Neutral Citation Number: [2026] EWHC 1355 (KB)

Case No: KB-2026-000801

IN THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 5th June 2026

Before :

DHCJ GUY VASSALL-ADAMS KC

- -

Between :

STEPHEN WILDEN **Claimant**

- and -

1. PERSON UNKNOWN

2. HUOBI GLOBAL S.A
(a company incorporated in Panama) **Defendants**

- -
- -

Damian Falkowski (instructed by **W Legal**) for the **Claimant**
The Defendants did not appear and were not represented

Hearing date: 14 May 2026

- -

Approved Judgment

This judgment was handed down remotely at 2pm on 5th June 2026 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

Deputy High Court Judge Guy Vassall-Adams KC:

Introduction

1. This is the return date of an application for injunctive relief in the form of a proprietary and worldwide freezing order against an unknown person who stole Bitcoin valued at about EUR 2.5 million from the Claimant and for a disclosure order against Huobi Global S.A, the owner of the cryptocurrency exchange HTX, which is believed to hold the relevant cryptocurrency and to know the identity of the account holder who perpetrated the fraud.

2. A proprietary and worldwide freezing order (the "Freezing Injunction") against the unknown person, who used the name Smith in his dealings with the Claimant ("Smith"), was granted on a without notice and urgent basis by Mrs Justice Obi on 17 March 2026. On the same occasion, Obi J granted a without notice and urgent disclosure order against Huobi Global SA ("Huobi"). These orders were served on the Defendants and they were put on notice of this return date, but there has been no response from Smith, while Huobi have replied by email suggesting the Claimant contacts the police but failing to comply with the Court's order. The issue for me is whether these injunctions should be continued until trial.

The parties

3. The Claimant is a German businessman who has worked in industry and mechanical engineering throughout his 25-year career. For the last 10 years he has been the managing director of a medium-sized German engineering company. The Claimant is not, and never has been, a crypto trader or speculator.

4. The First Defendant is an unknown person, believed to be of English nationality, who used the alias Brian Smith and who fraudulently induced the Claimant to transfer to him Bitcoin valued at 32.457826 BTC (EUR 2,586,845), in the circumstances described in this judgment.

5. The Second Defendant, Huobi Global SA, is the company which is believed to own the global cryptocurrency exchange HTX. According to experts instructed by the Claimant, the Claimant's Bitcoin can be traced into the hands of this exchange. HTX maintains a public online presence, including the website htx.com, where it markets itself as "Trusted by 59 Million Users for 12 Years". Relevantly for the purpose of this application, HTX is on the Financial Conduct Authority ("FCA") Warning List for operating in the UK without proper authorisation and the FCA has commenced legal proceedings against HTX in the Business and Property Courts (Claim FS-2025-000015) for communicating financial promotions in the UK contrary to s.21 of the Financial Services and Markets Act 2000.

Factual background

Bitcoin held on EuropeFX

6. In or around 2019, the Claimant made his first investment in cryptocurrencies. He purchased Bitcoin through an online platform known as EuropeFX, but did not actively trade it, he simply left the Bitcoin on that platform. The Claimant cannot now recall

precisely how much Bitcoin he purchased, what fees were deducted by the platform, or whether the Bitcoin increased in value while it remained on the EuropeFX platform.

7. EuropeFX subsequently ceased operating as an online platform in or around 2021 and the Claimant was unable to recover the Bitcoin held there. The Claimant does not know precisely what happened to the platform or why it closed. At that time, the Claimant did not pursue recovery of his Bitcoin. He was unsure how to go about recovering the Bitcoin and he was uncertain whether it would be worthwhile incurring legal costs in attempting to recover it. He therefore considered it lost.

Contact with Smith and the transfer of funds

12. On 1 December 2025, the Claimant received an unsolicited cold call to his work mobile phone from a man who introduced himself as "Brian Smith". Smith said that he was a UK-based investment adviser. The Claimant's records show that Smith contacted the Claimant using the following British telephone numbers: +44 1384 954328 and +44 20 7096 6186.

15. Smith's email address was brian-smith@europe.com. Smith spoke English with what the Claimant perceived to be a British accent. Although the Claimant is a German national and his first language is German, he also speaks good English.

