

Anti-money Laundering and Counter Terrorism Financing Requirements Extended to Cryptocurrency Exchanges

Nick Karagiannis, Partner, Luke Dale, Partner, and Daniel Kiley, Senior Associate, at HWL Ebsworth, consider new regulation of cryptocurrencies.

Money laundering is widely recognised as a key enabler for criminal activity, and the recent rise of pseudonymous cryptocurrencies has created new ways for this occur. Existing Australian laws in relation to money laundering were not fully equipped for these developments, but amendments have been passed by Parliament to address such matters.

These will commence shortly following a brief period of consultation. While the amendments place requirements on organisations running services to exchange traditional money for cryptocurrencies (or vice versa), and are designed to catch questionable activity, they will also potentially lessen the anonymity that everyday cryptocurrency users and investors would ordinarily expect.

The Australian Criminal Intelligence Commission (ACIC) recognises money laundering as one of the 'key enablers' for serious and organised crime in Australia. In its 2017 Organised Crime in Australia report, the ACIC stated that:

Money laundering remains a key risk to Australia and is the common element in almost all serious and organised crime. Money laundering enables criminals to hide and accumulate wealth, avoid prosecution, evade taxes, increase profits through re-investment, and fund further criminal activity. Money

laundering activities also have the potential to undermine the stability of financial institutions and systems, discourage foreign investment and alter international capital flows.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (Act)* accordingly establishes a system of reporting obligations on financial institutions and other designated service providers, whereby certain transactions must be notified to the Australian Transaction Reports and Analysis Centre (AUSTRAC). Relevant institutions are also required to verify a customer's identity before providing certain services to customers.

While the Act already has mechanisms in place to address large movements of money via traditional banking systems, it was underequipped to deal with issues that arise with respect to cryptocurrencies. This is of particular concern given that the ACIC has also reported that:

The two key enabling technologies currently used to facilitate serious and organised crime are virtual currencies and encryption. Virtual currencies, such as bitcoin, are increasingly being used by serious and organised crime groups as they are a form of currency that can be sold anonymously online, without reliance on a central bank or financial institution to facilitate transactions.

As such, on 7 December 2017 Commonwealth Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (Cth)* to bring digital currency exchanges (where traditional money can be exchanged for cryptocurrencies) within the scope of the Act, along with a number of other amendments.

Under the Act prior to these amendments, there was a concept of an *e-currency*, being a digital currency backed directly or indirectly by a precious metal or bullion. Plainly, this did not apply to the majority of the cryptocurrencies that are becoming increasingly popular, which generally are not backed by physical items in this way. Accordingly, a new and much broader defined term, *digital currency*, has been inserted.

As part of the changes to the Act, digital currency exchanges operated in Australia or by an Australian person or entity will be required to:

- register with AUSTRAC;
- adopt and maintain an Anti-Money Laundering/Counter-Terrorism Financing program to identify, mitigate and manage associated risks;
- identify and verify the identities of their customers;
- report all transactions with a value exceeding \$10,000 or more, along with any other suspicious activities, to AUSTRAC; and

- keep certain records of transactions, identities and Anti-Money Laundering/Counter-Terrorism Financing programs for at least seven years.

The precise matters to be reported to AUSTRAC are still to be finalised, as they are specified in a set of Rules made under the Act. AUSTRAC released a draft set of these Rules for public consultation on 16 January 2018, and submissions closed on 13 February 2018.

Under the Rules as currently proposed, reports to AUSTRAC on digital currency matters would include a range of standard details about the identity of the individual involved and the money sent or received, but also, uniquely to digital currency transactions, include:

- Internet Protocol (**IP**) addresses;
- email addresses and phone numbers;
- social media usernames;
- unique identifiers relating to the digital currency wallets (such as the public address of a wallet); and
- unique identifiers of devices involved, including Media Access Control (**MAC**) addresses, International Mobile Equipment Identity (**IMEI**), International Mobile Subscriber Identity (**IMSI**) numbers, and secure element ID (**SEID**) numbers.

The amendments to the Act only operate at the fringes of cryptocurrency networks, by capturing transactions that see traditional currency exchanged for virtual currencies and vice versa. However the pseudonymous public ledgers that form part of most cryptocurrencies (including Bitcoin, for example), allow anyone to observe the movement of funds between public wallet addresses. As wallet addresses are to be provided to AUSTRAC under the draft Rules,

this should theoretically allow it some visibility over the movement of funds after they take digital form.

While many like to think of cryptocurrencies as anonymous, this is typically not the case, with the wallet addresses associated with each user serving to pseudonymously identify them. With the reporting of wallet addresses to AUSTRAC, it should, over time, be able to amass a database of the real identities associated with otherwise pseudonymous wallet addresses. This may assist in discouraging the use of cryptocurrencies for black market transactions. However, many enthusiasts are likely to see it as going against the liberal ideals on which many cryptocurrencies were founded.

Newer cryptocurrencies have launched with different technologies that promise greater anonymity, which may become more appealing to users as government oversight increases through measures such as these changes to the Act.

The amendments to the Act, and associated new Rules, are expected to commence on 1 April 2018.

This article was written by **Nick Karagiannis**, Partner, **Luke Dale**, Partner, and **Daniel Kiley**, Senior Associate at HWL Ebsworth.