



Enterprise

CHAMBERS

WHAT IMMEDIATE RELIEF CAN BE SOUGHT FROM ENGLISH CIVIL COURTS IF A CRYPTOCURRENCY ACCOUNT IS HACKED BY 'PERSONS UNKNOWN' AND PERHAPS TAKEN ABROAD? AN INTERESTING CASE ON SERVICE OUT.

MADELEINE HEAL

1. If a cryptocurrency account is breached by fraudulent hackers, the first problem is that 'thine enemy is unknown'. It is possible to buy and sell cryptocurrencies using trading accounts with counterparties who are blind to the person operating the account. In *Fetch.ai Ltd v Persons Unknown*¹, hackers obtained access to Fetch.ai's crypto assets account with Binance Holdings Limited (registered in the Cayman Islands) ('Holdings') and Binance Markets Limited, (a UK company) and were able to trade those assets at massive undervalues, moving them out of Fetch.ai's account into accounts operated by the alleged fraudsters.
2. The trades at an undervalue resulted in losses to Fetch.ai of US\$2.6 million, sustained over a very short period.

¹ [2021] EWHC 2254 (Comm) HHJ Pelling QC sitting as a Judge of the High Court

3. A proprietary injunction was needed to freeze either the assets removed from Fetch.ai's account (if still identifiable in the fraudsters' account) or to restrain them from dealing with the proceeds. The personal and proprietary causes of action also made available a worldwide freezing order against those Persons Unknown and others including Binance to freeze their assets worldwide, so that any final judgment in favour of Fetch.ai could have real effect.
4. At the raw moment of discovery of crypto fraud, *how* the fraud was practiced by the hackers is not the focus. The first focus must be getting into court quickly to preserve the assets or their proceeds. Claims available against the hackers will include breach of confidence, unjust enrichment and an equitable proprietary claim based upon constructive trust. The 'private key' by which someone trades crypto assets is Confidential Information and the court will, within hours of an application being made, grant an injunction to preserve assets in the unknown fraudsters' hands in meritorious cases.
5. Care must be taken when framing the draft order against Unknown Persons. In *Fetch.ai*, Binance could be identified, but those who actually perpetrated the fraud and those who, perhaps innocently, may have received the assets, could not be named. At the stage of deciding whether or not to grant urgent interim relief, the description of each class of Unknown Persons and the relief sought against each class will be an important consideration for the court.

What if the stolen crypto assets have been taken abroad?

6. Transfer of crypto assets happens electronically in seconds. A claim against Unknown Persons can be brought against them in English courts in certain circumstances even if they are abroad, applying international jurisdictional rules.
7. Claims against the hackers in *Fetch.ai* for breach of confidence fell within the rules in the Rome II Convention and for the purposes of Article 4.1 of Rome II, the question will depend on where the cryptocurrency stolen is

located at the time of the fraud. In *Ion Science v Persons Unknown*², the answer was held to be the place where the person or company who owns the crypto asset is domiciled. In *Fetch.ai*, there was no real doubt that England was the place where Fetch.ai operated and held its crypto assets.

8. On the other claims available against the hackers in *Fetch.ai*, the English court decided it had jurisdiction over the equitable proprietary claim under Rome II Articles, 3, 10 or possibly 11³, and over the unjust enrichment claim because it comes within the scope of Article 10 of Rome II.

Permission to serve out of the jurisdiction on Persons Unknown

9. If there is evidence that the crypto assets or their proceeds may have been transferred abroad, permission from the English court will be required to serve the proceedings on those known and unknown defendants who are outside the jurisdiction of the English courts. This requires consideration of three questions: (1) does each claim raise a serious question to be tried on the merits; (2) is there a good arguable case that the claim falls within one of the gateways in CPR 6BPD; and (3) is England the proper place to bring the claim? In *Fetch.ai* for the reasons above, the cryptocurrencies were treated as a matter of English law as located in England and it was reasonably arguable that the losses were suffered in England.
10. The relevant CPR 6BPD gateways for breach of confidence are gateways 11 and 21. Crypto assets are moveable property and in *Fetch.ai* it was reasonably arguable that before the fraud, they were within the jurisdiction. The unjust enrichment claim fell under gateway 16, being obtained by the fraudsters within England.
11. On the proprietary claim, gateway 15 applies where a claim is made against a defendant as constructive trustee, or as trustee of a resulting

² Unreported, 21 December 2020, Butcher J

³ because the fraudulent recipient of the assets holds the legal title on constructive trust for the loser

trust, where the claim arises out of acts committed or events occurring within the jurisdiction or relates to assets within the jurisdiction. It was at least realistically arguable that the crypto assets in *Fetch.ai* were located in England. In addition, gateway 4A will apply where a claim is made in reliance on gateways 2, 6-16, 19 or 21 and a further claim is made against the same defendant which arises out of the same or a closely connected fact. That took care in *Fetch.ai* of permission to serve out on the claims against those Persons Unknown who may be actually responsible for fraud.

