Tracing and recovering cryptoassets for Cayman and BVI insolvency practitioners

Insights - 09/09/2024

In many of the recent insolvencies of digital asset companies, liquidators have been appointed over companies in which digital assets have been fraudulently transferred from wallets controlled by an insolvent company into other unidentified wallets in foreign jurisdictions.

The anonymity of cryptoassets causes serious difficulties for insolvency practitioners in identifying the third parties who received funds and the location of the digital wallets.

Two previous articles considered the legal position on whether cryptoassets could be classified as property and examined the two complex and as yet unsettled questions as to who owns cryptoassets and where they are located for asset tracing purposes. This article outlines the tools and legal remedies available to insolvency practitioners seeking to trace and recover misappropriated cryptoassets.

Safeguarding against volatility

The volatility of cryptoasset markets is one of the first concerns for liquidators appointed over a company trading in or holding cryptoassets. Unlike ordinary shares or currencies, cryptoassets are extremely volatile. For example, in November 2022, Bitcoin recorded a 10-day volatility of more than 100%. As a result, liquidators appointed over digital asset companies need to consider whether the risk of volatility or a crypto market crash creates a fiduciary obligation to convert any digital assets held by the company into fiat currency or a "stablecoin" to protect the assets in the interests of unsecured creditors. A stablecoin is a type of cryptocurrency where the value of the digital asset is pegged to a reference asset such as the US dollar or exchange-traded commodities.

This problem arose in *Smith v Torque Group Holdings (in liquidation)*[1], where the BVI appointed joint liquidators raised concerns relating to fluctuations in crypto markets. This resulted in the cryptocurrency the company held decreasing in value by 28%. Ultimately, they sought and obtained sanction of certain actions including converting certain crypto assets into either US dollars or

Tether (**USTD**), which is a stablecoin pegged to the US dollar.

Tracing the assets

English courts were historically hesitant to order foreign third parties to disclose information in all but the most exceptional cases.[2] However, in recent cases involving crypto fraud, the English court's have been willing to grant disclosure orders in favour of claimants allowing them to trace the misappropriated digital assets, including Norwich Pharmacal and Bankers Trust orders.

Both the Cayman [3] and BVI [4] courts have the power to permit service outside of the jurisdiction for claims involving interim relief in the absence of substantive proceedings. [5]

In the BVI, this now takes the form of a self-certification procedure rather than requiring permission. Both the Cayman and BVI courts have found they have the jurisdiction to grant Norwich Pharmacal Orders in support of potential proceedings before a foreign court despite the existence of additional statutory remedies. [6] In *K v Z*, [7] the BVI court considered that the relief was not a remedy of last resort and it was highly unlikely that the BVI legislature's intention was that such equitable relief should be restricted where statutory remedies may exist in a similar manner to English cases. [8] Ultimately, the court will ask itself whether the relief should be granted in the interests of justice. It is therefore anticipated that the Cayman and BVI courts will take a robust approach to requiring third parties to give disclosure to assist claimants and liquidators in tracing assets.

Norwich Pharmacal and Bankers Trust orders

A Norwich Pharmacal order is a court order for disclosure of documents or information against a third party (which has been innocently mixed up in wrongdoing) which assist in bringing legal proceedings against the wrongdoers. [9] The requirements for the grant of a Norwich Pharmacal order are:

1. a wrong must have been carried out, or arguably carried out, by an ultimate wrongdoer
2. there must be the need for an order to enable action to be brought against the ultimate wrongdoer
3. the person against whom the order is sought must: (a) be mixed up in so as to have enabled the wrongdoing, and (b) be able or likely to be able to provide the information necessary to enable the ultimate wrongdoer to be sued [10]

A Bankers Trust order is a court order against a bank or financial institution to disclose the state of, and documents relating to, the account of a customer who was, on the face of it, guilty of fraud to allow the applicant to trace the misappropriated assets. [11] The principles for Bankers Trust orders derived from the authorities are:

