Neutral Citation Number: [2022] EWHC 2954 (Comm)

Case No: CL-2022-000517

IN THE HIGH COURT OF JUSTICE
BUSINESS & PROPERTY COURTS OF ENGLAND AND WALES
COMMERCIAL COURT (KBD)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 29/11/2022

Before :

THE HON MR JUSTICE BUTCHER

- -

Between :

LMN **Claimant**

- and –

(1) BITFLYER HOLDINGS INC.
(a company registered in Japan)
(2) BINANCE HOLDINGS LIMITED
(a company registered in the Cayman Islands)
(3) PAYWARD INC
(a company incorporated in the USA)
(4) LUNO PTE LTD
(a company registered in Singapore)
(5) COINBASE INC
(a company incorporated in the USA)
(6) HUOBI GLOBAL LIMITED
(a company incorporated in the Republic of Seychelles)
(7) LUNO (Pty) LTD
(a company incorporated in South Africa)
(8) PERSONS UNKNOWN (BINANCE)
(being the individuals or companies or other entities who are identified in the Binance.com platform's terms and conditions as Binance Operators but not the Second Defendant)
(9) PERSONS UNKNOWN (BITFLYER)

(being the companies or other entities who own and/or operate the 'Bitflyer' cryptocurrency exchange and who have been informed about these proceedings and/or this order but not the First Defendant)
(10) PERSONS UNKNOWN (KRAKEN)
(being the companies or other entities who own and/or operate the 'Kraken' cryptocurrency exchange and who have been informed about these proceedings and/or this order but not the Third Defendant)
(11) PERSONS UNKNOWN (LUNO)
(being the companies or other entities who own and/or operate the 'Luno' cryptocurrency exchange and who have been informed about these proceedings and/or this order but not the Fourth or Seventh Defendants)
(12) PERSONS UNKNOWN (HUOBI)
(being the companies or other entities who own and/or operate the 'Huobi' cryptocurrency exchange and who have been informed about these proceedings and/or this order but do not include the Sixth Defendant) **Defendants**

- -
- -

Josephine Davies and Sam Goodman (instructed by **Rahman Ravelli**) for the **Claimant**
Nik Yeo (instructed by **DLA Piper UK LLP**) for the **5th Defendant** at the hearing on 11 November 2022

Hearing dates: 28 October, 11 November 2022

- -

Approved Judgment

.....

Mr Justice Butcher :

1. The present claim is made for information orders by LMN, which is a cryptocurrency exchange ('C') against six other cryptocurrency exchanges. I will refer to each of the Defendants as D1, D2 etc, respectively.

2. This judgment relates to two hearings. The first, on 28 October 2022, was an *ex parte* application made by C, without notice to any of the Defendants. I made certain orders, which are described below, and required that notice of the application for the substantive relief claimed should be given to the Defendants. A further hearing, on notice, occurred on 11 November 2022. At that hearing, D5 was represented by Mr Yeo and I am grateful to him for his helpful submissions. A representative of D1 was present at that hearing. The position of most of the other Defendants had also been made known to the court by that stage. I made further orders on that occasion. Again, I will refer to them below.

3. On each occasion, I indicated that I would provide my reasons for the orders made subsequently. These are those reasons.

Factual Background

4. The essential factual background to this case, as alleged by C, is as follows. C is a company incorporated in England and Wales. It operates a cryptocurrency exchange. Its analysis is that in doing so it does not hold the cryptocurrencies on trust. Rather, it holds cryptocurrency in its own name and, in a manner analogous to conventional banking, owes a personal obligation to pay the relevant amount to each customer.

5. A percentage of C's cryptocurrency reserves is accessible via the internet through what are called 'Hot Wallets', which is a term explained in the Securities and Exchange Commission's Glossary to the Cryptoeconomy as 'wallet[s] … connected to the internet, enabling [them] to broadcast transactions'.

6. C's evidence is that some two years ago, hackers obtained access to its systems, and transferred some millions of dollars-worth of cryptocurrency (consisting of Bitcoin, Ripple, Tether, Ethereum, ZCash and Ethereum Classic) from it. C sought help from a number of UK regulatory and law enforcement agencies, including the FCA, the National Crime Agency and the Metropolitan Police. It worked closely with officers of the Metropolitan Police's Cyber Crime Unit. After about 3 months, however, the Cyber Crime Unit said that it could provide no further assistance and suggested that C should consider civil proceedings.

