CRYPTO DISPUTES CONFERENCE

29 June 2022

Mark Pelling QC[1]

Issues in Crypto Currency Fraud Claims

Good morning and thank you for asking me to speak this morning. Everything I say in the next few minutes represent my personal views[2]. They are not those of the Judiciary of England and Wales.

Many of you will be very familiar with the joys of Smart Contracts, block chain, distributed ledgers, crypto assets and currencies, Public keys and Private keys. For those of you who are not as familiar as you would like to be, or wish to undertake a refresher course on these issues, I recommend The Legal Statement on Crypto assets and Smart Contracts published by the UK Jurisdiction Taskforce in November 2019 and Law Commission Paper No 401 entitled "*Smart legal Contracts – Advice to Government*". They provide an invaluable insight into this world and should be read by all practicing law in this field. The critical conclusion reached by the Law Commission is that no legislative reform is necessary and that the common law is well able to facilitate and support these emerging technologies. The primary focus of the Law Commission paper is on claims between parties to smart contracts rather than those who have been the victims of fraud. However there is no indication that any different approach will be adopted in relation to fraud claims.

Cyber currency fraud claims have shown a steady up tick in volume over the last 12 to 18 months. Many and perhaps most of these cases appear to be issued in the London Circuit Commercial Court. They pose very significant procedural and jurisdictional difficulties with the same common themes arising in most if not all cases. The problem is an acute one because very often the sums lost are relatively small by the standards of most claims started in the LCCC but the loss can nevertheless be life changing for the victims. Such victims are all too frequently faced with the loss of most, if not all, their life savings, or sums that they have borrowed and on occasion over borrowed and secured against their homes. At this moment of acute anxiety, they are faced with finding lawyers to attempt to recover what has been lost and to do so in a legal environment that is technically and legally difficult. This inevitably adds to the cost of commencing proceedings and I suspect that cost may beyond the means of at least some victims.

In the next few minutes, I will be focussing on some of the principal issues that arise in most cases, and on the solutions that the law has so far provided. A word of warning however- no crypto currency fraud claim has yet reached the Court of Appeal. Very few if any have yet been the subject of fully

[1] His Honour Judge Pelling QC, Judge in Charge, London Circuit Commercial Court, a constituent court of the Business and Property Courts of England and Wales, a group of specialist courts and lists within the High Court of England and Wales.

[2] I am grateful to Paul Lowenstein QC, who has kindly read and commented on this paper in draft. The responsibility for the contents remains mine alone however.

contested hearings between claimants and respondents and in consequence most of the principles that the courts have applied to date have been developed in without notice hearings or hearings at which the respondents have chosen not to participate.

The problems that arise are generally ones of identification and jurisdiction in relation to those who have engineered the fraud, those to whom assets belonging to the victims have been transferred and received either unconscionably or otherwise and those who can provide relevant information about the identity of those responsible for the fraud or the whereabouts of the victim's assets or their traceable equivalent.

The overarching difficulty is that in most of these cases the principal actors will be located outside England and Wales as will the exchanges that administer the wallets into or through which the victims assets have passed. In most cases therefore the victim of a cyber currency fraud domiciled and resident in England, or who has suffered losses in England will be faced with the need to seek information disclosure orders against those who administer the relevant wallets and a worldwide freezing and/or proprietary freezing order usually against fraudsters who can be identified initially only as persons unknown, who are almost certainly located in offshore jurisdictions and in respect of whom the only known contact details are the email addresses used to carry the fraud into effect.

Most of these frauds follow a similar pattern. Those instigating the fraud advertise the availability of an apparently very attractive investment opportunity via an internet site. The victim makes contact with the fraudsters typically via email or phone or both. The victim is encouraged to buy a crypto currency using their fiat currency savings or borrowings and then give those apparently offering a legitimate investment service access to the relevant wallets to which the victim's crypto assets are credited by supplying the private key or giving access to the victim's PC. The ostensible purpose of this access is to allow the victim's crypto assets to be used by the ostensible advisor to grow the assets. There are a number of schemes that are said to enable this to be done. One involves active trading between different crypto currencies. Another involves transferring crypto currency belonging to multiple different people in order to enable investment gains to be obtained that would not be available to those holding smaller parcels of the crypto asset concerned. Often these fraudulent schemes involve the generation of sham trading account statements suggesting substantial gains have been made. The existence of a fraud comes to light when the victim seeks to transfer some or all of the assets back to the victim's control when there will first be various excuses, then perhaps an invitation to make a further payment in order to secure release of the victim's assets and then no responses at all.