1. there must be good grounds for concluding that the assets about which information is sought belonged to the claimant, and there must be a real prospect that the information sought will lead to the location or preservation of such assets
2. the order should, so far as possible, be directed at uncovering the particular assets which are to be traced. The order should not be wider than is necessary in the circumstances, and the court should seek to achieve a just balance between those who seek such orders and those against whom they are sought.
3. the applicant must provide undertakings: (i) to pay the expenses of the defendant complying with the order, (ii) to compensate the defendant in damages should they suffer loss as a result of the order, and (iii) only to use the documents or information obtained for the purpose of tracing the assets or their proceedings [12]

There is a significant degree of overlap between Norwich Pharmacal and Bankers Trust orders [13] and, in many of the recent cases involving digital assets, the applicants have sought both types of orders, with the courts readily finding that the respondent crypto exchanges are required to give disclosure to the claimant.

The information sought

In the recent cases involving disclosure orders, the claimants have sought information which allows them to identify the holders of the wallets which the misappropriated digital assets are transferred into. This includes relevant "Know Your Customer" and anti-money laundering information relating to the wrongdoers collected by the exchange, the balances of cryptocurrency held in the wallets and details of transactions involving the wallets. This gives rise to confidentiality issues under the terms and conditions of the exchange, particularly where those terms and conditions are designed to protect the confidentiality of customers.

In *Fetch.ai Ltd v Persons Unknown*, [14] the claimant sought information from a cryptocurrency exchange following a fraudster gaining access to their account and misappropriating US$2.6 million of cryptocurrency. Pelling J noted that the terms and conditions of the defendant exchange made clear that personal data relating to customers would be retained by the exchanges. This suggested that there was no absolute contractual right of confidentiality. That means those who used the exchange would have been aware that there is at least a risk of personal data being revealed. [15] Accordingly, Pelling J found that there was a real chance that if a disclosure order was made in relation to the wrongdoer's account, it would lead to the location and preservation of the misappropriated digital assets. [16]

On the other hand, in *LMN v Bitflyer Holdings Inc* [17] disclosure orders were sought against a number of exchanges. Some of them appeared at the hearing and, although they did not oppose disclosure orders and took neutral positions, objected to the width of the information requests. They instead sought to engage constructively to narrow the scope of information provided. [18]

Similarly, in *Scenna v Persons Unknown*, [19] which involved a non-crypto related fraud, two Australian banks successfully set aside ex parte Bankers Trust orders on the basis that the orders would have put them in breach of Australian banking and privacy laws which laws prohibited the disclosure of confidential client information in the absence of an Australian court order. Pickering J in *Scenna* distinguished *LMN v Bitflyer Holdings Inc*. on the basis that, in that case, the location of the assets was unknown whereas in *Scenna*, the plaintiffs had a clear alternative remedy (applying to the Australian courts).

Securing the assets

Seeking relief against "persons unknown"

In cases where assets have been misappropriated from insolvent digital asset companies, the persons holding those assets, and even the jurisdictions in which they reside, are often not readily identifiable. In *Cameron v Liverpool Victoria Insurance Co Ltd*,[20] Lord Sumption identified two categories of persons unknown: (i) those identifiable but whose names are unknown (for example, squatters are unnamed but identifiable by location), and (ii) those who are both anonymous and cannot be identified (such as hit and run drivers). Lord Sumption noted that it was impossible to serve a person falling within the second category "due not just to the fact that the defendant cannot be found but to the fact that it is not known who the defendant is."

Some recent crypto fraud cases have recognised that it is possible for the court to grant relief against "persons unknown". The critical feature here is that the description used by the claimant in the originating process must be sufficiently certain in order to identify both those who are included and those who are excluded. [21] For instance, the decisions in *AA v Persons Unknown* [22] and *Chainswap Limited v Persons Unknown*, [23] highlight a variety of persons unknown: (i) "persons unknown who demanded Bitcoin on 10th and 11th October 2019", (ii) "persons unknown who own / control specified Bitcoin", (iii) "the owner of digital wallet (Insert address)" and (iv) "the owner of email address (insert email address)".