7. After a further four months, C instructed solicitors to pursue a civil action. C instructed an expert, Pamela Clegg of CipherTrace, to seek to trace the cryptocurrency which had been transferred by the hackers. Ms Clegg produced a report dated 14 September 2022, and then a supplementary report dated 7 November 2022. Ms Clegg's reports indicate that she was provided by C with details of the transactions believed to have been carried out by the hackers on the day of the hack. She then tracked the transactions on the relevant blockchains. Using proprietary software and public records, Ms Clegg was able to identify addresses under the same control; and through further software-based analysis of transactions was able to identify 'address clusters' that could be inferred to be under common control.

8. On any occasion where the chain of transactions reached an 'exchange address' Ms Clegg could not discover what became of the cryptocurrency thereafter. This is because 'exchange addresses' are addresses owned and operated by the exchange itself. Whilst such addresses tend to be associated with a particular customer, the actual crediting of cryptocurrency to the relevant customer's account takes place 'off-chain' (ie via an internal accounting exercise). Cryptocurrency received into an 'exchange address' will be often merged by the exchange into an 'omnibus wallet' which is used to service multiple customers' requests.

9. The result of Ms Clegg's exercise was the identification of 26 recipient addresses, which were 'exchange addresses', to which Bitcoin ('BTC') or Bitcoin Cash ('BCH') had been transferred. The distribution of these addresses amongst exchanges operated either by the relevant Defendant or a company in the same group (a point to which I will return) was as follows for BTC: D1, 1 account; D2, 5 accounts; D3, 1 account; D4, 2 accounts; D5, 1 account; and D6, 5 accounts. For BCH the distribution was: D2, 7 accounts; D6, 4 accounts.

10. C's evidence is that, as all these addresses are 'exchange addresses' it is impossible to trace the cryptocurrency any further without information from the exchanges about the individuals behind the transactions. In the case of exchanges either operated by one of the Defendants or by an associated company, C had reason to believe that each collected know your client ('KYC') and anti-money laundering ('AML') information, and thus might be able to provide relevant information.

11. As already indicated, C's evidence prepared for the initial hearing, while identifying the exchanges concerned, was not able to identify the exact legal entities which might be responsible for operating them and hold the information and documents which C sought. That evidence suggests that many exchanges use different companies to contract in different jurisdictions and thus the relevant entity might depend on where the natural person associated with a target address was located. Accordingly, in the initial Claim Form what was called the 'topco' for each exchange was identified. These 'topcos' had been identified by C from a number of sources, including websites, Bloomberg, WSJ, and regulatory and legal filings.

The 28 October 2022 Hearing

12. At the 28 October 2022 hearing, C sought a 'rolled up' hearing of applications for permission to serve the Defendants out of the jurisdiction and to serve by alternative means, and of the substantive application for information orders. I agreed that this hearing should be held in private, in order that publicity should not defeat the object of the proceedings by giving notice to the putative fraudsters of the attempts to identify them. I also agreed to consider the application for permission to serve out and to serve by alternative means. I declined, however, to proceed with the application for the substantive relief without notice being given to the Defendants. To do so appeared to me inappropriate in the present case given: (a) that the alleged fraud was not of very recent occurrence; (b) that the application was not made against the putative fraudsters; and (c) none of the Defendants (nor any associated company) was alleged to have been itself in any way fraudulent.

The application to serve out of the jurisdiction

13. The principal application which was, therefore, considered at the 28 October 2022 hearing was that for permission to serve out. The Claim Form in relation to which this permission was sought at that stage named six Defendants, to wit Ds 1-4 and 6, and Coinbase Global Inc as D5. The Claim Form stated in part:

> '[C] seeks disclosure of documents and information, and ancillary relief, against [Ds] in the form of the draft order appended to this Claim Form, pursuant to s. 37 of the Senior Courts Act 1981, the *Bankers Trust* jurisdiction, to assist in identifying Persons Unknown and locating the proceeds of [C's] property.
>
> … Part 8 of the Civil Procedure Rules applies to this claim.'