16. During their initial phone call, which lasted about an hour, Smith told the Claimant that he was working for a company called LedgerLock and that LedgerLock was working together with EuropeFX. During that conversation Smith revealed that he was aware the Claimant had invested in Bitcoin on the EuropeFX platform in or around 2019. Smith told him that he would be able to transfer the Bitcoin that had effectively been lost on EuropeFX to a new wallet that he was proposing to create for the Claimant. In that way, Smith offered to help the Claimant to recover his Bitcoin.

17. The Claimant did not know how Smith knew about his Bitcoin investments with EuropeFX or his lost 2019 Bitcoin purchase. During that call, Smith demonstrated a detailed knowledge of the Claimant's transactions in his EuropeFX account and referred specifically to the date of purchase, account balances, trades, credits and withdrawals. Smith said that he had access to EuropeFX and was working closely with the platform. Because of Smith's apparent inside knowledge the Claimant believe that he was legitimate and had institutional access to the platform. However, the forensic investigators which the Claimant subsequently instructed believe that this information may have been obtained from publicly available blockchain data or from purchased databases.

19. During the conversation Smith informed the Claimant that his Bitcoin was not safe on EuropeFX as it was an unregulated platform. The upshot of the call was that Smith persuaded the Claimant that the only realistic way for him to recover his Bitcoin was for Smith to create a LedgerLock wallet for him and move the Bitcoin from EuropeFX to that wallet. Smith said that this would allow the Claimant to regain access to the Bitcoin and ultimately withdraw it in Euros to his German bank account and that Ledgerlock would assist him in presenting the relevant tax documentation to the German tax office.

20. During the call, Smith used AnyDesk software to enable the Claimant to share his computer screen with him. Smith instructed the Claimant step-by-step in assisting him to set up a LedgerLock blockchain wallet with a password and what the Claimant believed was two-factor authentication (although the forensic investigators subsequently instructed by the Claimant have advised him that this was not genuine two-factor authentication). Smith then informed the Claimant that he had already transferred the Bitcoin from EuropeFX into that newly created LedgerLock wallet. Smith showed the Claimant the balance on the LedgerLock wallet and pointed out that it contained approximately 1.3 Bitcoin (BTC).

21. Smith then persuaded the Claimant to undertake what he described as the "IBM process". Essentially, the Claimant was led to believe that in order to regularise and secure the transfer of his Bitcoin from EuropeFX to Ledgerlock and to ensure that that the Bitcoin could then be transferred to a mainstream exchange and back into Europe, the Claimant would need to make a number of payments using Bitcoin in order to satisfy various technical and regulatory requirements. As a result of this conversation, the Claimant believed he needed to buy further Bitcoin and deposit it in the LedgerLock account. Smith also persuaded the Claimant that Bitcoin was an excellent investment and that his LedgerLock account would be profitable.

22. In subsequent weeks, the Claimant transferred Euros from his German bank account to a number of well-known cryptocurrency exchanges (Crypto.com, OKX, Binance and Kraken) where he purchased Bitcoin. Smith assisted the Claimant with buying the Bitcoin on the exchanges, using screen-sharing. After purchasing the Bitcoin, the Claimant transferred the Bitcoin onwards to the LedgerLock account that Smith had created for him. In the course of many transactions in December 2025 and January 2026 the Claimant paid out about Euros 2.6 million which were converted into 32.4572826 Bitcoin via the cyptocurency exchanges and then transferred to two Ledgerlock wallets.

23. In January 2026, the Claimant requested Smith to transfer some Bitcoin back into his Binance wallet and Smith arranged for a small transfer back to him. The Claimant also utilised the "Support" function on the Ledgerlock platform on multiple occasions, believing that he was interacting with a legitimate platform. On 26 January 2060 Smith told the Claimant that that the final "IBM step" was complete and the Ledgerlock dashboard showed Bitcoin sent back to Binance. But no Bitcoin arrived. The Claimant found himself locked out of Ledgerlock. His password no longer worked. Smith stopped responding. The Claimant realised that he had been the victim of a fraud.

Forensic tracing

24. The Claimant instructed specialist forensic investigators, Crypto Forensiq, to analyse the cryptocurrency transactions associated with the transfers that he made during the course of the fraud. Their report dated 15 March 2026 is exhibited to his affidavit.

