

## Article Information

Authors: Steven Pettigrove, Luke Higgins, Luke Misthos, Emma Assaf

Service: Blockchain

Sector: Financial Services

---

## Blockchain Bites: UK targets 2026 crypto tax reporting rules, AUSTRAC releases second consultation on AML/CTF rules, Cayman Islands ready to launch RWA and tokenised securities, and ASIC sues Blockchain Global director

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

---

### CARF in motion: UK targets 2026 implementation of crypto tax reporting rules

The United Kingdom's HM Revenue & Customs (HMRC) has [announced](#) that from 1 January 2026, all UK-based 'reporting cryptoasset service providers' (RCASPs) will be required to collect and report user and transaction data, in line with the [Organisation for Economic Co-operation and Development's \(OECD\) Cryptoasset Reporting Framework \(CARF\)](#).

[According to HMRC](#), a business will be classified as an RCASP if it either transacts cryptoassets on behalf of users or provides a means for users to transact cryptoassets. This includes, for example, cryptoasset exchanges, brokers and dealers.

The UK is not only implementing the CARF as an international standard but is also extending the reporting framework to apply to domestic reporting obligations. The move is part of a broader effort to increase transparency in the growing crypto sector and prevent tax evasion using digital assets.

For individual users, service providers must collect the full name, date of birth, home address, country of residence and either a National Insurance number or Unique Taxpayer Reference for UK residents. For non-UK residents, providers must obtain the individual's tax identification number and the country where it was issued.

For entity users, providers must gather the legal business name and main business address. For UK companies, the company registration number must be reported, while non-UK entities require a tax identification number and issuing country. Information about controlling persons may also be necessary. 'Users' will include those who are tax resident in the UK, or another country that is signed up to CARF rules.

Each transaction must include the transaction value, the type of cryptoasset involved, the nature of the transaction and the number of units.

Although the rules officially come into effect on 1 January 2026, HMRC is encouraging service providers to begin preparations early. Firms are advised to start collecting the required data ahead of the deadline and to implement due diligence processes to verify the accuracy of the information collected. Failure to comply with the reporting obligations, or submission of inaccurate or unverified reports, may result in penalties of up to £300 per user.

HMRC is expected to release further guidance in the lead-up to the implementation date.

Australia [conducted its own consultation on CARF implementation earlier this year](#) seeking guidance how best to implement domestic standards. The response to that consultation and any legislative proposals for implementation are awaited.

#### Anyone for another round? AUSTRAC releases 2nd consultation on AML/CTF Rules

AUSTRAC has opened a [second consultation](#) seeking further feedback on the proposed re-write of the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Rules. This follows the passage of the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024* (the **Amended AML/CTF Act**) by the Australian Parliament in November 2024.

While the major changes introduced in the first exposure draft were covered in a [previous article](#), several updates have been made following the initial consultation:

- (a) allowing delayed initial customer due diligence (**CDD**) in a broader range of circumstances;
- (b) providing greater flexibility in determining the lead entity of reporting groups;
- (c) clarifying how to form reporting groups;
- (d) clarifying the definitions related to value transfers and travel rule requirements (e.g., “ordering institution”, “beneficiary institution”); and
- (e) addressing practical implementation challenges for businesses.

In addition to these updates, the second exposure draft (**ED2**) introduces more onerous information requirements to obtain registration as a VASP, new requirements for suspicious matter reports, new obligations targeting financial sanctions compliance and policy requirements in relation to travel rule compliance.

#### Key Updates in the ED2

##### **Enrolment Applications**

Part 2 of the ED2 contains updated requirements for *all* enrolment applications. Reporting entities will now be asked to provide additional details such as the number of employees and membership in any industry or professional associations.

##### **Registration of RSPs and VASPs**

Under the amended AML/CTF Act and the ED2 Rules, remittance service providers (**RSPs**) and Virtual Asset Service Providers (**VASPs**) must apply for registration with AUSTRAC before providing registrable services, in addition to enrolling as reporting entities. Registration differs from enrolment in that AUSTRAC assesses the application before making a decision.

Part 3 of the ED2 introduces a more robust VASP registration process by expanding the information AUSTRAC must consider, aligning Australia with international standards (e.g. the UK, Singapore and Hong Kong). AUSTRAC will also maintain a VASP Register and publish key registration details (see Draft Rule s 3-2). By contrast, the current DCE register is not published by AUSTRAC.

Section 3-4 outlines the general information that must be included in a VASP’s application, such as the applicant’s identity, place of business, beneficial ownership and operational information.