14. The draft order there referred to sought from each D the following information:

> 1.1. In respect of any customer account(s) which the [relevant] Target Cryptocurrency were allocated to and/or received on behalf of:
>
> 1.1.1. The name the account(s) is held in;
>
> 1.1.2. All 'Know Your Customer' information and documents provided in respect of the account(s);
>
> 1.1.3. Any other information and documents held in relation to the account(s) which might or does identify the holder of the account(s), including but not limited to bank account and payment card details, email addresses, residential addresses, phone numbers, bank statements, correspondence and documents provided on account opening or verification.
>
> 1.2. To the best of the [the relevant D's] ability:
>
> 1.2.1. An explanation as to what has become of the [relevant] Target Cryptocurrency.
>
> 1.2.2. Insofar as the [relevant] Target Cryptocurrency has been transferred to any other accounts (Onwards Account(s)), the details of the Onward Accounts set out in paragraph 1.1 above.'

The requirements for an order permitting service out

15. The first question which accordingly needed to be decided was whether permission should be granted to serve out of the jurisdiction a Claim Form seeking such relief. This required a consideration of three matters, as summarised in Altimo Holdings and Investment Ltd v Kyrgyz Mobil Tel Ltd [2011] UKPC 7 at [71] per Lord Collins, namely:

> (1) Was there a serious issue to be tried on the merits?
>
> (2) Was there a good arguable case that the claim fell within one of the 'gateways' in CPR PD 6B §3.1?
>
> (3) Was England and Wales the appropriate forum for the claim to be tried?

The merits of the claim

16. As to the merits of the claim, C argued that there was at least a serious issue to be tried, and that indeed there was a good arguable case as to its entitlement to the orders sought. I am satisfied that C does have a good arguable case in this regard on the basis set out in the following paragraphs.

17. The court has a wide jurisdiction to grant injunctions under s. 37 Senior Courts Act 1981. Orders requiring the provision of information have been considered justifiable by two strands of authority. One is that stemming from Norwich Pharmacal Co v Comrs of Customs and Excise [1974] AC 133. The principles applicable to a Norwich Pharmacal order were conveniently summarised in Mitsui & Co v Nexen Petroleum UK Ltd [2005] EWHC 625 (Ch), where Lightman J said (at [18]-[21]):

> 18. … In its original form, the Norwich Pharmacal jurisdiction allowed a claimant to seek disclosure from an "involved" third party who had information enabling the claimant to identify a wrongdoer so as to be in a position to bring an action against the wrongdoer where otherwise he would not be able to do so. Lord Reid described the principle at page 175 as follows:
>
> "...if through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrong-doing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers. I do not think that it matters whether he became so mixed up by voluntary action on his part or because it was his duty to do what he did. It may be that if this causes him expense the person seeking the information ought to reimburse him. But justice requires that he should co-operate in righting the wrong if he unwittingly facilitated its perpetration."
>
> The required disclosure may take any appropriate form. Usually it takes the form of production of documents, but it may also include providing affidavits, answering interrogatories or attending court to give oral evidence.
>
> 19. In subsequent cases, the courts have extended the application of the basic principle. The jurisdiction is not confined to circumstances where there has been tortious wrongdoing and is now available where there has been contractual wrongdoing: P v T Limited [1997] 1 WLR 1309; Carlton Film Distributors Ltd v VCI Plc [2003] FSR 47 ("Carlton Films"); and is not limited to cases where the identity of the wrongdoer is unknown. Relief can be ordered where the identity of the claimant is known, but where the claimant requires disclosure of crucial information in order to be able to bring its claim or where the claimant requires a missing piece of the jigsaw: see Axa Equity & Law Life Assurance Society Plc v National Westminster Bank (CA) [1998] CLC, 1177 ("Axa Equity"); Aoot Kalmneft v Denton Wilde Sapte [2002] 1 Lloyds Rep 417 ("Aoot"); see also Carlton Films. Further the third party from whom information is sought need not be an innocent third party: he may be a wrongdoer himself: see CHC Software Care v. Hopkins and Wood [1993] FSR 241 and Hollander, Documentary Evidence 8th ed p.78 footnote 11.
>
> 20. Norwich Pharmacal relief is a flexible remedy capable of adaptation to new circumstances. Lord Woolf CJ noted in Ashworth Hospital Authority v MGN Ltd [2002] 1 WLR 2033 at 2049F:

"New situations are inevitably going to arise where it will be appropriate for the [Norwich Pharmacal] jurisdiction to be exercised where it has not been exercised previously. The limits which applied to its use in its infancy should not be allowed to stultify its use now that it has become a valuable and mature remedy."