The victim consults his solicitors and the first issue that arises is who is to be sued and for what. Investigations reveal that what appeared to be a bona fide investment organisation does not exist and is not registered with or regulated by the FCA or any overseas regulator. It may then be thought that information could be obtained by seeking it from the entities controlling the wallets to which or through which the victims crypto assets have been transferred. In conventional commercial fraud litigation such information is routinely sought by applying for information using either the Norwich

Pharmacal[3] or the Bankers Trust[4] jurisdictions. In conventional fraud litigation these applications are usually issued as Part 8 Claims with collection procedures against those responsible for the fraud being delayed until the information is to hand. However there is currently a trap for the unwary, where the entity from which information is sought is located outside England and Wales. In summary:

- there is first instance authority that there is no gateway within Practice Direction 6B that permits a claim for a Norwich Pharmacal to be served out of the jurisdiction whether as a free standing claim or as a claim made in the same claim form as a claim against those responsible for the alleged fraud[5]; but
- There is first instance authority[6] that a court can permit service out of a claim under the Bankers Trust jurisdiction but:
    - since that depends on the necessary or proper party gateway the claim has to be included in a claim against the putative fraudsters who at that stage will not have been identified;
    - There needs to be evidence of urgency and that the order is being sought in aid of hot pursuit[7] and
    - Since the jurisdiction is only available in support of a proprietary claim, the claim against the putative fraudsters has to be formulated in that way[8].

There is a further practical consideration in all this. The assumption that underlies what I have said so far is that the English court should be the court approached for orders of this sort. However, if the respondent entity is located out of the jurisdiction and is not amenable to enforcement procedures then seeking information orders from such entities may be an expensive and ultimately pointless exercise. In at least one case such an entity on being served with a Bankers Trust order asserted that it was not amenable to the English court's jurisdiction and therefore would not comply with the order and that if an order was required then it should be sought from the courts of the state where it was based – I think the BVI. This was not a particular difficulty in that case because the local courts applied essentially the same principles as the English court. This creates a risk for a claimant since if the entity considers itself not bound then it may well not comply with the anti tipping off gag imposed by such orders. It may be more effective to apply in the local court for the appropriate order if the local court

[3] Norwich Pharmacal Co. v. Customs and Excise Commissioners [1974] A.C. 133. The criteria that must be satisfied if an order is to be obtained are those summarised in Mitsui & Co v Nexen Petroleum UK Limited [2005] EWHC 625 (Ch), 3 All ER 511 at paragraph 21 (Lightman J)

[4] Bankers trust Co v. Shapiro [1980] 1 WLR 1275. This form of order is available to assist in locating assets in which a proprietary interest is claimed. The criteria that must be satisfied if an order is to be obtained are those summarised in Kyriakou v Christie's [2017] EWHC 487 (QB) at paragraphs 14 – 15 (Warby J as he then was).

[5] AB Bank Ltd v Abu Dhabi Commercial Bank PJSC [2016] EWHC 2082 (Comm) (Teare J) but see Lockton v Google Inc [2009] EWHC 3243 (QB) (Eady J).

[6] Ion Science Ltd and another v. Persons Unknown [2020] Unreported 21 December at paragraphs 19-21 (Butcher J)

[7] Mackinnon v Donaldson, Lufkin and Jenrette Securities Corp [1986] 1 Ch 482 (Hoffman J, as he then was).

[8] See also CMOC v Persons Unknown [2018] EWHC 2230 (Comm), where Waksman J considered that CPR 25.1(1)(g) could provide some assistance in non proprietary cases. However, this really begs the jurisdiction question where the party from which information is sought is overseas and has been joined only for the purpose of obtaining information.

has jurisdiction to make it. That said, the impression I have is that for most exchanges, the reputational risk posed by not complying with court orders encourages compliance.

This problem will hopefully be solved in part at least by the end of this year[9] with the introduction of a new Gateway 23 into CPR Practice Direction 6B[10]. The work relating to this has been led by a specialist sub-committee of the CPRC led by Foxton, Miles and Chamberlain JJs and supported by Paul Lowenstein QC and Sam Goodman. When enacted, the new Gateway will permit the service out of the jurisdiction of a Part 8 claim for disclosure of information regarding the true identity of a potential defendant or what has become of the property of a claimant in aid of proceedings which it is intended to commence, without the need to commence Part 7 proceedings against persons unknown. This will substantially reduce the cost of at least the information gathering stage of the process.

As things stand currently, assuming it is decided that the only course is to seek a Bankers Trust order, then it will be necessary to commence substantive proceedings against those responsible for the fraud before an application for a Bankers Trust order can be made. Given the constraints that apply to the Bankers Trust jurisdiction, any such claim will have to include a proprietary claim. However the next hurdle is that the identity of those responsible for the fraud will be unknown (hence the need for the Bankers Trust order) and they too are likely to be out of the jurisdiction.