Section 3-5 requires VASPs to identify the money laundering, terrorism financing and proliferation financing risks they may reasonably face in providing their registrable services. This includes risks associated with:

- (a) the types of customers they service;
- (b) foreign countries they operate in;
- (c) the specific products and services offered;
- (d) the delivery channels used to provide those services; and
- (e) the types of transactions undertaken.

Applicants must also explain how they review and update this ML/TF risk assessment. Under Section 3-6, VASPs must

outline their AML/CTF policies, including evidence of the knowledge, training and experience of key personnel in meeting AML/CTF obligations. Section 3-9 further requires due diligence on key personnel, including criminal history and findings from court proceedings or regulators.

Section 3-14 introduces additional requirements for VASP registration, including:

- the types of virtual assets offered in connection with registrable services;
- the delivery channels used to provide the services;
- how customers' virtual assets or funds may be used in exchanges;
- whether transaction or time limits will apply, and if so, their details;
- expected average monthly:
  - number of designated services provided; and
  - total value of customers' money, virtual assets, and property handled in the first 12 months after registration; and
- for each wallet controlled by the applicant, the types of virtual assets it can store and the wallet's address.

Transitional provisions are also proposed to allow VASPs to continue operating while AUSTRAC assesses their registration applications, helping to avoid unnecessary business disruption during the transition.

### ***Financial Sanctions Policies***

ED2 introduces a new requirement for all reporting entities to develop and maintain AML/CTF policies that ensure compliance with targeted financial sanctions (**TFS**), such as asset freezing, when providing designated services. For example, Section 4-12 of the ED2 Rules states that reporting entities must have policies to ensure that in providing its designated service, it does not *"use or deal with, or allow or facilitate the use of or dealing with, any money, property or virtual assets owned or controlled (directly or indirectly) by a person designated for targeted financial sanctions, in contravention of either of those Acts"*.

### ***Customer Due Diligence (CDD)***

Several updates have been made to Part 5 of the ED2, including:

1. removing the requirement to collect and verify a customer's place of birth (following submissions noting the difficulties of doing so);
2. allowing delayed verification of identification requirements for all reporting entities providing designated services, provided the conditions set out in the rules are met;
3. exempting certain low-risk customers from beneficial ownership due diligence such as government bodies, entities regulated by prudential, insurance, or investor protection authorities and publicly listed companies subject to disclosure obligations that ensure transparency of beneficial ownership; and
4. clarifying that the obligation to identify persons on whose behalf a service is provided is limited to establishing the beneficiaries of a trust (or foreign equivalents) on reasonable grounds (that is, there is no requirement to conduct CDD on a customer's customers).

### ***Suspicious Matter Reports (SMRs) and Threshold Transaction Reports (TTRs)***

ED2 provides new details on the required contents of SMRs and TTRs. These changes are meant to reflect the increased use of digital technologies and new financial products. Under Sections 8-4 (SMRs) and 8-8 (TTRs) of ED2, where the matter involves virtual assets, reports must include:

- (a) the type of virtual assets, including details of the backing asset (if any);
- (b) the quantity of virtual asset units;
- (c) the value in AUD;
- (d) the applicable exchange rate in determining the value;
- (e) the unique transaction reference number, including a transaction hash; and
- (f) the wallet address, including destination tag or memo details.

According to the [Consultation Paper](#), AUSTRAC will also be releasing new online forms for SMRs and TTRs.

### ***Transitional Arrangements for International Value Transfer Reports***

The Department of Home Affairs has proposed transitional arrangements to keep the current international funds transfer reporting framework in place until after 2026. This will give AUSTRAC and industry time to develop and consult on the new reporting requirements for:

- International value transfer services (under section 46 of the Amended AML/CTF Act), and
- Transfers involving unverified self-hosted virtual asset wallets (under section 46A of the Amended AML/CTF Act).

### ***The Travel Rule and Counterparty Due Diligence for Virtual Asset Transfers***

Section 66A of the Amended AML/CTF Act introduces the “travel rule”, which requires that certain identifying information about the payor and payee be transmitted with transfers of value, including virtual asset transfers.

However, a “sunrise issue” was raised during consultation. For example, Australian reporting entities may be required to transmit or receive travel rule information under domestic obligations but may interact with counterparties in jurisdictions where such requirements do not yet exist. To address this, subsections 66A(9) and (10) of the Amended AML/CTF Act provide limited exceptions. These permit an Australian reporting entity to omit travel rule information if it has reasonable grounds to believe that the counterparty institution:

- cannot securely comply with the travel rule, or
- cannot safeguard the confidentiality of the information.