Service of process on "persons unknown"

How the originating documents are to be served on defendants who cannot be identified, is an immediate issue (particularly since it is usually unclear what jurisdiction they are in). The claimant must follow the relevant procedure for service out of the jurisdiction, unless authoritative evidence exists suggesting the persons unknown are within the jurisdiction of the court.

In *AA v Persons Unknown*, the court concluded that, since it was unclear which jurisdiction the persons unknown were located, it was an appropriate case for alternative service by email and on the physical addresses provided by the crypto exchanges that related to the misappropriated Bitcoin. [24] In the later case of *D'Aloia v Persons Unknown*, the claimant was unaware of the

jurisdiction of the relevant persons unknown (who were internet scammers) but accepted that it was likely that they were outside the jurisdiction of the English court. Accordingly, the claimant sought orders for service by email and by non-fungible token (**NFT**) through a form of airdrop into the relevant wallet address, in respect of which the claimant made a transfer which would "embed the service in the blockchain." [25] Not only was Trower J satisfied that the form of airdrop was a valid form of service for the purposes of English Civil Procedure Rules, but he went on to say that "there could be no objection to it; rather it was likely to lead to a greater prospect of those who were behind the (relevant) website being put on notice of the making of the order and the commencement of the proceedings." Recognising the issues with identifying holders of cryptocurrency, the BVI court has also shown a willingness to grant alternative service including service by email and social media (including via X, formerly known as Twitter) [26] and, as well as service by NFT as was the approach taken in *AQF v XIO et al* [27], which endorses Trower J's comments in *D'Aloia*.

Seeking judgment against "persons unknown"

Two recent decisions involving cryptoasset fraud have come to contrary decisions following attempts by the plaintiff to obtain summary judgment against persons unknown. In *Boonyaem v Persons Unknown*, [28] Salter KC refused to grant summary judgment against one category of persons unknown, being the alleged fraudsters [29] on the basis that they fell within Lord Sumption's second category as they were both unknown and unidentifiable and "did not describe any identifiable person against whom judgment can properly be given".

Conversely, in *Mooij v Persons Unknown*, [30] dealing with defendant fraudsters described as "persons unknown" in a similar way, HHJ Russen KC questioned the outcome in *Boonyaem*, noting that in that case and on the facts of *Mooij*, jurisdiction had already been established over the fraudsters via alternative service orders made by the court. HHJ Russen KC considered that the comments of Lord Sumption in Cameron related to the impossibility of service on the second category of "persons unknown". However, in both *Boonyaem* and *Mooij*, the claimant had already served the proceedings, notifying the fraudsters of the proceedings and establishing jurisdiction. HHJ Russen KC said he could not: "see any obvious reason why that jurisdiction should not culminate in the ultimate purpose for which the claimant invokes it, which is to obtain judgment." [31]

Proprietary injunctions

When property is obtained by fraud, in order to secure the misappropriated digital assets a liquidator may seek a proprietary injunction against an entity which holds those assets. An applicant for a proprietary injunction must show that: (i) there is a serious issue to be tried; and (ii) the balance of convenience is in favour of the grant of an injunction; (iii) damages would not be an adequate remedy; and (iv) it is just and convenient to grant the order. [32]

In *Ion Science*, the claimants were victims of an elaborate fraud under which they transferred

cryptocurrency to individuals who represented that they were being invested in other cryptocurrency products. Butcher J found that the evidence established that the balance of convenience favoured the grant of an injunction given there was a prima facie case of wrongdoing and no evidence that the individuals (being persons unknown) would be able to satisfy a monetary judgment. [33]

The question of adequacy of damages is particularly noteworthy in the case of NFTs, which derive their value from being unique and impossible to replicate. In *Osbourne* it was found that damages would not be an adequate remedy as, although the NFTs in question were given a modest valuation of £4,000, the evidence demonstrated that the NFTs "have a particular, personal and unique value to the claimant which extends beyond their mere 'fiat' currency value". [34]