The development of the jurisdiction is illustrated by the disclosure relief ordered by McGonigal J in Aoot where he said:

"[17] In Norwich Pharmacal the information required was the identity of the wrongdoer (the applicant knew what wrong had been done but not who had done it) but I see no reason why the principle is limited to disclosure of the identity of an unknown wrongdoer and does not extend to information showing that he has committed the wrong.
"…The information held by [the respondent] may not conclusively reveal an alternate defendant to [one of the alleged wrongdoers] nor conclusively disclose who received any part of the prepayment moneys, but I am satisfied that there is a sufficient prospect that the information they hold will assist [the applicant] in its search for wrongdoers and the funds paid away …to justify making the orders sought.
….
[20] The potential advantages to [the applicant] of seeing this part of the jigsaw and the potential disadvantages of it being denied a sight of that part outweigh, in my view, any detriment to [the respondent]."

21. The three conditions to be satisfied for the court to exercise the power to order Norwich Pharmacal relief are:

i) a wrong must have been carried out, or arguably carried out, by an ultimate wrongdoer;

ii) there must be the need for an order to enable action to be brought against the ultimate wrongdoer; and

iii) the person against whom the order is sought must: (a) be mixed up in so as to have facilitated the wrongdoing; and (b) be able or likely to be able to provide the information necessary to enable the ultimate wrongdoer to be sued.

18. The second line of authority is that stemming from Bankers Trust Co v Shapira [1980] 1 WLR 1274 ('Bankers Trust'). This may itself be said to be founded on the principle in Norwich Pharmacal (as is suggested in Mackinnon v Donaldson, Lufkin & Jenrette Corp [1986] Ch 482 ('Mackinnon') at 498A/B per Hoffmann J), or to overlap with it (as suggested in Murphy v Murphy [1999] 1 WLR 282 at 290A/B per Neuberger J). The central requirements for an order under this jurisdiction were summarised by Warby J in Kyriakou v Christie Manson & Wood Limited [2017] EWHC 487 (QB), as follows:

'12. 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.

13. The jurisdiction has been considered on a number of occasions since; the main authorities being *Arab Monetary Fund v Hashim (No.5)* [1992] 2 All E.R. 911, *Murphy v Murphy* [1999] 1 WLR 282, both of those being High Court decisions, and *Marc Rich v Krasner* [1999] EWCA Civ 581, a decision of the Court of Appeal.

14. Five principles have been identified (and I accept can be identified) as emerging from those authorities. First, there must be good grounds for concluding that the money or assets about which information is sought belonged to the claimant; secondly, there must be a real prospect that the information sought will lead to the location or preservation of such assets; and thirdly, the order should, so far as possible, be directed at uncovering the particular assets which are to be traced. Although the specificity required will differ according to the facts of each case, the general principle appears to be that the order should not be wider than is necessary in the circumstances.

15. A key passage relating to this principle is to be found in the judgment of Morritt LJ in the *Marc Rich* case, where he said, referring to a passage in the judgment of Hoffmann J in *Arab Monetary Fund v Hashim*, the following:

"I do not understand Hoffmann J to be stating that a *Bankers Trust* order must be as specific as a subpoena in all cases …No doubt the degree of specificity required will differ according to the facts of each case and those facts will include the relationship between the person against whom the order is sought and the other persons against whom the claims are made. The court must in this, as in all other exercises of its discretionary powers, seek to achieve a just balance between those who seek such orders and those against whom they are sought. In striking such a balance it is necessary to consider the onerousness of compliance with the order sought without being tied down by rules relating to subpoenas."

Those words are also illustrative of the fourth principle; namely that 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.

16. Fifthly (and finally), it is established that 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.'

19. I will take the requirements for an order under the Bankers Trust jurisdiction in turn. As to the first, in the present case, I concluded that there is a good arguable case that whoever holds the cryptocurrency or traceable substitutes therefor does so as a constructive trustee for C. In this regard:

(1) There is a good arguable case that cryptocurrencies are a form of property. This is supported by the legal analysis in the Legal Statement of the UK Jurisdiction Task Force ('Legal Statement') paras. 71-84, referred to and adopted by Bryan J in AA v Persons Unknown [2019] EWHC 3556 (Comm) at [56]-[61].

