Article Information

Authors: Steven Pettigrove, Katrina Sharman, Will Deeb, Tahlia Kelly
Service: Banking & Finance, Banking & Finance Litigation, Blockchain
Sector: Financial Services, FinTech

Blockchain Bites: ASIC no-action deadline looms; Service in cyberspace: Victorian judgment targets crypto scams; Rewiring the system: ASIC consults on financial market infrastructure guidance

The Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

ASIC no-action deadline looms

ASIC issued a press release this week emphasising that digital asset businesses should move quickly to determine whether they are required to apply for an Australian financial services licence (**AFSL**), or a variation to an existing AFSL before ASIC's no-action position expires on 30 June 2026.

ASIC's no-action relief is a transitional position under which ASIC has indicated it does not intend to take enforcement action in respect of certain unlicensed financial services involving digital assets, provided a business lodges an AFSL (or variation) application by 30 June 2026 and complies with specified conditions while the application is determined. The relief also extends to some market operators and clearing and settlement facilities.

This announcement follows a period of significant regulatory change across the digital asset sector. The latest announcement concerns digital assets business involving financial services regulated under the current law. However, digital asset businesses will also need to grapple with further reforms in the near future. In particular, the passage of the *Corporations Amendment (Digital Assets Framework) Bill 2026 (Cth)* (**DAF Bill**) which will introduce new licence authorisations for Digital Asset Platforms (**DAPs**) and Tokenised Custody Platforms (**TCPs**) from April 2027.

In parallel to the no-action relief, ASIC's updated Information Sheet 225 (**INFO 225**) reinforces its long-standing position that many digital asset arrangements involve regulated services under the existing law. As a result, businesses must carefully assess their activities on a token-by-token and service-by-service basis to determine whether they operate under the AFSL regime. This includes considering whether products such as stablecoins, wrapped tokens, tokenised securities and wallet services constitute financial products requiring appropriate authorisations.

What is required for proposed licensees before the deadline?

Providers of financial services involving digital asset financial products should act promptly to determine whether their activities fall within the AFSL regime and, where required, take steps to continue offering services in Australia beyond 30 June 2026. In practice, this includes:

- applying for an AFSL or a variation to existing AFSL authorisations; or
- for entities that require an Australian market licence or clearing and settlement (CS) facility licence:
    - notifying ASIC in writing of their intention to apply; and
    - holding a pre-lodgement meeting with ASIC.

Firms that fail to take action before the deadline risk breaching financial services laws, exposing themselves to significant civil and criminal penalties, including substantial fines (which may reach up to 10% of annual turnover).

What questions should digital asset business be asking?

Businesses should now be actively assessing whether their current and proposed activities trigger AFSL requirements to continue operating in Australia. Key questions include:

- Have you assessed your product suite, including each token and service offering, to determine whether you are providing a financial service or operating a financial market?
- Can you rely on ASIC's no-action relief, or do you need to apply for a licence now?
- Have you identified and commenced the key steps required to apply for an AFSL or licence variation?
- Do you understand the core obligations applicable to AFS licensees, and how these may evolve under the emerging DAP and TCP regime?

If you require assistance understanding how these rules apply to your business, please reach out to the Piper Alderman Blockchain team. You can also access our licensing guide prepared in collaboration with the Digital Economy Council of Australia and Korda Mentha at this link.

Written by Steven Pettigrove and Tahlia Kelly

Service in cyberspace: Victorian judgment targets crypto scams

The County Court of Victoria has delivered a significant ruling in *Siegers v Nest Services Ltd & Ors* [2026] VCC 15, confirming that orthodox civil procedure rules can be deployed to pursue cryptocurrency fraud, even where perpetrators are unidentified and exchanges are offshore. In a practical win for scam victims, the Court allowed preliminary discovery against multiple cryptocurrency exchanges to obtain information capable of identifying the controllers of wallets through which allegedly stolen crypto moved. The Court also endorsed service by email on offshore exchanges, recognising the operational reality of globally-distributed, online crypto businesses.

Background

The applicant alleged that he had been induced, through misrepresentations by persons associated with a fictitious investment business, to transfer approximately AUD $463,000 into cryptocurrency during early 2023. The funds were converted to crypto (primarily USDT) and transferred through a series of wallets hosted by multiple cryptocurrency exchanges.