Worldwide freezing orders

An alternative, or additional, option for securing digital assets held by wrongdoers is a freezing order or Mareva injunction, which is an order preventing the disposal of the assets that is sought to preserve the assets until a judgment can be obtained. In order to obtain a freezing order, an applicant must show: (i) a good arguable case on the merits, (ii) a real objective risk of dissipation, (iii) there are assets held by the respondent within the geographical scope of the order, and (iv) it would be just and convenient in all the circumstances to grant the order. [35]

In cases involving digital asset fraud, it will generally be relatively easy to establish there is a risk of dissipation, due to the conduct involved and the inherent nature of digital assets. For instance, in *Ion Science*, Butcher J found the evidence established a real risk of dissipation given the nature of the claim (having involved fraud) and the defendant's conduct which involved the use of aliases and apparent false documents. [36] Similarly, in the Singapore case of *CLM v CLN*, [37] Lee Seiu Kin J found that there was a risk of dissipation due to the evidence showing that the digital assets were dissipated through a series of digital wallets that appeared to have been created solely for that purpose, and due to the nature of cryptocurrency which is "susceptible to being transferred by the click of a button, through digital wallets that may be completely anonymous and untraceable to the owner, and can be easily dissipated and hidden in cyberspace." [38]

In the *Chainswap Limited* decision, ChainSwap obtained a worldwide freezing order after unknown hackers exploited their system vulnerabilities, misappropriating assets from private users' wallets as well as apart of projects issuing digital tokens, which were subsequently received in separate digital wallets, and then traded and exchanged for different cryptocurrencies. Jack J considered that he had no difficulty in granting the freezing order as there was an "obvious risk of dissipation if no freezing order (was) granted". [39] In *Svirsky v Oyekenoc*, [40] the BVI Court of Appeal displayed flexibility by upholding a freezing order involving cryptoassets of a dissolved company (where there was a realistic prospect of its restoration)having been satisfied there was a good arguable claim in the amount sought to be frozen.

Further disclosure under the worldwide freezing orders

It is worth highlighting that the court has power to require a respondent to a worldwide freezing order to provide further information in relation to their assets. This includes what has become of assets which were or may have been previously held by the respondent, where there is "practical utility" in requiring such evidence and where it is "proportionate" and for a proper purpose. An example of where the court often considers it necessary to order further disclosure is where there is an obvious discrepancy between assets which were at one time held by a respondent, and the current assets disclosed in response to the disclosure orders in a freezing order, such that there is a real possibility that there are further assets to which the freezing order may apply. [41] That being said, the practice of the court is not to make an order for the purpose of investigating whether an injunction has been broken and (if so) to supply material for contempt proceedings. Instead, the purpose of any order which is made for further disclosure is to make the freezing order more effective. [42] For example, evidence as to historical transactions explaining what has happened to monies received can be regarded as falling within the scope of what is necessary to ensure that the freezing order is effective and can be policed.

Delivery up

Given the principle that stolen funds are held on trust for the victim, a claimant may seek an order for delivery up once the misappropriated cryptoassets are identified. Cayman office-holders in particular, may avail themselves of statutory powers to achieve similar results. [43]

In *Jones v Persons Unknown*, [44] after obtaining worldwide freezing orders and proprietary injunctions in respect of stolen cryptocurrency held on an exchange, the claimant sought summary judgment on his claim for relief including delivery up. Cooper J granted the relief, having found that the evidence provided by the claimant was "compelling" and sufficient to establish claims for unjust enrichment and deceit against the wrongdoers and that the exchange, as controller of the wallet, sat in the position of constructive trustee. [45]

Similarly, in *Law v Persons Unknown*, [46] after the claimant obtained default judgment against an alleged fraudster, and satisfied the court that certain cryptocurrency held in a wallet offshore contained the proceeds of fraud, the court ordered the cryptoassets be converted into fiat currency and delivered up to the jurisdiction to be paid into the court funds office, notwithstanding that the funds were already the subject of a worldwide freezing order.