This is addressed now as a matter of routine by commencing proceedings against Persons Unknown but again there is a trap for the unwary. The court will permit claims to be brought and will grant injunctions against persons unknown[11] but the court will require the claimant in such a case to identify by description those coming within the class of defendant so identified[12] In a crypto fraud claim it is likely that crypto assets will have been moved multiple times after removal from the claimant's wallet. It may be necessary therefore to bring proceedings against different classes of persons unknown in order to cater for these possibilities. Typically these will be (a) the individuals or companies who, without express authorisation or consent, obtained access to the victim's accounts; (b) the individuals

[9] Currently, it is thought that the relevant statutory instrument will be paid in Parliament on 15 July and come into force on 1 October 2022.

[10] The current draft text of the new Gateway is:

Information orders against non-parties

(23) 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) for the purpose of proceedings already commenced or which, subject to the content of the information received, are intended to be commenced either by service in England and Wales or pursuant to CPR 6.32, CPR 6.33 or CPR 6.36.

[11] See the initial and return date judgments in CMOC v. Persons Unknown at [2017] EWHC 3599 and 3602 and more recently AA v Persons Unknown [2019] EWHC 3556 (Comm) and Fetch.AI Limited and another v. Persons Unknown (categories A, B and C) [2021] EWHC 2254 (Comm).

[12] See e.g. Bloomsbury Publishing Group Limited v News Group Newspapers Ltd [2003] EWHC 1205 (Ch) [2003] 1 WLR 1633 and Hampshire Waste Service v Persons Unknown [2003] EWHC 1738 (Ch).

who were knowing receivers of the claimant's crypto assets and (c) those to whom the assets are transferred and who were not aware of the claimant's interest in the assets[13]. The purpose of the third class is to enable those who have received the claimant's assets without knowing or believing the assets belonged to the claimant to be excluded from the scope of freezing orders, whilst recognising that claims against such defendant might be made for the recovery of such assets through subject to defences such as bon fide purchase for value.

As I have said, if a Bankers Trust order is to be sought, it will be necessary to show that the claimant has at least a realistically arguable proprietary claim, which passes through at least one of the jurisdictional gateways set out in Practice Direction 6B so as to enable the claimant to obtain permission to serve the claim out of the jurisdiction. This begs the question whether crypto assets are property for these purposes. As to this, there are now a number of judgments made on applications for urgent interim relief that hold that they are[14]. However these cases all proceed on the basis of realistic arguability. Whilst there are real arguments that can be deployed to the effect that crypto currency is not property, which focus in particular on the intangibility of such assets, such a conclusion would significantly affect the rights of holders of such assets and would suggest that the judgment of the law Commission that the common law is well able to facilitate and support these emerging technologies is misplaced. In my view therefore it is unlikely that this direction of travel will be reversed. However this may depend on the nature of the asset concerned. It may be for example that different conclusions will be reached in relation to at least some non fungible tokens.

The other issue of importance that emerges from the current case law concerns the location of a crypto asset. This is important in particular in relation to extra territorial claims against alleged fraudsters because the gateways most relevant to a proprietary claim[15] each focus on events occurring within the jurisdiction or on property within the jurisdiction and because it is likely to be determinative in identifying the governing law[16] which in turn is highly material to the question of whether England and Wales is the most appropriate jurisdiction in which to commence the claim. The approach that has generally been adopted by the courts has been to treat crypto assets as located in the place where the person who owns it is domiciled or resident[17]. Although most of the cases where this issue has been considered have been without notice or unattended by respondents, the most recent[18] was a fully contested jurisdiction challenge. It is likely that in the future this authority will be referred to as a matter of course since it is the

[13] For an example see Fetch.AI Limited and another v. Persons Unknown (categories A, B and C) (ibid.) at paragraphs 6-7

[14] See e.g; AA v Persons Unknown ibid. at paragraph 57; Ion Science Ltd v Persons unknown, ibid. at paragraph 11; and Fetch.AI Limited and another v. Persons Unknown (categories A, B and C) (ibid.) at paragraphs 14-15 and most recently Tulip Trading Ltd v. Van Der Laan [2022] EWHC 667 (Ch) at paragraph 141 (Falk J). Similar conclusions have been reached by judges in New Zeeland – see Ruscoe v Cryptopia [2020] NZHC 728 – and Singapore – see Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.

[15] Practice Direction 6B, paragraphs 3.1(11) and (15)

[16] See Regulation (EC) No 864/2007 Of The European Parliament and of The Council of 11 July 2007 on the law applicable to non-contractual obligations ("Rome II"), Articles 3, 4,10 and 11.