25. The report explains that the investigators carried out a forensic blockchain analysis using specialised analytical tools and blockchain explorers in order to trace the movement of the Bitcoin transferred by the Claimant and to identify the destination wallets and exchanges involved. The analysis uses what they refer to as LIFO (Last-In-First-Out) method. The investigators explain that this is a recognised methodology used in

such investigations and enables an analysis to be made of movements between the victim's loss and the destination platform.

25. The analysis confirms that between 1 December 2025 and 26 January 2026 the Claimant transferred a total of 32.4572826 Bitcoin, with an approximate value of EUR 2,586,845.42, in connection with the fraudulent scheme.

26. The investigators identified the cryptocurrency exchange wallets from which the Bitcoin originated. These include wallets associated with the exchanges Binance, Crypto.com, OKX and Kraken. The report further identifies the destination wallet addresses to which the Bitcoin was initially transferred. These are described in the report as self-hosted wallets controlled by the perpetrators and are referred to in the report as the "scam wallets."

27. The report identifies the principal scam wallet addresses as:
    a) bc1qmf4k5unf8m3eqta2qczkf5hj7yxx9y8de0tua0
    b) bc1qvhmhd2mcvrrmd2h76dg3r0qmmj70p4prmxx9tr

28. The investigators confirmed that the Bitcoin was transferred from the Claimant's exchange wallets to those scam wallets in 49 separate transactions. The analysis successfully traced 100% of the lost assets (32.4572826 BTC) to infrastructure associated with the HTX cryptocurrency exchange.

29. The investigators analysed the subsequent movement of those funds through additional intermediary wallet addresses. The report explains that the perpetrators used pooling transactions in which funds from multiple wallets are combined before being transferred onwards. The investigators state that this technique is commonly used to obscure the origin of cryptocurrency funds.

30. Despite these attempts to obscure the transaction trail, the investigators were able to trace the Bitcoin through the blockchain and determined that the assets were ultimately transferred to infrastructure associated with the HTX cryptocurrency exchange (formerly Huobi). The report includes a detailed transaction table identifying the specific transfers to HTX, including the recipient address, transaction hash, the amount of Bitcoin transferred, and the date of each transfer.

31. The report further explains that the total amount received by the HTX infrastructure (33.03826 BTC) exceeds the Claimant's individual loss because the perpetrators combined his assets with funds from other sources through pooling transactions. The report therefore calculates the Claimant's specific "share of loss" within those pooled transactions, ensuring that the traced amount attributable to his transfers is precisely limited to the 32.4572826 BTC that he had transferred.

32. The investigators point out that as HTX is a centralised cryptocurrency exchange it would be expected to operate under Know-Your-Customer and Anti-Money-Laundering procedures, which means that the exchange should hold identifying information relating to the account holder controlling the receiving wallet.

Contact with HTX

33. The Claimant's lawyers contacted HTX making a number of specific requests, namely that it identifies all accounts and sub-accounts receiving the traced Bitcoin; freeze Bitcoin to the value of the Claimant's Bitcoin; prevent any withdrawal, transfer, conversion or dissipation and preserve all Know-Your-Client documentation, access logs, IP logs and transaction records.

34. HTX's replies have been dismissive and non-cooperative. Instead of engaging with the substance of the Claimant's requests, HTX's replies are entirely formulaic, recommending that the Claimant informs the local police, saying that his request will be escalated and so on. HTX has conspicuously failed to provide any meaningful assistance to the Claimant. What the correspondence shows is that HTX, a company which markets itself on the basis of its trustworthiness, is unwilling properly to engage with a legitimate request for the return of stolen cryptocurrency and is thereby providing a safe haven for the proceeds of crime. Presumably this is something that Smith and the other persons unknown who are behind this fraud are aware of and rely upon.

35. The Claimant's concerns are heightened by the fact that HTX is currently the subject of proceedings brought by the Financial Conduct Authority for marketing cryptocurrency in this jurisdiction without authorisation, contrary to s.21 of the Financial Services and Markets Act 2000. The FCA's claim is brought under Claim No FS-2025-000015 and the FCA's Particulars of Claim refer to the fact that the company hides its true ownership and hides the identities of the persons who control it.

