Article Information

Authors: Steven Pettigrove, Jake Huang, Luke Higgins, Luke Misthos
Service: Blockchain, FinTech
Sector: Financial Services, IT & Telecommunications

Blockchain Bites: Australia consults on crypto tax reporting standards, Australia mandates ransomware reporting as Cyber Security Act passes, UK clarifies crypto regulatory roadmap, and US Appeals Court overturns Tornado Cash sanctions

Steven Pettigrove, Jake Huang, Luke Higgins and Luke Misthos of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

CARF before the horse? Australia consults on crypto tax reporting standards

The Australian government has released a consultation paper on how to best implement the Crypto-Asset Reporting Framework (CARF), a global standard developed by the Organisation for Economic Co-operation and Development (OECD). CARF is intended to enhance tax transparency by facilitating the automatic exchange of information about crypto-asset transactions between jurisdictions.

The consultation paper published by Treasury states that CARF's implementation in Australia will require amendments to domestic tax laws to adhere to international standards. The government has proposed two options for implementing CARF in Australia which are outlined below, along with the types of entities and information that will be subject to reporting requirements.

What is CARF?

CARF is designed to deter tax evasion by ensuring the transparent reporting of crypto-asset transactions. In Australia, it would enable the Australian Taxation Office (ATO) to exchange data with other jurisdictions on transactions by Australian residents. The framework covers:

- Crypto-assets: digital assets using cryptographic security and distributed ledger technology, including bitcoin, ether, stablecoins, derivatives, and certain NFTs.
- Relevant transactions: crypto-to-crypto transactions as well as crypto-to-fiat or fiat-to-crypto.
- Reporting entities: crypto-asset service providers facilitating transactions.

The CARF mandates the reporting of customer-specific details for transactions exceeding USD $50,000, while smaller transactions are reported in aggregate without identifying individuals.

Implementation options

Option 1: Adopt the OECD CARF Model

Under this option, Australia would adopt the CARF Model Rules as developed by the OECD, making only minor adjustments to integrate them into domestic law. Key features include:

- Alignment with global standards: ensuring consistency with international norms to support efficient reporting and information exchange.
- Comprehensive reporting obligations: crypto-asset service providers report user data, transaction details, and controlling persons.

- De minimis thresholds: Customer-specific reporting applies only to transactions exceeding USD 50,000; smaller transactions are reported in aggregate.
- Benefits:
    - Facilitates global data exchange for improved tax compliance.
    - Reduces duplication and compliance costs for entities operating in multiple jurisdictions.

Option 2: Develop a Bespoke CARF Framework

Alternatively, Australia could create its own reporting framework tailored to the specific needs of the ATO. This approach would still align with the policy goals of CARF but would allow for greater flexibility:

- Custom thresholds and scope: Australia could adjust reporting thresholds, exclude certain information fields, or specify additional requirements.
- Selective targeting: Focus on entities and transactions providing the most value for tax compliance efforts.
- Drawbacks:
    - Potential misalignment with global CARF standards.
    - Higher compliance costs for entities with cross-jurisdictional operations.
    - Reduced data-sharing efficiency with other jurisdictions.

Entities and reporting obligations

CARF applies to 'Reporting Crypto-Asset Service Providers', which currently include crypto exchanges, wallet providers, brokers, dealers, and ATM providers facilitating exchanges between crypto-assets and fiat currencies or between crypto-assets.

To be regulated under Australia's model, entities must have a 'nexus' to Australia according to one of various tax concepts being tax residency, Australia being its place of incorporation, central management and control, or a regular place of business (e.g., a permanent establishment). Reporting requirements include:

- User and transaction data: Details on crypto users, taxpayer identification numbers, jurisdictions of residence, and reportable transactions.
- Transaction types: Exchanges involving relevant crypto-assets, payments for goods/services over USD 50,000, and transfers to external wallets.
- Provider details: Information about the reporting service provider, including name, address, and identifying numbers.

Consultation period

The government's consultation period for CARF implementation is open from 21 November 2024 to 24 January 2025. Industry participants, market stakeholders, and interested individuals are invited to share their perspectives on how the framework should be implemented Downunder.

It would be remiss to understate the importance of clarity, efficiency, and consistency in CARF implementation. Industry members would prefer an approach that minimises compliance costs, particularly for smaller crypto service providers, and ensures that the rules align closely with the global OECD standard to avoid duplicative reporting obligations across jurisdictions.