[17] See Ion Science, ibid. at paragraph 13, followed in Fetch. AI Limited (ibid) at paragraph 14. In Tulip Trading (ibid.) the corporate entity was registered in the Seychelles but operated by an individual resident in England. The Judge held that the *lex situs* of the crypto asset concerned was to be tested by reference to domicile or residence.

[18] Tulip Trading (ibid.)

most comprehensive consideration currently available. These conclusions depend ultimately on an academic conclusion[19] however. On balance it seems unlikely that this direction of travel will be reversed either if only on the pragmatic grounds that it is predictable, easy to apply and is capable of being applied to all crypto currency assets.

I have emphasised the advantages in formulating a claim as a proprietary claim. There are a number of causes of action available of course, including deceit, unjust enrichment and breach of confidence, but these are personal rather than proprietary. That is not a reason for not including them and such claims are routinely included.

In relation to proprietary claims, generally it is argued that English law imposes a constructive trust on a fraudulent recipient of property obtained by fraud[20]. Courts have generally held this principle to apply in respect of crypto assets obtained by fraud[21]. However this issue is highly fact sensitive. It is well established now that if property is transferred under a contract or arrangement induced by fraud, title passes to the recipient until the contract is rescinded[22], at which point the recipient holds the sums received on constructive trust for the transferor. There is a significant legal issue here, which it has not been necessary for courts to grapple with in crypto fraud claims to date because of the nature of the applications being made and the tests that the court will apply on without notice applications for proprietary and world wide freezing orders. In many and perhaps most crypto currency fraud claims, the allegation will be that assets have been removed from wallets without consent and so a constructive trust may be said to arise immediately. However, there are cases where a victim has been fraudulently induced to transfer assets to the fraudulent recipient, or enter into a contract under which assets were transferred, where the rescission issue may become important. However the practical significance of this as an issue will be significantly reduced once Gateway 23 becomes available.

In the time that remains I should briefly address service issues. As will be apparent from what I have said so far in relation to those responsible for the fraud it will very often only be possible to serve proceedings either directly using the messaging or email addresses used by the fraudsters when carrying the fraudulent scheme into effect or indirectly by passing pleadings evidence and orders to the entities that provided the wallets used by them to carry the fraudulent scheme into effect. This requires an order permitting service by an alternative means[23]. Although there is a distinction to be drawn between service in Hague Service Convention states and non signatory states, it will make no practical difference simply because the only possibility of serving the Persons Unknown defendants will be by such means. However different consideration apply to the service of Bankers Trust orders on entities likely to have KYC information in relation to the persons unknown. Whilst service by an alternative means will only be

[19] See Fox et al, Cryptocurrencies in Public and Private Law at paragraph 5.106-109.

[20] Westdeutsche Landesbank Girozentrale v London Borough of Islington [1996] AC 668 at 716C-D (Lord Browne-Wilkinson)

[21] See CMOC v Persons Unknown [2018] EWHC 2230 (Comm) at paragraphs 76-77, AA, ibid at paragraph 62, Ion Science, ibid. at paragraph 14; and Fetch. AI Limited (ibid) at paragraph 15.

[22] See e.g. LIA v. Credit Suisse International [2021] EWHC 2684 (Comm) at [117]-[119].

[23] See CPR r.6.15

permitted in a Hague Convention state in exceptional circumstances[24], a court will usually permit service by an alternative means where mandatory order have been made that require compliance in early course particularly where there are gagging provisions included[25].

It is likely that these claims will proliferate as more people become more familiar with the availability of crypto assets. By their nature those who deal and administer such assets deal across frontiers. Managing the jurisdictional issues that arise in conventional claims between crypto counterparties may ultimately be require regional or global service regimes to be adopted across the sector, possibly using arbitration rather than state courts to resolve disputes. However none of that will assist in recovering assets lost by fraud though it may in the future at least provide a quicker, cheaper and more universally applicable method of obtaining information to enable fraudsters and stolen assets to be traced. That said, the white light of publicity would not be available under such a regime and potentially very difficult questions concerning the seat of any such arbitration will arise and with it the degree to which the arbitral process could be supervised by state courts.

There are some cases where it would appear that recipients of assets lost by fraud are starting to engage with the legal process. It is likely therefore that at least some of the issues I have referred to will be clarified in the months ahead.

[24] Russian Commercial Bank (Cyprus) Ltd v Khoroshilov [2020] EWHC 1164 (Comm) at paragraph 97 (Cockerill J)
[25] AA, ibid at paragraph 77 and Fetch. AI Limited (ibid) at paragraph 46-47