LMN v Bitflyer Holdings Inc and Others – another string in the bows of crypto fraud claimants.

Alex Wiltshire (Associate)

10TH JANUARY 2023

HUMPHRIES KERSTETTER

www.humphrieskerstetter.com

LMN v Bitflyer Holdings Inc saw the High Court award Bankers Trust disclosure orders under the new service gateway 25 for the first time. This gateway was specifically introduced to assist claimants in crypto fraud cases seek crucial information about unknown defendants from third parties outside England and Wales. These orders are particularly valuable to claimants in these cases where the defendants' identities, and the claimant's misappropriated funds, can be exceptionally difficult to identify given the degree of anonymity crypto users possess.

Since Bitcoin's launch in 2009, the rapid growth of blockchain based asset markets such as cryptocurrencies and NFTs has outpaced the development of the law designed to govern their operation. The novel issues specific to the "decentralised" nature of crypto-assets that flow over international borders between owners hiding behind pseudonyms that have evolved since are by now well known. However, they are still largely untested, creating legal uncertainty for users, organisations and governments.

It is fitting then that in a year in which cryptocurrency markets suffered significant depreciation, and the collapse of FTX caused headlines as perhaps the biggest crypto-market scandal to date, the law has taken significant steps to catch up. In July 2022, the UK Law Commission released a consultation paper with a particular focus on provisional proposals for reform of private law, and particularly private property law, in relation to digital assets. This focus is to continue with the launch of the project, *"Digital assets: which law, which court?"* concluding in the second half of 2023.

However, achieving certainty for users and organisations via legislative reform will take time. In the interim, the courts are required to approach novel issues using established tools, often in a piecemeal fashion, to complement the legislation that is slowly developing. Mr Justice Butcher's decision in *LMN v Bitflyer Holdings Inc and others [2022] EWHC 2954 (Comm)* is one such example.

The claimant, *LMN*, operates a cryptocurrency exchange, incorporated in England and Wales. In a manner analogous to conventional banking, it holds cryptocurrency in its own name and owes a personal obligation to pay the relevant amount to each customer. In 2020, hackers stole millions of dollars-worth of cryptocurrency which was traced back as far as several recipient "exchange addresses" operated by the six defendants, but no further. The claimant sought information from the exchanges that might identify the defendants and locate the proceeds of its property. The claimant's evidence suggested that many exchanges contracted the services of companies in different jurisdictions and thus the relevant entity might depend on where the natural person associated with a target address was located.

The claimant sought relief in respect of multiple issues presented by crypto-assets, namely:

- whether it was appropriate to make a Bankers Trust order to require the provision of information that might identify the identities of the alleged thieves hiding behind online pseudonymity and trading exchanges;
- whether it was appropriate to permit the claimant to serve the defendants and unspecified related entities, outside the jurisdiction; and
- whether the UK was the proper forum for a dispute in respect of an asset with an indeterminate physical location.

The Bankers Trust jurisdiction was first established by the Court of Appeal in *Bankers Trust Company v Shapira [1980] 1 WLR 1274*, well before the internet, let alone the emergence of crypto-markets. These orders are generally confined to cases in which there is strong evidence that the claimant's property has been misappropriated. Traditionally, these orders

sought disclosure by a third-party bank however, as this case shows, they can also be sought in respect of other similar institutions that hold this type of information.

Conversely, the order permitting service upon the defendants and their related entities out of the jurisdiction was sought under the recently enacted information gateway in *Practice Direction 6B.3.1(25)*, which came into effect on 1 October 2022, only weeks prior to the application being heard. In fraud proceedings, identifying who the defendants are, how the fraud had been committed, and the location of misappropriated assets is often challenging. These challenges can be even greater in cases involving cryptocurrency fraud and this amendment seeks to assist victims in these disputes where disclosure from third-parties can assist in establishing these critical elements.

The principal hearing for permission to serve out of the jurisdiction required the claimant to establish that:

- the claim for a Bankers Trust order was meritorious;
- there was a good arguable case that one of the gateways for service outside the jurisdiction applied; and
- England and Wales was the appropriate forum for the claim to be tried.

Mr Justice Butcher found the following elements under the Bankers Trust jurisdiction were at least arguable:

- ***The assets about which information is sought belonged to the claimant;*** assuming UK law applied, Butcher, J considered that the cryptocurrency was either a form of property held on constructive trust for the claimant or, alternatively, if a new asset was created in the hands of the acquirer, that transfer could be the subject of tracing.
- ***There was a real prospect that the information sought will lead to the preservation of such assets;*** the information was sought to identify the relevant account holders and the destination of the transfers.
- ***The order directed was no wider than necessary to uncover the assets to be traced;*** Butcher, J limited the scope of the orders to information that might identify the alleged fraudsters such as names, "Know Your Customer" information, documents held in relation to accounts which identify email addresses, residential addresses, phone numbers and bank account details, and, to the best of the defendant's ability, explanations as to what had become of the cryptocurrency.
- ***The interests of the claimant were not outweighed by any detriment to the respondent in complying with the order, including with respect to any potential infringement of privacy rights or confidentiality;*** Butcher, J found that there was clear benefit to the claimant in obtaining the information sought and that the potential detriment to the defendants could be eliminated, or at least very effectively mitigated, by the claimant's undertakings.
- ***The claimant undertakes to pay all of the expenses of the respondents in complying with the orders, compensate the respondent in damages should loss be suffered as a result and to only use the documents or information obtained for the purpose of tracing the assets;*** these undertakings were offered to all defendants.

Mr Justice Butcher then considered whether the new gateway for service outside the jurisdiction in *Practice Direction 6B.3.1(25)* was available. The test is a simple one, namely:

a) the application for disclosure must be made to obtain information regarding (i) the true identity of a defendant or a potential defendant; and/or (ii) what has become of the property of a claimant or applicant; and

b) the application must be made for the purpose of proceedings already commenced or which, subject to the new information received, are intended to be commenced either by service in the UK or CPR rule 6.32, 6.33 or 6.36.

The information sought plainly fell within (a)(i) and (a)(ii). Mr Justice Butcher was also satisfied (b) was met given that, should the information obtained reveal potential causes of action against defendants in the jurisdiction, the claimant intended to commence proceedings against them here. Equally, if the information indicated that they were outside the jurisdiction, the claimant intended to commence proceedings in the UK and seek to serve such proceedings out of the jurisdiction.

In respect of the third issue, Butcher, J considered that the law of England and Wales appeared to be the appropriate forum in which to bring the claim given the claimant was an English company carrying on its relevant business in the UK. Accordingly, the cryptocurrency could be regarded as having been taken from the claimant's control in England.

Bankers Trust orders are a critical tool in cryptocurrency fraud cases, sharpened by the new gateway which mitigates potential issues arising in circumstances in which the respondent, and the information subject to the disclosure order, are outside the UK. Mr Justice Butcher's decision demonstrates this and can be viewed as another incremental step towards legal certainty in a rapidly evolving industry. These steps will be welcomed by individuals and organisations wishing to advance claims of cryptocurrency fraud and should incentivise prospective claimants to bring such claims in the UK.

Alex Wiltshire

Associate

Admitted as a Barrister and Solicitor of the High Court of New Zealand

aw@humphrieskerstetter.com
+44 203 960 3992

Humphries Kerstetter LLP
St. Bartholomew House
92 Fleet Street
London EC4Y 1DH

Tel: +44 207 632 6900
www.humphrieskerstetter.com