

When the wrongdoer is unknown

Protecting misappropriated assets through the courts

Australia – October 2026

What can you do when your property has been stolen or misappropriated, but you do not know who is responsible? Whether the subject matter is money, cryptocurrency, confidential documents or commercially sensitive data, identifying the perpetrator is often difficult, particularly where transactions cross borders or run through digital platforms.

A recent English High Court decision, *Wilden v Person Unknown & Anor* [2026] EWHC 1355 (KB), illustrates two important points. First, it is not always necessary for victims to identify the wrongdoer before seeking urgent court intervention to protect their assets and pursue recovery. Secondly, courts can make orders for the disclosure of information needed to pursue legal action.

The decision

In *Wilden*, Deputy High Court Judge Guy Vassall-Adams KC continued, until trial:

1. A proprietary and worldwide freezing injunction against the unidentified fraudster
2. A disclosure order against Huobi Global S.A, the company believed to own the HTX cryptocurrency exchange, which was believed to hold the stolen Bitcoin and the information needed to identify the perpetrator

The claimant, a German businessman, received a cold call from a man identifying himself as “Brian Smith”, who offered to help him recover Bitcoin stranded on a platform that had closed in 2021. Smith persuaded him to buy fresh Bitcoin and send it to wallets that Smith controlled, as part of supposed regulatory steps. Over December 2025 and January 2026, the claimant purchased about €2.6 million (approximately AUS\$4.2 million) before being locked out.

Forensic investigators traced the Bitcoin through 49 transactions into two “scam wallets” and onwards to infrastructure associated with HTX. The perpetrators had pooled the funds with other assets to obscure their origin, but the investigators were still able to isolate the claimant’s share. The investigators noted that a centralised exchange, such as HTX, would be expected to hold know-your-customer information on the account holder.

Freezing injunction

The Court was satisfied that the requirements for a freezing injunction to protect the traced assets were met:

1. A good arguable case on the merits
2. A real risk that any judgment would go unsatisfied due to the dissipation of assets
3. That it was just and appropriate, as a matter of discretion, to grant the injunction

The claimant had a good arguable case in deceit, and the Court accepted that cryptocurrency could attract proprietary rights and remain identifiable despite mixing with other assets. The Court also found a “very high” risk of dissipation, given the perpetrator’s attempts to conceal the Bitcoin through pooling transactions and the exchange’s failure to assist in its recovery.

