Article Information

Authors: Alexa Bowditch, Barbara Vrettos, Jade McGlynn, Michael Bacina
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: AUSTRAC's online overhaul: the suggestion box is now open, El Salvador Opposition shake an angry fist at new Bitcoin law, Ransomware: report now, pay later

Michael Bacina, Alexa Bowditch, Barbara Vrettos and Jade McGlynn of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

AUSTRAC's online overhaul: the suggestion box is now open

Registered digital currency exchanges (DCEs) often need to report to and interact with AUSTRAC, and no doubt have formed some views as to what could be done differently or better. AUSTRAC is now giving everyone a chance to provide feedback and use it to improve (over the next 4 years).

AUSTRAC is undertaking a systems transformation program over the next 4 years which will replace AUSTRAC Online. The much loved/hated AUSTRAC Business Profile Form has recently been replaced with a web-based form (which is a great step in the right direction).

The new system is intended to be user-friendly with improved reporting capability and self-service options.

AUSTRAC is currently in the discovery phase of their improvement program and are focused on understanding from regulated entities how they can change, do better, or do things differently – to make it easier for those entities to engage and report to AUSTRAC, and meet AML/CTF obligations.

If you would like to be involved, email haveyoursay@austrac.gov.au with your feedback and your contact details. If you would like to have your AML Program reviewed or consider how you manage reporting as part of giving this feedback, we can also help with that.

El Salvador Opposition shake an angry fist at new Bitcoin law

It's not just US Regulators who are divided when it comes to the regulatory treatment of digital assets. A little over a week ago, El Salvador's president, Nayib Bukele made history when his proposal to declare Bitcoin legal tender was approved by El Salvador's Congress. This week, Jamie Guevara, deputy leader of the El Salvador opposition party made a stand to oppose the legislation, teaming up with a group of Salvadoran citizens to file a lawsuit that argues El Salvador's "Bitcoin Law" is unconstitutional.

As one disgruntled citizen told El Mundo, a Spanish Newspaper:

> I bring a lawsuit of unconstitutionality against the decree issued by the Bitcoin Law for being a decree lacking legality, lacking foundation, without considering the significance and harmful effects that such a law will cause to this country.

This perspective contrasts to the Salvadorian President who asserts the Bitcoin laws purpose is to foster financial flexibility and freedom, to: "*bring financial inclusion, investment, tourism, innovation and economic development for (their) country*".

At the Miami Bitcoin 2021 conference, Bukele portrayed his legislative proposal as a means to "design a country for the future." He used his twitter account to remark that if just 1% of the world's bitcoin moved to El Salvador as a result of this new law, it would equate to a quarter of El Salvador's annual economic output.

El Salvador has an unfortunate history of corruption and the government does not enjoy a high level of trust. This is seen in the talk from unimpressed citizens who say that, "*The Bitcoin Law is to loot people's pockets, it is tax-exempt (and) they want to force us to trade.*"

Given the law only applies to businesses and not individuals, it remains to be seen how this lawsuit will progress. On the flip side, there are serious issues in forcing businesses to use an electronic transfer system which requires an investment in hardware to facilitate. Credit cards and online payments are voluntary and may be demanded by customers, but legal tender must be accepted by businesses under the Bitcoin Law, meaning businesses will have to find a way to accept Bitcoin.

The question of the 6 billion a year in remittances is thankfully a simpler one, as Bitcoin already provides an inexpensive transfer system for moving value globally.

Ransomware: report now, pay later

After the surge of discussion following the Colonial Pipeline cyber attack it is unsurprising that combatting cybercrime is high on the agenda. Most recently, Australia Home Affairs Minister Karen Andrews is considering a proposal put forward by the Labour party to mandate that ransomware victims report before paying any ransom.

The idea of mandatory notification is not new and has been recommended by a variety of international authorities. Citing the recent cyber attacks on JBS food, Nine Entertainment and Uniting Care Queensland, Shadow Assistant Minister for Cyber Security Tim Watts stated "*It's time we saw some real action.*"

Watts put forward the private members bill, the 'Ransomware Payments Bill' earlier this week which aims to mandate that businesses and government agencies to notify the Australian Cyber Security Centre (**ACSC**) before paying any ransom demands. Watt's call to action was echoed in the explanatory memorandum citing suggestions that "*the cost to the Australian economy of ransomware attacks in 2019 alone was in the order of $1 billion.*" The bill oddly defines "ransomware payments" in a way which is identical to "ransom" so we will stick with the traditional definition in our reporting.

If passed, the bill mandates notice be provided to ACSC as soon as practicable with details such as:

- the identity of the attacker, or what information the entity knows about the identity of the attacker (including information about the purported identity of the attacker);
- a description of the ransomware attack, including:
- any payment methods for ransom sought, and if digital currency is involved, the wallet to which the attacker demanded the ransom be paid;
- the amount of the ransom payment; and
- any indicators of compromise known to the entity (which is defined as "technical evidence left by an attacker that indicates an attacker's identity or methods).

Failure to comply could lead to a civil penalty of 1,000 penalty units (currently $222,000), a steep fine when a business may already be reeling from a cyber attack.

The necessity to report first, act later draws similarities with the current mandatory data breach notification scheme which has been in place since early 2018. The similarities in existing policy in this area has gained favour with commentary that the bill will likely be rolled out soon. Watts further said that:

Such a scheme would be a policy foundation for a coordinated government response to the threat of ransomware, providing actionable threat intelligence to inform law enforcement, diplomacy and offensive cyber operations.

Innovation Australia reports that the Opposition has put this high on the list for debate when Parliament returns in August.

In the interim the ACSC recommends that businesses not pay ransoms as there is no guarantee payment will lead to affected devices being fixed. Payments may also make businesses more vulnerable to future attacks. The Australian Cyber Security Centre has published a ransomware Prevention and Protection Guide as well as an emergency response guide available here.

For all the headlines about digital currency being involved in ransomware attacks, the US Department of Justice tracked

and recovered (with the help of the FBI) a substantial portion of the ransom paid during the Colonial Pipeline attack, because digital currency on public blockchains is almost entirely traceable, and is one of the worst possible method to launder money or receive ransomware payments.