The bona fide purchaser defence

It is important to note that misappropriated cryptoassets transferred into a hot wallet held by an exchange will not necessarily be held on constructive trust by that exchange. Whether it is held may depend on the way in which the exchange holds its assets on behalf of its accountholders. It is a defence to any claim for tracing based on fraud if the misappropriated funds are paid to a bona fide purchaser for value without notice of the fraud. [47] The claimant in *Pizoozzaadeh v Persons*

Unknown [48] learned this lesson the hard way. The exchange (on which the wallet receiving misappropriated assets was located) sought to discharge the injunction and adduced evidence that it did not retain property in any cryptocurrency transferred to its users. The exchange argued that (i) any cryptocurrency received was not specifically segregated to be held for the sole benefit of the user and was instead swept into the central unsegregated hot wallet as part of the exchange's general assets, and (ii) the user's account was credited with the amount of the deposit and the user was permitted to draw against any credit balance as in any conventional banking arrangement.

Accordingly, the exchange successfully argued that this arrangement meant that the exchange was a purchaser of the cryptocurrency (it purchased the user's cryptocurrency through granting it a credit balance) and it thus would not be susceptible to a remedy unless it could be shown to not be acting bona fide. [49]

Conclusion

The laws surrounding the use of digital assets are still in their infancy. However, as outlined above, there is a clear trend in creditors, insolvency practitioners and courts across the common law world successfully using traditional legal remedies and solutions to resolve the insolvency, asset tracing and recovery issues arising in respect of non-traditional cryptoassets.

This article was first published in IFLR on 13 August 2024.

Case citations

[1] BVIHC (COM) 0031 of 2021.

[2] See, for example *Mackinnon v Donaldson, Lufkin & Jenrette Corp* [1986] Ch 482.

[3] See Grand Court Rules, Order 11, rule 1(1)(n); Grand Court Act (2015 Revision), section 11A.

[4] See ECSC Civil Procedure Rules (Revised Edition 2023), rule 7.3(11).

[5] By contrast, a similar jurisdictional gateway was only introduced in Practice Direction 6B of the English Civil Procedure Rules in October 2022 which now permits service out applications against non-parties for the provision of information regarding the true identity of a defendant or potential defendant and/or what has become of the claimant's property where the information in question is required for the purposes of proceedings which have been, or are to be, brought in England. This gateway was first utilised in *LMN v Bitflyer Holdings Inc.* [2022] EWHC 2954 (Comm).

[6] *Essar Global Fund Limited v Arcelormittal USA LLC* [2021 (1) CILR 788].

[7] BVIHC (COM) 2020/0016 (Judgment on 10 March 2020).

[8] For example, see *R (Omar) v Secretary of State for Foreign Affairs* [2013] EWCA Civ 118 and *Ramilos Trading Ltd v Buyanovsky* [2016] EWHC 3175 (Comm).

[9] *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133.

[10] *Mitsui & Co Ltd v Nexen Petroleum UK Ltd* [2005] 3 All ER 511 at [21] as approved by the Cayman Islands Court of Appeal in Essar *Global Fund Limited v Arcelormittal USA LLC* [2021 (1) CILR 788] at [16].

[11] *Bankers Trust Co v Shapira* [1980] 1 WLR 1274.

[12] *Kyriakou v Christie Manson & Wood Limited* [2017] EWHC 487 (QB) at [12]-[16].

[13] See *Murphy v Murphy* [1999] 1 WLR 282 at 290.

[14] [2021] EWHC 2254 (Comm).

[15] *Fetch.a*i at [36].

[16] *Fetch.ai* at [33].

[17] [2022] EWHC 2954 (Comm).

[18] *LMN v Bitflyer Holdings Inc.* [2022] EWHC 2954 (Comm) at [38]-[48]. See also *Scenna v Persons Unknown* [2023] EWHC 799 (Ch)

[19] [2023] EWHC 799 (Ch).

[20] [2019] 1 WLR 1471.

[21] *Ion Science* at [11]; *Fetch.Ai Limited v Persons Unknown* [2021] EWHC 2254 (Comm) at [6]-[7].