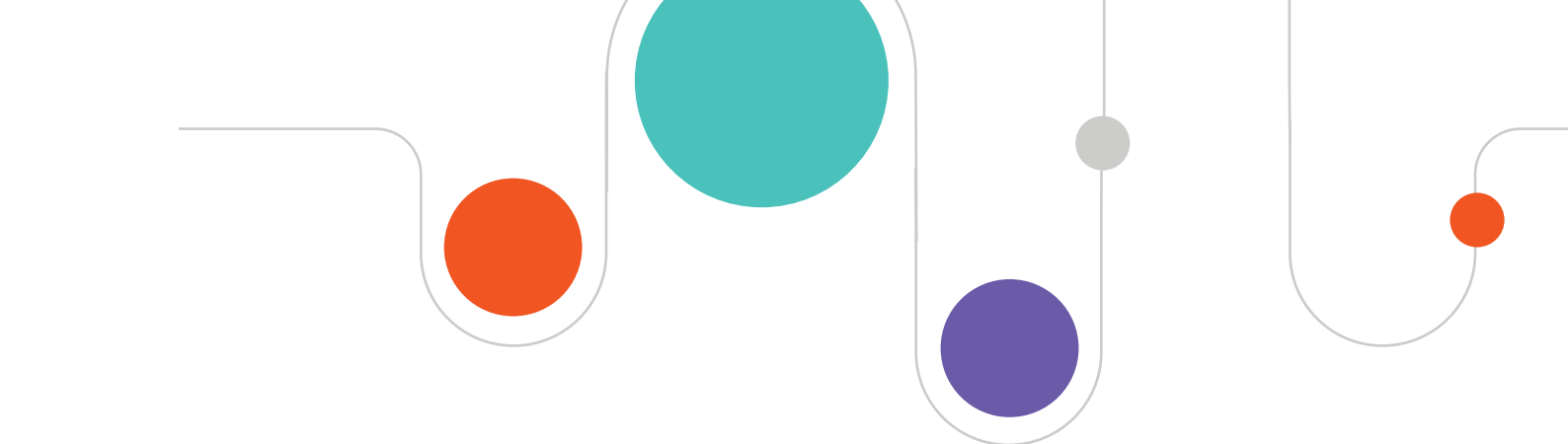
Disclosure order

An order requiring disclosure of information about the customer was made against Huobi under the *Bankers Trust* jurisdiction, applying the principles enunciated in *Kyriakou v Christie Manson & Woods* [2017] EWHC 487 (QB). These require:

- Good grounds for believing that identified assets belong to the claimant
- A real prospect that the requested information will lead to their location or preservation
- The court being in position to make appropriately tailored orders that are no wider than necessary to achieve the interests of justice
- The orders being appropriate when the interests are the parties are balanced
- The offering of appropriate undertakings as to damages

In this case, the Court was content to accept the claimant’s undertakings despite his limited means, as the fraud had taken his life savings.

The Court also addressed a practical obstacle: how to notify parties who cannot easily be found. It gave permission to serve the application on Huobi, a Panama-incorporated company, outside the jurisdiction, and allowed service by email. It also allowed the claim to be served on the unknown fraudster by email.



Finally, the Court awarded the claimant his costs of £60,993.91 (approximately AUS\$116,000) on an indemnity basis against both defendants. It described Huobi's failure to engage with the claimant's requests for information as "wholly unreasonable", noting that a cooperative response might have avoided a costs order.

In practical terms, what this case demonstrates is that not knowing a defendant's identity or location need not stall urgent proceedings.

The position in Australia

Comparable remedies are available in Australia.

Australian courts have jurisdiction to grant freezing orders over assets located within or outside Australia, together with ancillary orders for disclosure of information concerning those assets. These powers are reflected in the *Federal Court Rules 2011* (Cth) (rr 7.32–7.37) and equivalent rules of state and territory courts.

Australian courts have also granted injunctions against unidentified defendants. By way of example, in *HWL Ebsworth Lawyers v Persons Unknown* [2024] NSWSC 71, the Supreme Court of New South Wales restrained unidentified hackers from using or disclosing confidential information obtained through a cyberattack. Similarly, in *Qantas Airways Ltd v Persons Unknown* [2025] NSWSC 776, the Court considered urgent injunctive relief against unidentified persons following a cybersecurity incident.

Preliminary discovery and other disclosure mechanisms may also assist in identifying unknown wrongdoers and tracing misappropriated assets.

Importantly, these remedies are not limited to cryptocurrency or conventional financial assets. Depending on the circumstances, injunctive relief may be available where a wrongdoer has misappropriated money, documents or commercially sensitive data, or obtained unauthorised control of digital infrastructure, including through compromised administrator credentials. Although data and confidential information are not necessarily recognised as property under Australian law, they may be protected through equitable obligations of confidence and appropriately framed injunctions.

Key takeaways

- Not knowing the wrongdoer's identity does not prevent urgent court action. Freezing and disclosure orders can work together to preserve assets and identify those responsible.
- Early forensic tracing is critical. Evidence that the assets remained identifiable despite pooling underpinned both orders.
- Platforms that stonewall legitimate requests risk being joined to proceedings and facing indemnity costs.
- Acting early is essential in preserving evidence, preventing further loss and improving the prospects of recovery.

Authors



Scott Crabb
Partner, Perth
T +61 8 9429 7582
scott.crabb@squirepb.com



Richard Shaw
Associate, Perth
T +61 8 9429 7403
richard.shaw@squirepb.com