(2) There is a good arguable case that 'when property is obtained by fraud equity imposes a constructive trust on the fraudulent recipient: the property is recoverable

and traceable in equity' (to use the words of Lord Browne-Wilkinson in Westdeutsche Landesbank Girozentale v Islington BC [1996] AC 668 at 716). This principle was applied in relation to intangible property which was neither a thing in possession nor a thing in action in Armstrong GmbH v Winnington Networks Ltd [2012] EWHC 10 (Ch), esp at [127]; and see *Snell's Equity* (24th ed), para. 26-012.

(3) While there are arguments, drawn to my attention by Mr Yeo, that transfer of Bitcoin on the Bitcoin blockchain may create a new asset in the hands of the acquirer (Legal Statement para. 47), nevertheless there is a good arguable case that the transfers can nevertheless be the subject of tracing, on the basis that there is a relevant substitution (see *Lewin on Trusts* 20th ed., 44-063-071, *Civil Fraud: Law, Practice & Procedure* ed. Grant and Mumford, 23-014-015).

20. The case summarised in the preceding paragraphs has been formulated on the basis that the law of England and Wales is applicable. I concluded that there is a good arguable case that that is so. Specifically there is a good arguable case that:

(1) The claim can be regarded as one involving a non-contractual obligation arising out of a tort/delict for the purposes of Article 4(1) of the Rome II Regulation (Reg (EC) No. 864/2007, as amended).

(2) That the relevant cryptocurrencies were at the time of the hack located and has their *situs* in England and Wales, on the basis that C is resident and carries on its relevant business here. This is supported by the analysis in Dickinson *Cryptocurrencies in Public and Private Law* para. 5.109 and *Dicey Morris & Collins on the Conflict of Laws* (16th ed) para. 23-050; and by the reasoning in Tulip Trading Ltd v Bitcoin Association for BSV [2022] EWHC 667 (Ch) at [147]-[149] per Falk J. I consider that there is a good arguable case that this is so, notwithstanding the fact that C's servers are located in Romania, which may be regarded as an adventitious circumstance.

(3) That accordingly, either the cryptocurrency can be regarded as 'damaged' in England and Wales because it is in England that it was taken from C's control (see *Dicey Morris & Collins* op cit at para. 35-027) or because C as an English company has suffered loss and damage in England.

21. The second principle in relation to the grant of an order under the Bankers Trust jurisdiction is that there should be a real prospect that the information sought will lead to the location or preservation of the misappropriated cryptocurrencies. I was satisfied that, given the nature of the apparent fraud and of the information sought, which is in particular as to the identity of account holders and the destination of transfers, that this was so.

22. The third principle in relation to the grant of a Bankers Trust order is that the order should not be wider than is necessary. This is a matter which has been addressed in the context of exactly what information was ordered to be provided: see below.

23. The fourth principle is that the interests of the claimant in obtaining the order must be balanced against the possible detriment to the respondent(s) in complying with the order. As to this, there was and is a clear benefit to C in obtaining the information sought. I was satisfied that the potential detriment to Ds could be eliminated or at

least very effectively mitigated by C's undertakings as to expenses and damages, the restriction on collateral use, and the provision in the order that Ds are not required to do anything which would contravene local law.

24. The fifth principle relates to the undertakings to be given by C. Such undertakings were offered in this case.

25. Accordingly, I considered that there was a good arguable case on the merits of a claim under the Bankers Trust jurisdiction. I should add that, given that there seems no doubt that the Ds were 'mixed up' in the fraud (in the relevant sense, which does not involve any fraud or wrongdoing on their part), I consider that these considerations also show that there was a good arguable case that relief should be granted under the Norwich Pharmacal jurisdiction.

The existence of a 'gateway'

26. The second jurisdictional issue is whether there is a good arguable case as to the availability of a 'gateway' for service out. I considered that there clearly was, namely the new 'gateway' in PD 6B §3.1(25) which applies where:

'A claim or application is made for disclosure in order to obtain information —

(a) 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 claim or application is made for the purpose of proceedings … which, subject to the content of the information received, are intended to be commenced either by service in England and Wales or CPR rule 6.32, 6.33 or 6.36.'