36. This was a sophisticated fraud carried out by a person with a detailed knowledge of the Claimant's previous Bitcoin transactions and a high degree of knowhow about cryptocurrency transactions. I have included Smith's *modus operandi* in this judgment as it seems likely to me that there may well be other victims of this fraud. I suspect many Bitcoin investors, like the Claimant, have only a superficial knowledge of how cryptocurrencies work, making such investments fertile ground for fraudsters. The fact that there are unregulated exchanges operating online behind hidden ownership and management structures heightens the risks still further as there is nobody to hold to account when they refuse to return stolen funds.

The Freezing Injunction

Legal Framework

37. The power to grant a freezing injunction is part of the High Court's general armoury to grant injunctions in any case in which it appears to it to be "just and convenient" to do so, pursuant to s.37 of the Senior Courts Act 1981. Part 25 of the CPR contains provisions on the full range of interim remedies, including freezing injunctions. The rules provide, among other things, that evidence in support of a freezing injunction must be in the form of an affidavit and that freezing injunctions must use the wordings of the Model Order. These requirements have been complied with in this case and the Freezing Injunction of Obi J, which I am asked to extend, is based on the Model Order.

38. The purpose of a freezing injunction is to prevent the respondent from disposing of his assets which could be used to satisfy a judgment in the claimant's favour. In the case of an interim injunction, this restraint lasts until the claim has been determined at trial.

39. In summary, an applicant for a freezing injunction must persuade the Court of three matters:

    (1) The claimant has a good arguable case on the merits against the defendant;
    (2) There is a real risk that a judgment or award may gone unsatisfied by reason of the unjustified disposal by the defendant of his assets, unless he is restrained by court order from disposing of them;
    (3) It is just and appropriate as a matter of discretion to grant the injunction.

Assessment

40. As to the first requirement, it has recently been held that, at least for the purposes of interim applications, there is a good arguable case that crypto assets are to be treated as assets to which property rights can attach: *D'Aloia v Persons Unknown and Ors* [2024] EWHC 2342 (Ch) at [107], [115]. Furthermore, not just the remedy of tracing, but the remedy of following is also available as a matter of principle if the evidence shows that the identity of the crypto asset is preserved despite mixing: see [210]. I am satisfied on the basis of the Claimant's expert report that the identity of the crypto assets has been preserved here.

41. At the time of the hearing the Claimant had not yet issued a claim form, but in his skeleton argument the Claimant referred to potential claims in civil fraud generally with specific reference to claims in deceit and conversion among others. It is not necessary for me to address each of the potential claims as I am satisfied that the Claimant has a good arguable case that the elements of a claim in deceit are made out and it does not appear that Smith would have any defence to such a claim.

42. It is self-evident that in a case of fraud there will be a real risk that a claimant's crypto assets will be dissipated and that any judgment in the claimant's favour will go unsatisfied. In this case there is a very high risk of dissipation as the Claimant's expert evidence shows that Smith has already tried to dissipate the Claimant's cryptocurrency through "pooling transactions" involving other crypto assets. Smith has also placed the Claimant's Bitcoin on the HTX platform, which has shown no willingness to assist in the return of the Claimant's stolen cryptocurrency.

43. I consider that a Freezing Injunction is just and appropriate in this case. This was a serious fraud which has had devastating consequences for the Claimant, resulting in the loss of his life savings. The Claimant has a good arguable case on the merits. The risk of dissipation is very high as Smith has already tried to obscure the origin of the cryptocurrency through pooling transactions. In spite of this, the Claimant's expert evidence establishes that his crypto assets can still be identified. There are, in short, compelling grounds for injuncting Smith to prevent him from disposing of the Claimant's stolen assets. I will make an order continuing the injunction of Obi J until trial or further order.

The Disclosure Order

Legal Framework

44. The Claimant seeks a Disclosure Order pursuant to the jurisdiction established by the Court of Appeal in *Bankers Trust Co v Shapira* [1980] 1 WLR 1274 ("*Bankers Trust"*), which empowers the court to make an order requiring a third party to provide information about a claimant's property or other assets. The same information can also be sought pursuant to a *Norwich Pharmacal* order. Where permission to serve out of the jurisdiction is required, the appropriate gateway is CPR Practice Direction 6B, paragraph 25, "Information orders against non-parties".

45. In *Kyriakou v Christie Manson & Woods* [2017] EWHC 487 (QB) Warby J held at [44] that:

> "The *Bankers Trust* jurisdiction arises where there is strong evidence that the claimant's property has been misappropriated. The case decided that where there is such evidence the court will not hesitate to make strong orders to ascertain the whereabouts of property and to prevent its disposal, and those orders may intrude into what would otherwise be confidential customer information."