[22] [2019] EWHC 3556 (Comm).

[23] Claim No: BVIHC (COM) 2022/0031 (Judgment on 4 May 2022).

[24] AA at [75].

[25] *D'Aloia v Persons Unknown* [2022] EWHC 1723 (Ch) at [39]. Orders for service by NFT were also granted in *Jones v Persons Unknown* [2022] EWHC 2543 (Comm). The *Chainswap Limited* decision suggests that the BVI Court permitted alternative service outside of the jurisdiction at [4] and [15]; however, it does not specify the permitted methods in the decision.

[26] See *Russell Crumpler and Christopher Farmer (as joint liquidators of Three Arrows Capital Ltd (in liquidation) v Su Zhu and Kyle Davies* Claim No: BVIHC (COM) 2022/00119 (Judgment on 19

December 2022).

[27] Claim No. BVIHC(COM) 2023/0239 (Judgment on 23 November 2023).

[28] [2023] EWHC 3180

[29] The fraudsters were described as: "the natural and/or legal person(s), describing themselves as being or connected to IngfxGroup and/or INGFX, and/or who operated/owned/controlled and/or were associated with the website www.ingfxgroup.com and/or with the phone numbers: 0616399663 and/or 0618374508 and/or with the Second and/or Third Respondent, who or some of whom gave the name Suthep Chansudarat, utilising a Facebook account by the same name, and who participated in a scheme to induce the Applicant to transfer 425,836.62 USDT to the Second and/or Third Respondent between 19 February 2022 and 16 June 2022)"

[30] [2024] EWHC 814 (Comm).

[31] *Mooij* at [56].

[32] *American Cyanamid v Ethicon* [1975] AC 396.

[33] *Ion Science* at [17]. See also *Osbourne* at [17].

[34] *Osbourne* at [20]-[21].

[35] *Les Ambassadeurs Club Ltd v Yu* [2021] EWCA Civ 1310 at [10]; *Broad Idea International Ltd v Convoy Collateral Ltd* [2021] UKPC 24 at [101].

[36] *Ion Science* at [18].

[37] [2022] SGHC 46.

[38] *CLM v CLN* [2022] SGHC 46.

[39] *Chainswap Limited v Persons Unknown* Claim No: BVIHC (COM) 2022/0031 (Judgment on 4 May 2022) at [16].

[40] BVIHCMAP2021/0040BVIHCMAP2021/0046BVIHCMAP2022/0005 (delivered 8 November 2023).

[41] *Public Institution for Social Security v Al Rajaan* [2020] EWHC 1498 (Comm) at [24]-[25].

[42] *JSC Mezhdunarodniv Promyshlenniy Bank v Pugachev (No.2)* [2016] 1 W.L.R. 781 at [38].

[43] See Cayman Companies Act, s 103(3)(b); BVI Insolvency Act 2003, s 274A.

[44] [2022] EWHC 2543 (Comm).

[45] *Jones v Persons Unknown* [2022] EWHC 2543 (Comm) at [19]-[21].

[46] [2023] 1 WLUK 577.

[47] *Akers v Samba Financial Group* [2017] AC 424 at [83].

[48] [2023] EWHC 1024 (Ch).

[49] *Pizoozzaadeh v Persons Unknown* [2023] EWHC 1024 (Ch) at [26]-[27].

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

Key Contacts

Gemma Bellfield (nee Lardner)

Partner

Cayman Islands

E: gemma.bellfield@ogier.com

T: +1 345 815 1880

Nicholas Brookes

Partner

British Virgin Islands

E: nicholas.brookes@ogier.com

T: +1 284 852 7366

Corey Byrne

Senior Associate

Cayman Islands

E: corey.byrne@ogier.com

T: +1 345 815 1842

Romauld Johnson

Associate

British Virgin Islands

E: romauld.johnson@ogier.com

T: +1 284 852 7387

Related Services

Legal

Dispute Resolution

Crypto Disputes

Related Sectors

Technology and Web3

Restructuring and Insolvency