27. The information sought falls within the terms of (a)(i) and (a)(ii). As to (b), C's stated intention is that, should the information obtained reveal potential cause of action defendants in the jurisdiction, it will commence proceedings against them here. Equally, if the information indicates that they are outside the jurisdiction, C intends to commence proceedings here and to seek to serve such proceedings out of the jurisdiction. I concluded that there is a good arguable case that this would be possible on the basis of the potential applicability of the 'gateways' in PD 6B §3.1(11) and/or (15). There is an argument, based on what was said in Fujifilm Kyowa Kirin Biologics Co Ltd v Abbvie Biotechnology Ltd [2016] EWHC 2204 (Pat) at [97] per Arnold J, that the location of the assets should be their location at the time permission to serve out of the jurisdiction is sought, but I do not consider that what was said in that case, which were *obiter dicta*, means that there would not be a good arguable case as to the availability of service out in such a case as this.

Is England and Wales the proper forum?

28. The third jurisdictional issue is whether England and Wales is the proper place in which to bring the claim. On the basis of the information presently available (and which was available on 28 October 2022), England does appear to be the proper place for the action to be brought. C is an English company; there are good grounds for considering the *situs* of the cryptocurrency to be in England; relevant documents are

in England; and the law of England and Wales at least arguably governs the proprietary claim.

The Application for Service by Alternative Means

29. The second principal application which needed to be determined on 28 October 2022 was C's application to serve the Defendants by alternative means, pursuant to CPR 6.15, 6.27 and 6.37(5)(b). There must be 'good reason' for such permission to be granted. Further, in the case of defendants situated in Hague Service Convention countries, at least where those countries have entered a reservation under Article 10, there need to be exceptional or special circumstances, which I take to mean that there must be a factor which provides a sufficiently good reason for such service notwithstanding the significance to be accorded to the reservation.

30. I was satisfied that there was a good reason (and to the extent necessary, exceptional circumstances) afforded by the nature of the claim and the need for steps to be taken as soon as possible to seek to identify the relevant defendants and to preserve property. I recognised that the case could not be properly described as one of 'hot pursuit', given the length of time between the fraud and now, but I did not consider that C was blameworthy in this regard, and the fact that time had elapsed did not mean that it was no longer important for there to be expedition. Steps should be taken before the scent goes colder. Accordingly I made orders for service by alternative means by email at a number of specified email addresses and in one case additionally by posting a link to the documents on the online contact form on the relevant Defendant's website. The order provided that the Defendants should be able to apply to set this order aside.

Further orders

31. The order made on 28 October 2022 also ordered that the hearing of C's application on notice to the Defendants should take place on 11 November 2022. In order that the purpose of the application should not be defeated by publicity, I also made confidentiality orders, which directed Ds, until the hearing, or further order of the court, and except for the purpose of obtaining legal advice, not to inform persons (other than subsidiaries) of the proceedings or the contents of the order. It also ordered that if the Defendants contacted their subsidiaries about the claim, they should obtain an undertaking from those subsidiaries that they should not inform others about the claim, in a form which was annexed to the order.

The 11 November 2022 Hearing

32. According to the information which C provided and which was available to the court at the hearing on 11 November 2022, it appeared that each of the Defendants named in the Claim Form for which permission to serve out had been given on 28 October 2022 had received notice of the hearing by the means ordered. None had applied to set aside that order for service by alternative means. At the hearing itself, D1 attended personally through a representative. As I have said, D5 was represented by Mr Yeo. I will return to the position of the different Defendants in due course.

33. C sought that the hearing should be in private. This was not objected to by those Defendants participating. I considered, again in order that publicity should not defeat

the object of the application, that it was necessary to hold the hearing in private. I indicated however, that I would wish to ensure that there should be a public judgment setting out the reasons for what had been determined (anonymised or redacted only to the extent necessary to ensure that the object was not defeated).

34. The hearing was being conducted and orders were being sought by C at a point at which it was still open to the Defendants to challenge the jurisdiction of the court under CPR Part 11, including by a challenge to the order permitting service out of the jurisdiction. None of the Defendants had positively stated that it would challenge the court's jurisdiction, but D2, D3 and D5 had expressly reserved their positions in relation to this. The orders to be made had necessarily to be tailored to preserve the Defendants' right to challenge the jurisdiction, and any participation in the hearing by D1 and D5 and any concessions made by D2 and D3 in relation to the relief sought were without prejudice to such rights.

