Davis Polk

Hong Kong Court discharges proprietary injunction against cryptocurrency exchange Binance

November 21, 2025 | Client Update | 6-minute read

On 17 October 2025, the Hong Kong Court of First Instance discharged a proprietary injunction obtained ex parte against a Binance digital asset wallet allegedly containing cryptocurrencies stolen from the plaintiff, due to the plaintiff's failure to provide full and frank disclosure and failure to demonstrate urgency and secrecy.

Introduction

This decision concerned the jurisdiction of the Court to grant *ex parte* injunctive relief and the requirements for any such application. As far as legal principles are concerned, the decision traverses very familiar ground: it is a classic example of the discharge of an *ex parte* interim injunction on the grounds of (i) failure to comply with the duty of full and frank disclosure on the part of the applicant and (ii) the absence of the fundamental pre-requisites for applying to the Court *ex parte*, i.e. the lack of urgency or secrecy.

However, this briefing highlights other elements of the decision which address more interesting issues relevant to cryptocurrency trading platforms and custodians and those dealing with them, including (i) the question of identification of the proper defendants; (ii) the use of a *Bankers Trust* order compelling disclosure by virtual asset trading platforms and custodians; and (iii) the steps Binance took prophylactically to render an application for a freezing order unnecessary and inappropriate.

Background facts and procedural history

The plaintiff claimed that various cryptocurrencies had been stolen from him. He traced the assets to several virtual asset wallets, including one pooled funds hot wallet of the cryptocurrency exchange known as Binance.

In correspondence between Binance and the plaintiff, Binance explained that the digital assets stored in pooled fund hot wallets did not legally belong to any single user, but to multiple users. Therefore, while Binance agreed to provisionally freeze funds in specific Binance accounts identified by the plaintiff, it declined to freeze funds in the pooled funds hot wallet.

The plaintiff subsequently applied for, and obtained, *ex parte* Mareva and proprietary injunctions over a number of Binance wallets, including the pooled funds hot wallet.

Binance challenged the injunctions against the pooled funds hot wallet on the basis that (a) the plaintiff failed to give full and frank disclosure as the plaintiff did not draw the court's attention to its correspondence with Binance where Binance explained the nature of the hot wallet, and (b) there was no justification for proceeding on an *ex parte* basis without notice.

Prior to the hearing, the plaintiff agreed to discharge the Mareva injunction against the hot wallet, so the ruling concerns the proprietary injunction only.

Highlights of decision

Identification of one of more unknown entities in large business organization

The plaintiff's application was initially taken out against the 1st defendant, the plaintiff's assistant who the plaintiff suspected as a perpetrator of the fraud, and unknown 2nd defendants described in the writ as "unknown person or person(s) who has access to or operates" a list of wallets allegedly containing cryptocurrencies which can be traced back to the plaintiff.

In a previous application, the plaintiff applied to join "Binance Operators" as unknown 3rd defendants to the proceedings. "Binance Operators" was described as "Binance Operators (being all parties that run Binance, including but not limited to legal persons (including Binance UAB), Unincorporated Organisations and Teams that provide Binance Services and are responsible for such services)", based on the terminology used in the terms of use of Binance.

The Court pointed out that the description given by the plaintiff for "Binance Operators" included "Binance UAB," a specifically identified entity, and remarked that joinder of "persons unknown" should only be granted against defendants who have not been identified. Any person fitting the description that is known and identified must be joined as an individual defendant.

Ultimately, the plaintiff was granted leave to withdraw his joinder application and to take out a fresh application, but the plaintiff never did. Instead, Nest Services Ltd identified itself as the operator of Binance fitting the definition of the 2nd Defendant. Nest's application for leave to intervene was not opposed and Nest was joined as the 3rd defendant upon the plaintiff's unopposed application.