AUSTRAC has stated that these are objective tests, and the reason for the determination must be documented.

Another question raised in submissions was *how* a VASP can undertake counterparty due diligence to determine whether a third-party virtual asset wallet is controlled by a regulated VASP, an unregulated VASP, an illegally operating VASP or is a self-hosted wallet. In response, AUSTRAC has stated that further guidance will be issued with examples of how to assess the status of a third-party wallet. Nonetheless, Section 4-13 of ED2 require entities to have AML/CTF policies that explain how they will undertake counterparty due diligence.

### ***Class Exemptions and Other Matters***

In addition to ED2, the exposure draft of the [AML/CTF Rules \(Class Exemptions and Other Matters\) 2007](#) has been released for public consultation for the first time. Only selected chapters are being retained, with most older provisions removed or replaced by updated rules in ED2. Some exemptions include issuing or selling a security or derivative in specified circumstances (Chapter 21), designated services related to OTC derivatives involving certain commodities or products (Chapter 22) and designated services to a risk-only life policy member of a superannuation fund under certain conditions (Chapter 47).

Submissions for the second round of consultation will close on 27 June 2025.

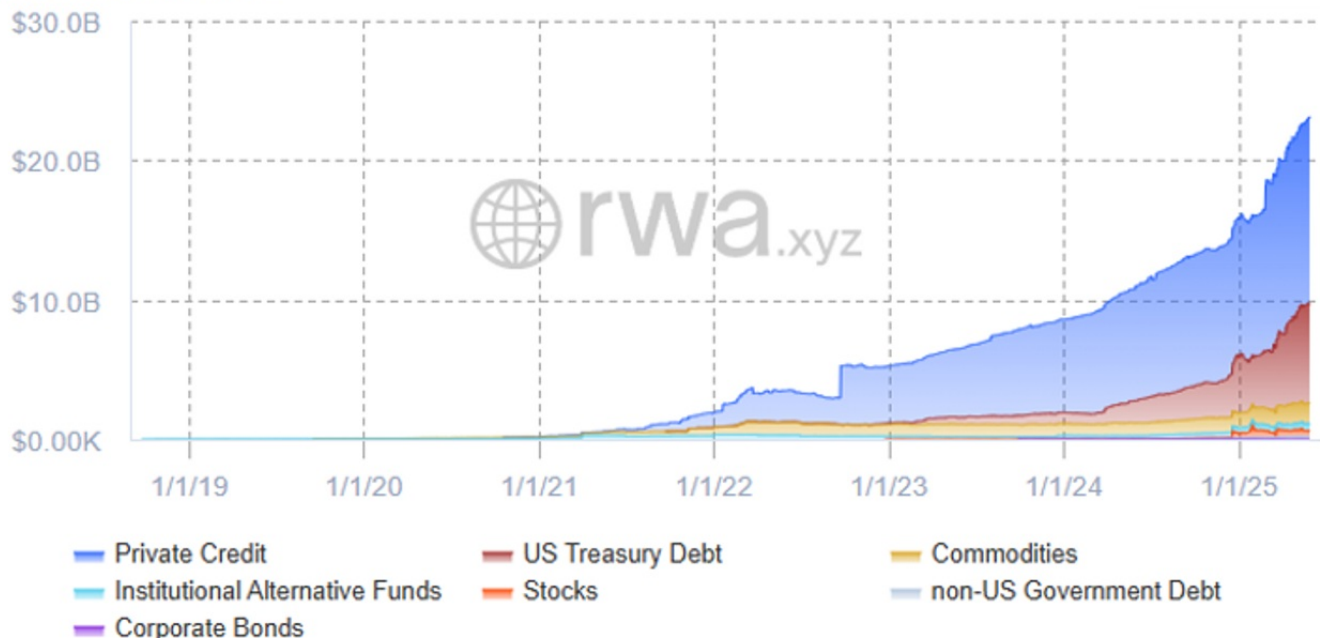
*By Steven Pettigrove, Luke Misthos and Emma Assaf*

### **Cayman Islands getting ready to launch RWA and tokenised securities with law update**

Real World Assets (RWA) and tokenised securities have been a growing and hot area of growth for blockchain and crypto, as businesses see the potential to move towards lower friction trading and interesting lending and other smart contract interactions, but using tokens which represent ownership in underlying assets. Total RWA's are reported to be US\$23B at present (excluding Stablecoins) and growing:

## Total RWA Value

Include Stablecoins



Many challenges need to be overcome before RWA and tokenised securities become a reality at present some offerings, like the xStock being announced on Kraken, and Midas, rely on “Blockchain based certificates” issued under Swiss/Lichtenstein laws which appear to restrict them to professional investors and rely heavily on exemptions to function, and other jurisdictions like the United Arab Emirates have recently announced plans to get real property on the blockchain (something which has been a holy grail for many).