Common CARF concerns include data security and confidentiality, especially given the sensitive nature of personal and transactional information being collected and shared under the CARF and across jurisdictions. Ensuring robust data protection mechanisms will be of paramount importance to maintaining trust and compliance within the crypto ecosystem.

It may also be practical to seek de minimis thresholds, streamlined reporting processes, and flexibility in reporting deadlines to accommodate the dynamic and fast-moving blockchain ecosystem. Many will also urge the government to avoid overly burdensome requirements that could stifle innovation or drive businesses offshore.

Conclusion

Curiously, the push for CARF implementation comes before any significant reforms to Australia's broader crypto tax regime and regulatory reform more generally – a case of putting the CARF before the horse, perhaps. This raises questions about the order of regulatory priorities, as market participants will need to navigate new reporting obligations within an already complex tax landscape. There may also be a need to revisit CARF implementation again in future.

The adoption of CARF in Australia aims to align with global efforts in combating tax evasion in the crypto-asset space. By

contributing to the consultation, participants can help ensure the resulting legislation supports global tax compliance whilst fostering growth, innovation and participation in the Australian crypto industry.

Written by Steven Pettigrove and Luke Higgins

Australia mandates ransomware reporting, as Cyber Security Act passes

Australia has taken a decisive step in enhancing its cyber security framework, passing the *Cyber Security Act 2024* (Cyber Security Act) on 25 November 2024 and amendments to related legislation. As we previously reported, the law is set to reshape the cyber security landscape for Australian businesses, particularly with the introduction of a mandatory ransomware payment reporting.

Mandatory Ransomware Payment Reporting

The Cyber Security Act now mandates organisations report ransomware payments to the Department of Home Affairs and the Australian Signals Directorate (ASD) within 72 hours of payment or becoming aware of the same.

This reporting requirement applies to:

1. Critical infrastructure entities regulated under the Security of Critical Infrastructure (SOCI) Act; and
2. Private sector businesses with an annual turnover exceeding the forthcoming threshold (likely AUD 3 million if the same threshold under the *Privacy Act 1988* (Cth) is applied).

Organisations face a civil penalty of 60 penalty units (currently AUD 19,800) for failing to comply.

Notably, the obligation is triggered upon payment, not the mere discovery of an attack or receipt of a ransom demand. Boards must weigh the implications carefully, given that the Australian Government's policy remains firmly against paying ransoms.

The Reporting Dilemma

While reporting payments enhances transparency and government response capabilities, it complicates decision-making for directors, who must balance:

- Risks of paying a ransom: Encouraging further attacks, violating sanctions or anti-money laundering laws, and uncertainty over effectiveness.
- Risks of not paying: Operational disruptions, reputational damage, third-party claims, and data loss.

Adding another layer of complexity, the Government may use its directions powers under the SOCI Act to compel certain organisations to pay or refrain from paying a ransom.

Limited Use Protections

The Cyber Security Act introduces limited use protections for ransomware reports, restricting how disclosed information can be used. Reports cannot be used for general enforcement actions or admitted as evidence in most proceedings, with exceptions for crimes and breaches of the Act itself. However, the Act stops short of providing a full safe harbour:

- Regulators can still use investigatory powers to access the underlying information.
- Other mandatory reporting regimes, such as those under the Privacy Act or ASX Listing Rules, remain enforceable.

Voluntary Information Sharing: Building Trust

The Act also establishes a voluntary reporting regime via the National Cyber Security Coordinator (NCSC). The scheme is structured to encourages entities to disclose information about cyber incidents to the NCSC for assistance and coordination without fear of it being used against them in regulatory enforcement (outside limited exceptions).

However, this remains distinct from ransomware reporting, and businesses must tread carefully in balancing transparency with the risk of disclosure.

Looking Ahead

The Cyber Security Act is awaiting Royal Assent. The mandatory reporting requirement for ransomware payments is

expected to come into force six months after that date or such other date as is designated.

Businesses should ensure that they:

1. Review and update cyber incident response plans to ensure compliance with ransomware reporting requirements.
2. Train directors and executives on the implications of ransomware payment decisions and reporting obligations.
3. Test cyber playbooks with scenarios incorporating ransomware attacks, mandatory reporting, and government engagement.
4. Consider legal implications, including sanctions laws and directors' duties, when deciding how to respond to ransomware demands.

The Cyber Security Act signals a shift toward greater transparency, accountability and collaboration in cyber security following several high profile incidents. While the new reporting regime is intended to provide valuable intelligence in combatting cyber breaches, it also introduces significant challenges for businesses navigating compliance, governance, and operational risk.