46. In *Kyriakou,* Warby J identified five principles that emerge from the authorities which have considered *Bankers Trust* at [13]-[19]:

    (1) There must be good grounds for concluding that the money or assets about which information is sought belonged to the claimant.

    (2) There must be a real prospect that the information sought will lead to the location or preservation of such assets.

    (3) The order should, so far as possible, be directed at uncovering the particular assets which are to be traced and the order should not be wider than is necessary.

    (4) The interests of the claimant in obtaining the order must be balanced against the possible detriment to the respondent in complying with the order, and the detriment to the respondent includes, in a case where this arises, any infringement, or potential infringement, of rights of privacy or confidentiality.

    (5) The applicant must provide undertakings, first of all to pay the expenses of the respondent in complying with the order; secondly, to compensate the respondent in damages, should loss be suffered as a result of the order; and thirdly, only to use the documents or information obtained for the purpose of tracing the assets or their proceeds.

Assessment

47. I consider that the *Bankers Trust* criteria identified in *Kyriakou* are satisfied in this case. The Claimant's affidavit evidence establishes his ownership over the Bitcoin in relation to which he seeks information from Huobi. It seems likely Huobi will hold the

information which would enable the Claimant to identify Smith, who is now in control of the Claimant's stolen Bitcoin. The order is specific about the Bitcoin in respect of which the information is sought and does not go any wider than necessary. The Claimant has a strong interest in recovering his stolen Bitcoin that outweighs any detriment to Huobi in complying with the order, which I consider to be minimal. The Claimant has given appropriate undertakings to Huobi, although his ability to meet the financial undertakings is limited. There is authority that a freezing injunction should not be refused solely on the basis that a Claimant's lack of means makes an undertaking of limited value, where the other criteria are satisfied: *Allen & Ors v Jambo Holdings* [1980] 1 WLR 1252 (CA). Given that the Claimant's lack of means is because this fraud deprived him of his life savings, it is plainly appropriate to accept his financial undertakings even if they are of limited value.

48. The Claimant requires permission to serve the application out of the jurisdiction and the appropriate gateway is CPR PD 6B, paragraph 3.1(25) (Information orders against non-parties). Some of the earlier *Bankers Trust* authorities refer to the lack of any gateway for serving a *Norwich Pharmacal* claim out of the jurisdiction, but this provision, introduced from 1 October 2022, appears to provide the relevant gateway both for *Norwich Pharmacal* claims and *Bankers Trust* applications.

49. The criteria for permission to serve out of the jurisdiction on Huobi are met in this case. There is a good arguable case that the application falls within the CPR PD 6B, paragraph 3.1(25) gateway. There is a serious issue to be tried on the merits in relation to Huobi and the involvement of HTX. England is clearly the appropriate forum for the claim given that it appears that Smith is present here and the fraud was committed here. For these reasons I grant the Claimant permission to serve the application out of the jurisdiction. I also grant the Claimant permission to serve the application by alternative means pursuant to CPR 6.15. It appears that Huobi's location and address for service is opaque, so it is appropriate for the Claimant to serve the application to the email address which is currently their only means of communication.

50. I also make an order granting the Claimant permission to serve the claim form on Smith by email, pursuant to CPR 6.15, as this is the only means the Claimant has of contacting him.

Costs

51. The Claimant seeks his costs of the applications against both Defendants. The default position in relation to the costs of a freezing injunction follows the general rule on costs under CPR 44.2(2)(a), namely that the unsuccessful party pays the costs of the successful party: *Dos Santos v Unitel SA* [2024] EWCA Civ 1109; [2025] KB 438. I am satisfied that both Defendants should be potentially liable for the costs. Smith perpetrated a fraud on the Claimant and it is clear he should be liable for the costs to date. Huobi might well have avoided any order on costs had it responded cooperatively to the Claimant's requests for information, but its complete lack of engagement with the Claimant's requests for information about Smith and its failure to assist with the return of the Claimant's stolen cryptocurrency have been wholly unreasonable and accordingly I find that Houbi should also be liable. Assessing the costs summarily and on the indemnity basis I award the Claimant all of his costs of £60,993.91 inclusive of VAT.