Cayman Islands was early with a Virtual Asset Service Provider (**VASP**) regime and has long had a fit for purpose and well regarded fund regime, but uncertainties between when a token would fall under one regime or/and the other have been a point of concern, with most tokenised funds launching in the British Virgin Islands. That may be about to change, with the Cayman Ministry of Finance and Parliament releasing amendments to the [Virtual Asset \(Service Providers\) Act](#) making clear that tokenised funds and securities which meet certain requirements will not fall under the VASP Regime. The explanatory reasons for the amendment state the:

The ... new definition expands the meaning of the words “ “issuance of virtual assets” or “virtual asset issuance” ” to exclude, in accordance with a statement of guidance or rule that may be issued by [the Cayman Islands Monetary Authority], the issuance of an equity interest as defined under the Mutual Funds Act (2025 Revision) and the Securities Investment Business Act (2020 Revision) or an investment interest as defined under the Private Funds Act (2025 Revision).

Aaron Unterman, a professional director at IMS [said](#):

This alignment ensures that tokenized instruments fall under the most appropriate and tailored oversight—enhancing legal clarity and investor confidence.

Importantly, the legislative changes have *retrospective* effect, which may give past RWA projects a way to migrate safely into the regulatory framework.

The Cayman Islands Monetary Authority (**CIMA**) will have the opportunity for formal rule-making and to issue guidance, further providing clarity for tokenised funds and securities. In the interim this amendment continues the Cayman Islands’ lead as the preferred web3 jurisdiction for projects to reach the world.

By Michael Bacina

### Call of duty: ASIC sues Blockchain Global director

The Australian Securities and Investments Commission (**ASIC**) has launched civil penalty proceedings in the Federal Court against Liang “Allan” Guo, a former director of Blockchain Global Ltd (in liquidation), in connection with the collapse of the ACX cryptocurrency exchange, which [we wrote about in Feb 2020](#) when the exchange mysteriously changed the name of the operating company shortly before customers were unable to make withdrawals.

[According to ASIC's press release](#), the regulator alleges Mr Guo breached his duties as a director by misusing customer funds, failing to maintain proper records, and making misleading statements regarding the company's operations. The charges come in the wake of Blockchain Global's spectacular collapse in late 2019, when users of the ACX Exchange were abruptly unable to withdraw funds or crypto assets.

Blockchain Global was [placed into external administration](#) in 2022 following significant governance concerns and other missteps, including the refusal of a financial services licence and a halted IPO bid in 2017. Liquidator reports filed in October 2023 revealed that over AUD\$58 million was owed to unsecured creditors, more than AUD\$22 million of which was attributed to ACX customers. Investigations also uncovered that customer funds were co-mingled with company money and funneled into related entities, drawing parallels with other high-profile exchange failures.

ASIC's investigation formally commenced in January 2024, [culminating in interim travel restrictions on Guo](#). However, Guo departed Australia in September 2024, just weeks after the orders expired, and has not returned since.

Compounding concerns are Guo's claims to liquidators that private wallet credentials to millions in crypto were lost due to a laptop theft in China, an incident for which no police report was ever lodged.

The collapse has also spawned [new case law confirming the court's powers to order freezing orders in respect of cryptocurrency and that bitcoin may be treated as property](#) and is capable of being held on trust.

These proceedings mark a significant step in ASIC's pursuit of accountability in one of Australia's first and most notable crypto exchange collapses. The broader Blockchain Global saga continues to unfold, with co-director Sam Lee also facing legal scrutiny overseas for his alleged role in unrelated global investment schemes.

ASIC's decision to pursue director's duty breaches shows the broad tools which the regulator already has in hand to target alleged misconduct in the cryptocurrency sector notwithstanding that Blockchain Global was not an AFSL holder.

While the legal action demonstrates ASIC's willingness to enforce corporate compliance in the sector, the fact that Guo has already left the jurisdiction suggests that any judgment in the case will likely be of symbolic value rather than resulting in returns for creditors of the defunct exchange, highlighting that swift action is needed by regulators if justice is to be done.

*By Steven Pettigrove and Luke Misthos with Michael Bacina*