High Court confirms cryptocurrency is property, grants proprietary injunction and protective orders (AA v Persons Unknown)

28/01/2020

Dispute Resolution analysis: In granting an interim proprietary injunction further to a cyberattack and payment of ransom in Bitcoin, the High Court embraced the UK Jurisdictional Task Force (UKJT) Legal Statement on Cryptoassets and Smart Contracts and, importantly, confirmed that cryptoassets are property. The interim injunction was also supported by ancillary orders intended to better police and protect it, including orders: (i) for a private hearing; (ii) preservation of the applicant's anonymity (given the risk of further cyberattacks); (iii) to identify those responsible and now holding the Bitcoin; and (iv) for alternative service given the urgency and to seek to preserve the Bitcoin. The case exemplifies the court's responsiveness in granting urgent relief and ancillary orders in respect of sophisticated cyber incidents in an increasingly complex FinTech landscape. Written by Danielle Carr, partner, at Rosenblatt Limited.

AA v Persons Unknown & Ors, Re Bitcoin [2019] EWHC 3556 (Comm) (13 December 2019)

What are the practical implications of this case?

In this case, the High Court granted an interim proprietary injunction on the application of an English insurer (AA) which had (further to computer hacking, blackmail and extortion perpetrated on its insured) paid a ransom in Bitcoin to persons unknown.

Importantly, this case provides judicial confirmation that cryptoassets are a form of property capable of being the subject of a proprietary order. Consistent with two previous English court decisions, and adopting the 'compelling' analysis in the UKJT Legal Statement on Cryptoassets and Smart Contracts, which was considered 'an accurate statement as to the position under English law', Bryan J regarded cryptoassets, such as Bitcoin, as property. They were also considered to meet the criteria of being definable, identifiable by third parties, capable in their nature of assumption by third parties and having some degree of permanence. On this basis, Bryan J granted the interim proprietary injunction against the four defendants in respect of the Bitcoin.

Of further interest was the court's readiness to support the proprietary injunction with orders that may better ensure its efficacy. In particular:

- departing from the open justice principle, the hearing was held in private
- the anonymity of AA and its insured were preserved (given the risk of further cyber or copycat attacks)
- orders were made seeking to identify those responsible and now holding the Bitcoin, and
- alternative service was granted, given the urgency and being mindful that 'the very nature of Bitcoin [is] they can be moved at the click of the mouse' (at para [77])

What was the background?

This case arose from the hacking of a Canadian insurance company (insured customer), itself insured including as against cybercrime attacks by the applicant, AA. The insured customer received notes left on the encrypted system by the first defendant (persons unknown who demanded Bitcoin (unknown first defendant)). Given the importance of access to the insured customer's systems, AA agreed to pay a ransom sum of US$950000, payable in Bitcoin, for provision of a decryption tool. On transfer of the 109.25 Bitcoin, the decryption tool was received and executed over the relevant systems. AA is unable to identify the second defendant, persons unknown who own/control specified Bitcoin (unknown second defendant).

Following payment, a specialist provider of software to track payment of cryptocurrency determined that some of the Bitcoin was then transferred into fiat currency, with the balance of 96 Bitcoin transferred to a specified address linked to the exchange Bitfinex operated by the third and fourth defendants, iFinex and BFXWW Inc, each BVI companies trading as Bitfinex (Bitfinex parties). On an application made without notice to unknown first defendant and unknown second defendant and

proceeding ex parte (albeit on limited notice to the Bitfinex parties), AA sought a proprietary injunction and associated orders.

What did the court decide?

At the outset the court confirmed that the application was properly made ex parte and it was appropriate to anonymise AA due to the risk of retaliatory cyberattacks upon it and the insured customer. Further, it was appropriate for the hearing to be conducted in private, as publicity would defeat the object of the hearing, since it may tip off the persons unknown (who may dissipate the Bitcoin), reveal confidential information, and given the risk of further cyber or copycat attacks. Equally, it would be unjust to refer to the defendants (in particular the Bitfinex parties, who have not had an opportunity to be heard and are mixed up in wrongdoing perpetrated by unknown first defendant and unknown second defendant) in a public hearing. As such, it was necessary to sit in private to secure the proper administration of justice.

As regards the interim proprietary order, Bryan J was satisfied, to the level required to grant the interim relief, that cryptocurrencies are a form of property capable of being the subject of a proprietary injunction (see above). Further, it was determined that there was a serious issue to be tried. Indeed, the claims against unknown first defendant and unknown second defendant were considered to be very strong, to the extent they appear to have committed the extortion and blackmail and obtained, by ransom, the sums concerned. Although the position was less clear in relation to the Bitfinex parties (who may simply have been mixed up in the wrongdoing), they were understood to hold the Bitcoin belonging to AA, which arguably came into their possession in furtherance of fraud and where they have no entitlement to it. The balance of convenience was in favour of granting the relief sought, with damages being an inadequate remedy given that the 96 Bitcoin could be dissipated.

In order to police the injunction, Bryan J ordered the four defendants to provide information on the identity and address of unknown first defendant and unknown second defendant (which those two defendants clearly knew themselves and which would no doubt be in Bitfinex's records and KYC). Finally, the court made orders to allow amendment of the claim form, permit service out of the jurisdiction, and alternative service on unknown first defendant and unknown second defendant (by email or delivery to any physical address relating to the Bitcoin account and service by filing in court) and on the Bitfinex parties (by email, given the urgency and to seek to preserve the 96 Bitcoin).

Case details

- Court: High Court, Commercial Court, (QBD)
- Judge: Mr Justice Bryan
- Date of judgment: 13 December 2020

Danielle Carr is a partner at Rosenblatt Limited, and a member of LexisPSL's Case Analysis Expert Panels. If you have any questions about membership of these panels, please contact caseanalysis@lexisnexis.co.uk.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.