The case highlights the point that the Court has jurisdiction to assist plaintiffs facing large, opaque business organisations and take a flexible approach to allow proceedings to be pursued against unknown entities, for so long as they remain unknown, with the Court being perhaps particularly sympathetic when business organisations are not transparent about their corporate structure and the specific entities involved. This is not an uncommon feature of the crypto industry, where services may be unregulated or decentralised. But it also highlights the importance of careful consideration from the outset of the extent to which the proper operator of cryptocurrency products and services can be identified, and not lumping together known and unknown entities.

Disclosure order against third party operators and custodians to trace stolen crypto assets and funds

The Court held that *Bankers Trust* jurisdiction could be invoked to compel the unknown 2nd defendants and Nest to use best endeavours to provide (i) details of the Binance accounts identified by the plaintiff as having received the allegedly stolen funds (the Relevant Accounts), (ii) details of accounts or addresses to which cryptocurrencies had been transferred from the Relevant Accounts and (iii) the date, time, currency and amount of the relevant transactions, in order to enable the plaintiff to further trace his assets.

In granting the order, the Court noted that a *Bankers Trust* order had previously been made compelling disclosure from Binance, in its capacity as a cryptocurrency exchange, in the English case *Ion Science Ltd v Persons Unknown* [2020] EWHC 3688 (Comm).

The *Bankers Trust* order was made subject to the plaintiff's undertaking to indemnify Binance in respect of its costs of complying with the disclosure order; demonstrating that the Hong Kong Court will follow the English courts in making *Bankers Trust* orders available against cryptocurrency exchanges to aid in tracing of digital assets.

Steps taken by Binance prophylactically to render an application for a freezing order unnecessary and inappropriate

When the plaintiff first notified Binance of the alleged theft and tracing of funds to Binance wallets, Binance agreed to place a temporary courtesy freeze for 7 days on the Binance accounts identified by the plaintiff, stating that the freeze was to allow time for law enforcement agencies to make a direct official request for assistance or for the plaintiff to secure a freezing order.

Binance stipulated that if the account holder queried why their account is frozen, Binance may inform the user of the allegations and, if appropriate, supply them with a copy of the correspondence.

Binance also explained in correspondence the nature of the pooled funds hot wallet. When a Binance user deposits cryptocurrencies into their Binance account, the user would initially transfer such assets to a deposit address that is linked and assigned to their Binance account. Deposited cryptocurrencies are periodically swept from these deposit addresses into Binance's pooled funds hot wallet address used to store cryptocurrencies deposited by multiple users. Thereafter, a user's entitlement to their assets is tracked by reference to the user's account ledger rather than the deposit wallet address.

Practical conclusions

The use of pooled funds wallets is standard for centralised cryptocurrency exchanges and custodians.

Platform operators and custodians should be ready to quickly respond to tracing claims by voluntarily putting in place temporary freezes on accounts or wallets, provided the claims contain appropriate details. But generally, these voluntary freezes should be short-lived and not inappropriately impact other persons with interests held through the platform or wallets.

Platform operators and custodians should ensure their terms of business and operation are drafted so as to permit appropriate temporary freezes and review the terms before imposing any freeze.

Dry-run modelling against various potential fraud and claim scenarios is desirable.

Prospective plaintiffs should bear in mind the distinction between user accounts and the platform's client wallet, with the former of which typically tracking funds belonging to a specific user, and the latter of which typically containing funds belonging to multiple users.

Prospective plaintiffs should ensure that any application for injunctive relief is appropriately framed: it is generally inappropriate to freeze funds in pooled funds wallets, as it will cause significant disruption to the operations of an exchange.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Martin Rogers
+852 2533 3307
martin.rogers@davispolk.com

James C. Lin
+852 2533 3368
james.lin@davispolk.com

Yuan Zheng
+852 2533 1007
yuan.zheng@davispolk.com

Lok Cheung
+852 2533 1029
lok.cheung@davispolk.com

Sophie Ng
+852 2533 1012
sophie.ng@davispolk.com