outlined the requirements for designated services under the AML/CTF regime:

> The sort of obligations in our act then are for them to have an anti-money laundering and counter-terrorism financing program, which means that they need to assess the risks of money laundering for their customers and the types of transactions that they are dealing with. They have to have a program in place to mitigate those risks. They have to carry out know your customer procedures with their customers. They have to have ongoing due diligence programs around watching whether their customers risk is going up and down and whether they need to do more than they have done before.
>
> They need transaction monitoring systems so that they can report whatever equivalent—perhaps you would have an equivalent of $10,000 digital currency. You might have a report about that and you might have a report where they were transmitting internationally, as we talked about. If they are going to transact in the same way as what we would call remittance providers transact, then there would seem to be at the moment—off the top of my head—no policy reason why you would not cover them in the same way. We would certainly want suspicious matter reporting.[39]

6.31 Mr Mossop, Attorney-General's Department, noted that the pace of innovation makes it difficult to anticipate where the technology will go and where it will lead. 'We need to regulate in a way that prevents having to come back and regulate again in a relatively short amount of time for a new product that comes out'.[40]

---

36 Ms Jane Atkins, Australian Transaction Reports and Analysis Centre, *Committee Hansard*, 7 April 2015, p. 57.

37 Ms Jane Atkins, Australian Transaction Reports and Analysis Centre, *Committee Hansard*, 7 April 2015, p. 57.

38 Ms Jane Atkins, Australian Transaction Reports and Analysis Centre, *Committee Hansard*, 7 April 2015, p. 52.

39 Ms Jane Atkins, Australian Transaction Reports and Analysis Centre, *Committee Hansard*, 7 April 2015, pp. 56–57.

40 Mr Daniel Mossop, Attorney General's Department, *Committee Hansard*, 4 March 2015, p. 9.

6.32 ADCCA outlined the views of Australian digital currency businesses. It stated:

> In Australia the vast majority of Digital Currency businesses and users are law-abiding and desire the enhanced legitimacy of appropriate legal oversight and recognition. Incorporating Digital Currency into law enforcement legislation, particularly through the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, is a necessary step toward guaranteeing the security and legitimacy of Digital Currencies in Australia.[41]

6.33 Bitcoin Group Limited stated that it fully anticipates the 'costs associated with being subject to compliance protocols and the likelihood of the obligations from national laws requiring access to our records and compelling our company to actively monitor and proactively report suspicious transaction activity'.[42]

6.34 Given that digital currencies are a global phenomenon, the Attorney-General's Department emphasised the importance of ongoing international cooperation through forums such as the Financial Action Task Force. It argued international cooperation was essential to developing a consistent international approach to regulation to avoid the risk of regulatory arbitrage, where businesses take advantage of more favourable regulations in other jurisdictions.[43]

Committee view

6.35 In order to help manage relationships with banking services and be prepared for future regulation, some digital currency businesses have tried to mirror the obligations that are required by designated services under the AML/CTF regime, such as implementing know your customer programs. However, the AML/CTF Act currently does not cover digital currencies that are not backed by precious metal or bullion.[44] Consequently, digital currency businesses are not able to access the Document Verification Service which would better facilitate identity checking to meet AML/CTF requirements. Furthermore, they currently stand outside this robust regulatory regime designed to detect and deter money laundering and terrorism financing.

6.36 The committee strongly supports applying AML/CTF regulation to digital currency exchanges, noting that similar steps have been taken in Canada, the UK and Singapore. The committee notes that the Attorney-General's Department is currently conducting a statutory review of the AML/CTF Act which is examining whether digital currency businesses should be brought under the AML/CTF regime, and if so which businesses should be included.

---

41 Australian Digital Currency Commerce Association, *Submission 15*, p. 14.

42 Bitcoin Group Limited, *Submission 38*, p. [2].

43 Attorney-General's Department, *Submission 42*, p. 17.

44 Attorney-General's Department, *Submission 42*, p. 10; see chapter 2 of this report.

Recommendation 4

6.37 **The committee recommends that the statutory review considers applying AML/CTF regulations to digital currency exchanges.**

Senator Sam Dastyari
Chair