Forensic tracing identified wallet addresses, transaction hashes, and transaction flows across exchanges including Binance, Bitstamp, Galaxy Digital, KuCoin, HitBTC, N.Exchange and VALR. However, despite reasonable inquiries, the individuals controlling most of those wallets could not be identified. The exchanges indicated they held relevant KYC and account information but would only disclose it pursuant to court order.

The applicant therefore sought:

1. **preliminary discovery** under rule 32.03 of the *County Court Civil Procedure Rules 2018*(Vic) to identify potential defendants; and
2. **substituted service** under rule 6.10, given that most respondents were domiciled overseas and operated almost entirely online.

Preliminary discovery to identify crypto wallet holders

Rule 32.03 permits discovery where an applicant, having made reasonable inquiries, cannot sufficiently identify a prospective defendant, but another party is likely to hold information assisting that identification.

Judge Wise emphasised that the rule does not operate on a mere suspicion or "hunch", the applicant must establish a plausible case of wrongdoing. On the evidence, including forensic tracing reports and documentation of the applicant's losses, the Court was satisfied that the applicant had been defrauded and that the unidentified wallet holders were potentially involved in the wrongdoing.

A key issue was scope of permissible discovery. Rule 32.03 is directed to discovering documents that assist in identifying the "description" of a person, being terms defined to include matters such as name, residence, occupation and whether the person is an individual or corporation. At first glance, transaction records, IP addresses and account statements might appear to exceed that purpose.

The Court rejected a narrow reading and accepted that, in a crypto fraud context, transactional documents may assist in identifying wallet holders or downstream recipients of assets and therefore fall within the permissible scope of preliminary discovery, this is in light of the fact that the identity of one wallet holder was ascertained through IP addresses and email

addresses.

Substituted service on offshore exchanges

The Court granted substituted service under Rule 6.10 for seven of the eight exchanges.

Evidence showed that the exchanges operated digitally, had engaged with the applicant's solicitors via email or online portals, and had indicated they would act on court orders.

Applying established authority, the Court concluded that requiring formal service in multiple foreign jurisdictions (i.e., Seychelles, Luxembourg, New York, Hong Kong, Turks and Caicos Islands, Costa Rice and South Africa) would be impracticable and inconsistent with the overarching purpose of the *Civil Procedure Act 2010* (Vic). The Judge determined that email service was likely to bring the proceedings to the respondents' attention and was therefore appropriate.

Judge Wise stated:

> *…the respondents each operate their business almost entirely online. The choice of domicile of the corporation concerned is likely to be a matter of convenience to the corporation concerned…. I do note that all but one of the respondents have structured their affairs so as to engage with the applicant's solicitors via some electronic communications, whether by email (predominantly) and in one instance by a Zendesk-type ticketing arrangement.*

Service was deemed effective where documents had already been provided electronically. One respondent, which had not responded to any communications and for which no reliable electronic service method was available, was excluded from the substituted service orders.

Crypto as property – and why it matters

The Court's reasoning reflects a broader and increasingly settled judicial view that decentralisation or offshore structuring will not place digital asset activity beyond the reach of the courts where intermediaries exercise real control or hold identifying information.

That approach is consistent with views expressed by Judge Wise outside the courtroom. In a recent presentation on cryptocurrency fraud and civil procedure, his Honour addressed the treatment of cryptoassets as property – a question that has featured prominently in recent cases – and the practical consequences of that characterisation for proprietary claims, tracing and discovery. Those views are reflected in *Siegers* and sharply illustrate why characterisation matters.

As Judge Wise explained in that presentation:

> *"I accepted that the plaintiff's case was properly characterised as one involving the misappropriation of 'property', not merely the misuse of information… That characterisation informed both the availability and the scope of preliminary discovery."*

By framing cryptocurrency as property rather than information, the Court unlocked a full suite of proprietary and equitable claims – including deceit, constructive trust, knowing assistance and tracing – and was willing to deploy procedural tools to identify the persons controlling the wallets through which the assets had moved.

For fraud victims, this materially expands the remedies and procedural avenues available. For exchanges and intermediaries, it underscores that courts will look past technical labels and offshore structures to the underlying substance of how digital assets are held and controlled.