The Application for Bankers Trust relief

35. As to the merits of the application for Bankers Trust relief, I considered, for reasons I have already given in the context of the application for permission to serve out, that C has a good claim to such relief.

36. I should, however, address one specific point to which reference was made in correspondence with C's solicitors by the solicitors for D2. That is that there is an argument to the effect that the making of Bankers Trust orders against foreign defendants constitutes an infringement of the sovereignty of a foreign jurisdiction and should only be made in exceptional circumstances. It was suggested that such an argument can be made on the basis of what was said in Mackinnon esp at 493-4 per Hoffmann J.

37. In my judgment the approach indicated in Mackinnon is inapplicable in the present case. Here, it is not known where the relevant documents are located. While there is clearly a possibility that the documents are in another or other jurisdictions, they may be in this one. Furthermore, it may well be that the location of the documents (which may be electronic) is of little significance. The court is faced with the novel challenges of fraud in relation to cryptocurrency transactions, and an approach adopted in relation to banks in 1985 does not seem to me to be apposite. In any event, Hoffmann J himself recognised in Mackinnon that such orders might be made in exceptional circumstances, and that exceptional circumstances had been found where crime and fraud were involved (see at 498 by reference to London and County Securities Ltd v Caplan (Unreported) 26 May 1978). The present case involves crime and fraud and the pursuit of assets. Although that pursuit cannot be said to be 'hot', it is nevertheless important that there should be no further avoidable delay. It would be impractical and contrary to the interests of justice to require a victim of fraud to make speculative applications in different jurisdictions to seek to locate the relevant exchange company and then to seek disclosure, probably in aid of foreign proceedings. That would be productive of increased costs, and delay, and reduce the possibility of effective location of the fruits of fraud. Concerns about national laws can be catered for by the terms of the order which make clear that no respondent is required to do anything contrary to local laws.

The position of the Ds

38. The position of the various Ds was, as it appeared at the hearing on 11 November 2022, as follows.

D1

39. D1 appeared at the hearing, and raised the entirely legitimate concern that there should not be identification of an inappropriate defendant. D1 did not raise substantive objections to the relief sought.

D2

40. As I have said, D2 had, through its solicitors Herbert Smith Freehills, made reference to Mackinnon. It had, however, also made it clear that it would not actively oppose the granting of a Bankers Trust order, and would take a neutral position in the present case. In addition, it raised points about the confidentiality provisions and the terms of the order. And, significantly, it stated that D2 is not the ultimate entity which owns or operates the Binance.com exchange and does not hold the information sought, nor does it have an unfettered legal right to demand that information from any other Binance entities. Nor was it willing to identify the relevant entity. It said that, nevertheless, if the court granted the order it would request the information from other 'Binance Operators' (as defined in the terms and conditions on the Binance website).

41. The difficulty of C not knowing which was the precise legal entity concerned, in circumstances where the exchange 'topco' was not willing or able to say, was addressed by C by seeking to add a 'Persons Unknown' Defendant in respect of the Binance exchange. Thus, at the hearing on 11 November 2022 I gave permission for the addition of an eighth Defendant, namely 'Persons Unknown (being the individuals or companies or other entities who are identified in the Binance.com platform's terms and conditions as Binance Operators but not [D2])'.

D3

42. D3 was named because C contended that it is the 'topco' in relation to the Kraken exchange. D3's response to service of the proceedings was that C was in breach of a contract between C and D3 whereunder C had agreed not to bring an action against Payward entities without complying with its terms and conditions. It is not necessary to set out that issue in any detail. D3 maintained that position, but indicated, without submitting to the jurisdiction, that it would comply with an order if made.

D4

43. Issues were raised in correspondence from D4 as to the whether the correct Defendant had been named. This led to C seeking permission, which I granted, to add the 7th Defendant. A concern was also raised as to whether the order required a cross-border transfer of personal information. It appeared to me that that issue would be sufficiently dealt with by the provision that the order did not require the defendant to do anything prohibited by local law.