By Steven Pettigrove and Luke Misthos

Yes, Minister! UK clarifies crypto regulatory roadmap

The UK Economic Secretary Tullip Saddiq has confirmed that the UK Government under Labour plans to continue policy reforms in relation to crypto-assets and digital markets initiated under the Conservative Government with a draft regulatory framework slated for release next year.

Speaking at a Tokenisation Summit in London, Saddiq said:

If we are to maintain the UK's position as a leading financial services hub, we need to lean in to the emerging and disruptive technologies that could change our industry dramatically in the coming years.

Saddiq outlined an ambitious agenda for the UK which includes:

- make the UK a global hub for securities tokenisation
- taking forward financial market infrastructure sandboxes through the Digital Securities Sandbox
- the pilot issuance of Digital Gilts or DIGIT within the sandbox
- creation of various new regulated activities for cryptoassets, such as operating a cryptoasset trading platform, as well as associated regimes for both admissions to trading and market abuse
- new regulated activities for stablecoin, which will be implemented to the same timetable as the rest of the regulatory regime for cryptoassets
- proceeds with clarifying legal treatment of staking as not falling within the scope of a collective investment scheme

With refreshing clarity, the Minister observed that crypto-assets have both proven the use case for blockchain technology and are here to stay. In a call to action, Saddiq observed:

If we are going to truly unlock the best of what tokenisation, blockchain technology, and cryptoassets have to offer in the UK, then we need to tie the threads together properly. That means recognising and facilitating the opportunities for traditional markets and cryptoassets to succeed to their mutual benefit. It also means ensuring a coherent joined-up approach across UK authorities, so that firms have the certainty to invest and grow, as well as the space and flexibility to innovate.

Meanwhile, this week, the UK's Financial Conduct Authority (FCA) released its Crypto Roadmap (see Annexure) setting out its plans for the development of the nation's crypto-assets regulatory regime. The roadmap outlines a wave of discussion papers and consultations over the next 18 months with a view to full go live on the UK's comprehensive crypto-assets regime in 2026.

Reforms to date – Money Laundering, financial promotions and stablecoin regulations

- Since January 2020, the *Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017* (MLRs) have required firms providing certain specific activities in relation to cryptoassets, such as exchanging cryptoassets for money, to register with the FCA and to comply with the requirements of the MLRs (e.g. risk assessments and due diligence on customers).
- Following legal reforms in 2023, the FCA is responsible for regulating cryptoasset promotions. In the first year of the regime, the FCA has taken significant action against firms illegally promoting to UK consumers. This includes

issuing 1702 alerts, taking down over 900 scam crypto websites and over 50 apps.
- In November 2023, the Bank of England and the FCA published discussion papers on their respective plans to regulate stablecoins.

Next up – Token admissions and disclosures, market abuse and intermediaries

The next destination on the FCA's roadmap is two discussion papers scheduled in Q4 2024 and Q1/Q2 2025 respectively. The first will cover:

1. Admissions and disclosures. This includes admission/rejection processes for token listings, disclosure liability, due diligence, and the National Storage Mechanism (NSM). Matthew Long, Director of Payments and Digital Assets at the FCA, said:

Admissions and disclosures are a crucial aspect of the new crypto regime we're proposing… It's an area that's fundamental to investor protection as it allows people to make informed financial decisions.

2. Market abuse, including systems and controls, information sharing, and inside information disclosure. According to Matthew Long:

Market abuse can manifest in crypto markets in novel and distinct ways, giving rise to new challenges… we want to achieve the same outcomes wherever possible when it comes to a crypto version of market abuse regulation

The second paper will address trading platforms and intermediaries, including:

1. Trading platform rules including location, access, matching and transparency requirements
2. Intermediation rules including order handling and execution requirements
3. Lending rules including ownership, access and disclosures
4. Staking including ownership and disclosures
5. Prudential considerations for cryptoasset exposures

These discussion papers will build on a series of recent roundtables with over 100 stakeholders — including crypto exchanges, banks, trading firms, law firms, academics and regulators.

Further consultations – stablecoins, custody, prudential and beyond

In Q1/Q2 2025, building on previous discussions, the FCA is also moving ahead with consultation papers on:

- Stablecoins including backing assets and redemption
- Custody including recordkeeping, reconciliations, segregation of assets, and use of 3rd parties
- Prudential including the introduction of a new prudential sourcebook, including capital, liquidity and risk management

It is anticipated that the FCA will publish all policy statements (i.e. final rules) by 2026 and start to get ready for the application of the full regime. This timeline is nevertheless subject to change according to parliamentary timeline and government priorities.