12. But the court in *Fetch.ai* also asked itself whether Binance should be ordered to give disclosure⁴ of information on which of its entities conduct what business, so that Fetch.ai could advance its claims. The judge described material generated by the Binance Group concerning this question as “remarkably opaque” and decided that an order against Holdings in Cayman would give Fetch.ai the best chance of obtaining the information needed⁵.
13. The court concluded in *Fetch.ai* at [30] that there were serious issues to be considered at trial regarding whether the distinction between granting a *Norwich Pharmacal* order and/or a *Banker’s Trust* order can be maintained and whether or not any of the jurisdictional gateways can, on a proper analysis, apply to disclosure orders. In the meantime, the judge was prepared to grant Fetch.ai permission to serve a *Bankers Trust* disclosure order against Holdings out of the jurisdiction by reference to one of the gateways Butcher J had identified in *Ion Sciences* at [21]. A *Norwich Pharmacal* order would not be made against Holdings, however, applying Teare J’s decision in *AB Bank Limited, Off-shore Banking Unit v Abu Dhabi Commercial* ⁶.
14. It is doubtful that *Norwich Pharmacal* relief is a cause of action as it is an order for discovery and disclosure against a person. It may be relief ordered before any substantive proceedings and there may never be

⁴ under either *Bankers Trust* or *Norwich Pharmacal*

⁵ the fact that BINANCE trade mark registrations named Holdings as proprietor was held by Butcher J to be indicative that it was the Group’s controlling entity

⁶ [2017] 1 WLR 810

substantive proceedings. *Bankers Trust* orders are ancillary to an action to recover trust assets. In *Fetch.ai*, the assets were obtained by hacking and fraud and there was a proprietary claim⁷.

15. In reaching that conclusion in *Fetch.ai*, the judge found that the five criteria required for a *Bankers Trust* order⁸ had been made out against Holdings: (1) that there were good grounds for concluding that the crypto assets or their proceeds belonged to Fetch.ai; (2) that there was a real prospect that the information sought would lead to the location or preservation of those assets, because Holdings held “Personal Data” in relation to its customers; (3) an order could be crafted to focus on those directly involved in perpetrating the fraud and to direct the search to uncovering the particular assets to be traced and not any wider; (4) any detriment occasioned to Holdings by complying with the *Bankers Trust* disclosure order was outweighed firstly, by the “very strong evidence” of a significant fraud by which Fetch.ai was deprived of its crypto assets and secondly, by the contractual terms on which Binance operates. Those terms contemplate that personal data may be disclosed to others, including “your transaction counterparty” and “regulatory agents or law enforcement agencies to comply with the laws or regulations formulated by government authorities”. This suggests that all who trade on Binance’s contractual terms are aware that there is at least a risk of personal data being revealed, particularly on an order made by a court of competent jurisdiction; and (5) Fetch.ai would be required to give an undertaking to meet Holdings’ expenses of complying with the disclosure order. With Fetch.ai’s assets exceeding £150 million, there was no reason to believe that it would be unable to meet those expenses.
16. As the third respondent, Binance UK, is within the jurisdiction, the judge in *Fetch.ai* granted *Norwich Pharmacal* relief against it as he was satisfied that (1) a wrong had been carried out by an ultimate wrongdoer; (2) there was a need for the order to enable the action to be brought against the ultimate wrongdoer, without which it would be impossible to identify who was involved with the wrongdoing and what had become of the assets;

⁷ *Westdeutsche Girozentrale v London Borough of Islington* [1996] AC 668

⁸ summarised by Warby J in *Kryiakou v Christie’s* [2017] EWHC 487 (QB) at [4] to [15]

(3) Holdings and Binance UK were administering the accounts into which fraudsters were able to gain access, so to that extent they were mixed up in the wrongdoing and were likely to be able to provide KYC information necessary to enable the ultimate wrongdoer to be sued; and (4) *Norwich Pharmacal* relief was necessary and proportionate in all the circumstances.

17. The judge in *Fetch.ai* also granted against Holdings located in Cayman (a Hague Service Convention state) an order for alternative service. He was satisfied that there were special or exceptional circumstances for departing from the machinery for service which the Convention adopts for its signatory countries⁹ as the only means by which the English court's order could be drawn speedily to Holdings' attention.
18. The judge in *Fetch.ai* noted that applications for both *Bankers Trust* and *Norwich Pharmacal* relief are conventionally sought in CPR Part 8 proceedings brought before commencement of substantive proceedings against the individuals concerned, but in the circumstances before him, the sums involved and Binance's mixed messages gave rise to a real possibility that unless disclosure orders were also made against the classes of Persons Unknown, Binance might be tempted to unfreeze the account. At one stage Binance had already threatened to do this and carrying out that threat might defeat Fetch.ai's litigation.

Madeleine Heal

Enterprise Chambers

Tele: 020 7405 9471

Disclaimer: These notes are produced for educational purposes only. The views expressed in them are those of the author. The contents do not constitute legal advice and should not be relied on as such advice. The author and Enterprise Chambers do not accept legal responsibility for the accuracy of their contents. The contents of these notes must not be reproduced without the consent of the author.

⁹ *Russian Commercial Bank (Cyprus) Limited v Khoroshilov* [2020] EWHC 1164 (Comm) at [97] Cockerill J