D5

44. Coinbase Inc, through its solicitors DLA Piper UK LLP and counsel, had indicated that it, rather than Coinbase Global Inc, which had originally been named, was the

relevant entity. I made an order substituting it as D5.

45. D5 pointed out that the sum allegedly received by a Coinbase user was very small, but it indicated that it was nevertheless prepared to provide information to assist C to identify the alleged fraudster. D5 made a number of points as to the terms of the order, and in particular as to the width of the information which should be provided. In substantial measure as a result of these submissions, the information which I ordered should be produced (for all Defendants) was as follows:

> 1. In respect of any customer account(s) which the Target Cryptocurrency was allocated to and/or received on behalf of:
>
> (a) the name the account(s) is held in;
>
> (b) All 'Know Your Customer' (**KYC**) information and documents provided in respect of the account(s);
>
> (c) Any other information and documents held in relation to the account(s) which does (or which the relevant Defendant consider is likely to) identify the holder of the account(s), including email addresses, residential addresses, phone numbers and bank account details, save that any bank account details and/or social security numbers may be partially redacted by the relevant Defendant.
>
> 2. To the best of the Defendant's ability:
>
> (a) An explanation as to what has become of the Target Cryptocurrency (for the avoidance of doubt, this should be with reference to the customer account which is not necessarily the same as the recipient address listed in Schedule 1);
>
> (b) The balance in the customer account referred to under sub-paragraph (a) above: (i) immediately before it was allocated and/or received the Target Cryptocurrency; and (ii) at the time of that Defendant's response pursuant to this order;
>
> (c) (In respect of the 1st-4th and 6th-8th Defendants only) insofar as transfers have been made from (or on behalf of) that customer account to any other recipient address between [date A] and [date B], if those recipient addresses are associated with customers of the relevant exchange, the name and residential address of each accountholder.

46. D5 also submitted that the court should not make a Confidentiality Order in the form which had been included in the order of 28 October 2022, and which was included in C's draft order for 11 November 2022. That form of order required, in outline, that if a defendant needed to contact a subsidiary to respond to the claim, it should seek to obtain a written undertaking from that subsidiary that it would not disclose the existence of the proceedings or order and agree that the undertaking was subject to English jurisdiction. D5's submission was that it was inappropriate to order a Defendant to obtain an undertaking from a subsidiary (which included an obligation to submit to the jurisdiction of the English court). I considered that that objection had considerable force. Accordingly no such provision was included in the order made on

11 November 2022. The position in relation to subsidiaries who needed to be informed was dealt with by adding the 9th to 12th Defendants, so that any persons who fell within those limited categories would be directly bound by the confidentiality provisions of the order. D5 reserved its position as to whether that was an appropriate way in which the issue was dealt with (since it did not affect D5 in the case).

47. D5 also submitted that C's undertaking as to collateral use should specifically prohibit use of the information obtained for the purpose of a substantive claim against any of the Defendants without the leave of the court. Accordingly, the terms of the undertaking which was required from C in this respect was in the following terms:

> As to collateral use:
>
> (1) Subject to sub-paragraph (2) below, the Claimant shall only use the information and disclosure provided by the Defendants for the purpose of recovering their (allegedly) misappropriated assets or damages in respect of the misappropriation (which shall include (i) taking further steps in this claim or to obtain further information / documentation from third parties as well (ii) bringing proceedings against any persons who may be liable to the Claimant in relation to the alleged misappropriation of assets).
>
> (2) The Claimant will not use the information or disclosure provided for the purpose of any substantive claim against any of the Defendants without prior permission from the court.
>
> (3) The Claimant shall use reasonable endeavours to keep the disclosure and information provided confidential to the extent that is possible and permitted by the court (including redaction and/or ensuring such disclosure is subject to protective orders to prevent public inspection).

D6

48. D6 had made no substantive comments (whether by way of objection, reservation of position or otherwise).

Summary

49. In the circumstances I was prepared to make an order requiring the provision of information and documentation. The dates for compliance were adjusted so that they fell after the date on which any application under Part 11 had to be made. Insofar as Defendants were added, provisions were included as to permission to serve out, alternative service, and time for challenging the jurisdiction of the court. C was required to give undertakings covering expenses and loss in usual terms. It was also required to provide an undertaking as to collateral use in the terms which I have set out above. End dates for the confidentiality and privacy obligations, subject to further order of the court, were provided for.