With these latest Government and regulatory pronouncements, the UK looks set to challenge Europe and the United States as a hub for digital finance in the 21st century. The Government's decision to provide clear policy direction backed by a regulatory roadmap is likely to give significant confidence to innovators looking to build businesses in the UK. The Government's clear-eyed focus on both digital markets and crypto-assets while working in tandem with its lead regulator is also likely to give significant encouragement to the UK blockchain industry.

Written by Steven Pettigrove, Jake Huang and Matt Norton

Storm in a teacup? US Appeals Court overturns Tornado Cash sanctions

In a whirlwind turn of events, the US Fifth Circuit Court of Appeals has ruled that the Treasury Department's Office of Foreign Assets Control (OFAC) blew past their authority by sanctioning Tornado Cash, a set of decentralised software known as a "crypto mixer" which permits users to have privacy in their transactions by mixing multiple transactions together (but paying out the correct amounts to each person entering the mixer). This appeal court decision overturns the lower court's ruling and has been hailed as a "historic win" for the crypto industry by Coinbase's Chief Legal Officer, Paul Grewal.

At the heart of the case is a critical distinction: Tornado Cash is not a legal entity but rather is a collection of smart contracts powered by blockchain technology – self-executing lines of code which perform a function designed to enhance privacy. There is no central party who can turn the code on or off. The lower court decision determined that the software contract address for Tornado Cash could be sanctioned and that it was "property" which could be the subject of sanctions. The appeals court has disagreed, saying these smart contracts cannot be classified as "property" under US sanctions laws such as the International Emergency Economic Powers Act (IEEPA). The court emphasised that OFAC exceeded its mandate, as the smart contract code itself cannot be owned *or* blocked.

The clouds of this case gathered in August 2022 when OFAC sanctioned Tornado Cash's smart contract address, alleging that the Tornado Cash mixer had been used by North Korea's nuclear weapons program and notorious hacking group Lazarus Group. The sanctions designation sparked a lawsuit from various plaintiffs, including Tornado Cash users, who argued that the sanctions infringed on their rights to privacy and improperly inflated the definition of "property" under US law to high altitude. The appeals court has now agreed, holding that Tornado Cash's open source smart contracts are "immutable smart contracts" and not capable of being owned.

The Court went on to find that the smart contracts were not in fact contracts at all, being in the nature of a unilateral contract, there being no operator of the code in this case. The Court indicated that its analysis might be different if the smart contracts were in fact mutable (e.g. upgradeable) and otherwise controllable or custodial.

The Court observed the Tornado Cash contracts remain available to users to fill their sails with privacy and navigate an otherwise transparent public blockchain network with that benefit. This issue was raised in the earlier decision, as open source smart contracts cannot be taken down without co-operation from a majority of nodes in a blockchain network, and with those nodes geographically disbursed and relatively easy to set-up, a near impossibility.

On the basis of this ruling, the Appeals Court observed that it was not necessary to go on to consider whether Tornado Cash was an entity or capable of holding an interest in the immutable smart contracts, themselves not being capable of being property.

After the ruling, Tornado Cash's governance token, TORN, surged dramatically, with the token up ~500% in the last 24 hours at the time of writing.

While this fresh breeze of judicial clarity is welcome for blockchain enthusiasts and innovators more used to the doldrums of regulation by enforcement, it is important for businesses and developers to keep a clear eye on the regulatory horizon. Tools like Tornado Cash, like any tool for privacy, can be used for good – ensuring financial privacy in a world of increasing surveillance – but also can be used by criminals for nefarious purposes. Striking the right balance between innovation and accountability is crucial to weathering any storms and charting a course to a clearer day.

Meanwhile, persons involved in the development of mixing services have been the subject of a wave of prosecutions by US regulators. The developers of Tornado Cash themselves have been prosecuted in the United States and the Netherlands. Some experts have speculated that the Appeals Court decision may prompt Congress to act to introduce tougher restrictions on the development of these types of services.

For now, Tornado Cash and the list of designated smart contracts remains on OFAC's Specially Designated Nationals List. It remains to be seen if OFAC will now take steps to remove Tornado Cash entirely or perhaps only the list of immutable smart contracts from the designation upon the matter being remitted to the lower court to enter judgment. Of course, OFAC may yet seek to appeal to the US Supreme Court.

With a new US administration set to take over in January, this case underscores the need for clear and fit for purpose laws that foster innovation while mitigating harm appropriately.

Written by Steven Pettigrove and Luke Higgins