Conclusion

The decision confirms that Australian courts are prepared to pursue cryptocurrency fraud using orthodox civil procedure tools, even where perpetrators are unidentified and platforms operate offshore. By taking a pragmatic approach to discovery and service, the Court signalled a willingness to look through digital structures and jurisdictional complexity to the reality of how crypto assets are controlled. For fraud victims, this materially strengthens available remedies. For exchanges and intermediaries, it underscores growing judicial scrutiny of businesses that hold transaction-level or identifying information, sharpening the focus on compliance, engagement and litigation-risk strategy.

Written by Steven Pettigrove, Katrina Sharman, Will Deeb and Tahlia Kelly

Rewiring the system: ASIC consults on financial market infrastructure guidance

Following the commencement of Australia's reformed financial market infrastructure (FMI) regime late last year under the *Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Act 2024* (Cth), ASIC has released Consultation Paper 50 (CS 50).

CS 50 proposes targeted updates to ASIC's regulatory guidance to give practical effect to the new framework and ASIC's expanded powers.

1. **What guidance is changing?**

ASIC is proposing updates to three cornerstone Regulatory Guides:

- RG 172 *Financial markets: Domestic and overseas operators*;
- RG 249 *Derivative trade repositories*; and
- RG 268 *Licensing regime for financial benchmark administrators*.

Together, these guides apply to the vast majority of entities that enable, facilitate, and support trading in Australia's capital markets.

2. **Why these reforms matter**

The changes implement long-standing recommendations from the Council of Financial Regulators (July 2020), aimed at addressing three structural weaknesses in Australia's FMI regime:

1. **Crisis management and resolution**: enabling FMIs to be stabilised or resolved without systemic disruption
2. **Licensing enhancements:** modernising licensing frameworks to reflect operational complexity and cross-border activity; and
3. **Stronger supervision and enforcement**: giving regulators earlier and sharper intervention tools.

What is CS 50?

Broadly, CS 50 aims to:

- align ASIC's guidance with the reformed legislative framework and expanded powers;
- explain how ASIC will apply new statutory concepts introduced by the FMI reforms;
- promote consistency in definitions and regulatory approach across FMI settings; and
- streamline and "market-neutralise" guidance by removing outdated and ASX-centric assumptions.

Key themes and practical takeaways

Key issue	Summary of changes
New statutory concepts explained	CS 50 provides ASIC's first detailed articulation of how it will apply several new statutory concepts, including: • the '*material connection test*' for overseas entities, replacing the more impressionistic 'targeting Australia' analysis; • 'fit and proper' and 'capability' obligations for core officers; and • the expanded control and ownership approval regime.
Market neutrality and simplification	Legacy references are stripped out, guidance is consolidated, and assumptions tied to a single market operator model are wound back — signalling a more flexible, market-neutral approach.
Transfer of Ministerial powers to ASIC	The guidance reflects ASIC's shift from adviser to decision-maker, following the transfer of key powers from the Minister. ASIC now directly determines licence grants, conditions, suspensions, cancellations and rule disallowance — aligning Australia more closely with international FMI supervision models.

Sharper Governance expectations	Across RG 172, RG 249 and RG 268, ASIC reinforces expectations that licensees actively monitor and document the fitness, propriety and capability of core officers. While the legislation sets high level obligations, ASIC flags it will draw on familiar AFSL, credit and ADI fit-and-proper frameworks when assessing compliance.
Overseas entities: trigger for licensure	The updated guidance reflects a statutory two-step test for offshore FMIs: 1. is there a connection with Australia? and 2. if so, is that connection material?
Control and ownership approvals	The consultation also explains the new requirement for ASIC approval where ownership or voting power exceeds 20% in a domestically incorporated FMI licensee. ASIC applies a legitimate control test, and CS 50 clarifies that: • ownership approvals are assessed separately from licence applications; and • approvals may be considered concurrently but are not automatically bundled.
Expanded supervisory toolkit	The guidance highlights ASIC's enhanced information-gathering and supervisory powers, including the ability to require licensee-funded expert reports, suspend or cancel licences due to inactivity, and intervene earlier where emerging risks are identified.

For FMI operators, now is a timely chance to consider the impact of the new rules, revisit cross-border assumptions and engage early with ASIC, while the regime and ASIC's supervisory posture is still taking shape.

Submissions on CS 50 can be made to submissions-fmi.reforms@asic.gov.au until 25 May 2026.

Written by Steven Pettigrove, Katrina Sharman and Tahlia Kelly