# SEARCHING FOR ASSETS IN CYBERSPACE

# A NEW GATEWAY OPENS?

Authored by: Andrew James - PCB Byrne, and Hannah Daly - 4 New Square

*In this article, Andrew James, solicitor at PCB Byrne LLP and Hannah Daly, barrister at 4 New Square examine the new gateway 25 in Practice Direction 6B.3.1 which came into force on 1 October 2022 and allows service out of information orders. They look at what problems the gateway is designed to solve and how much further it is likely to get victims of cryptocurrency fraud who want to get substantive proceedings off the ground.*

## Introduction

On 1 October 2022, a new gateway 25 was added to Practice Direction 6B. This was one of a larger set of amendments and additions to the gateways which have subtly expanded the scope of the English courts' jurisdiction in a number of areas. The purpose of this new gateway is to put on a firmer footing the court's jurisdiction to make orders against foreign non-parties to obtain information or documents. This should be of assistance to claimants with an urgent need to identify the correct defendant or trace misappropriated assets. The gateway was developed specifically with cryptocurrency fraud claims in mind.[1]

In this article, we examine the problems currently faced by victims of cryptocurrency frauds looking to obtain information or documents from non-parties who are out of the jurisdiction and consider the effectiveness of the new gateway in addressing those challenges.

## Current problems in getting information from foreign non-parties

### The typical fraud

Although difficulties with identifying potential defendants and tracing assets are not unique to cryptocurrency fraud cases, the nature of crypto assets – and the anonymity associated with them - makes these problems more acute.

In a typical cryptocurrency fraud case, a fraudster induces the victim to buy cryptocurrency on the promise of high investment returns. The fraudster then persuades the claimant to grant access to their cryptocurrency wallet by providing the private key on the premise that they will manage the assets as an investment on the victim's behalf. At first, the fraudster impresses the victim by evidencing apparently lucrative returns, and on the strength of that apparent evidence, the victim is persuaded to transfer further funds for the alleged investment. Usually at the point when the victim seeks to make a withdrawal, he discovers that the fraudster has depleted the wallet and has disappeared with the funds.

1 As explained in the speech given by HHJ Pelling QC at the Crypto Disputes Conference, "Issues in Crypto Currency Fraud Claims", 29 June 2022 (https://www.judiciary.uk/announcements/speech-by-judge-mark-pelling-qc-issues-in-crypto-currency-fraud-claims/).

## The problems: who to sue, where to sue

Victims who turn to the law for assistance face serious obstacles since they may lack even the most basic information needed to bring a claim: identifying who to sue and where to sue them. All the victim may have to go on is the name of the fraudster's company, but they will likely soon discover that it is a sham entity or an empty shell if it exists at all. They might have an email or web address, but that alone is not enough to identify an individual. Nor does the victim have any means of knowing what has become of their investment.

A would-be claimant is therefore put in the position of obtaining the information they need from third parties. Who are those third parties likely to be? One of the most obvious targets for obtaining information are the cryptocurrency exchanges, such as Binance, Kraken or Coinbase, which administer or control accounts of users who trade through the exchange.[2] Another, less obvious, candidate might be individual software developers who maintain or develop the software on which cryptocurrency networks are based.[3]

What is the best way to get at this information where the relevant third-party refuses to volunteer it and is out of the jurisdiction? Absent their submission to the jurisdiction, or an applicable jurisdiction clause, the claimant will have to show that permission should be given to serve out in the normal way under the CPR.

## The traditional approach to information sought from non-parties abroad

Where a claimant is pursuing proceedings in England, English civil procedure furnishes them with a number of tools to obtain documents or information. For example, applications can be made for pre-action disclosure under CPR r.31.16 (against a prospective party to the proceedings, if there are likely to be substantive claims against them); r.31.17 (against a non-party); for Norwich Pharmacal Orders ("NPOs") (which have the advantage of allowing for the recovery of information as well as documents); and Bankers Trust Orders ("BTOs").

While these applications are comparatively straightforward to make against third parties in the UK, traditionally, the courts have been very circumspect about making information or disclosure orders against parties outside of the jurisdiction[4] – which crypto currency exchanges frequently are.

Broadly, that is because:

**a.** As a matter of policy, the courts have tended to refrain from asserting jurisdiction over foreign parties where there is no substantive cause of action against them.[5]

**b.** There is already an established international regime, in the form of the 1970 Hague Convention on Taking of Evidence Abroad, for obtaining evidence and documents from other jurisdictions.[6]

In the absence of assistance from the English court, the solution for a claimant is to turn to the local courts where the third party is domiciled or incorporated. However, this requires the instruction of an additional legal team, increases costs and slows matters down. Moreover, it will only be of assistance if the foreign jurisdiction provides equivalent relief at all.

However, there has been a notable shift in the English courts' approach to granting disclosure and information orders against foreign defendants in recent years, driven in part by a recognition by the judiciary of the need to tackle the particular problems which arise in cyber and cryptocurrency frauds. As Sir Geoffrey Vos MR remarked in a speech earlier this year, "[i]n the world of crypto fraud, there are no national barriers"[7]. Accordingly, a number of judgments have emerged in which the High Court has granted permission for service of various kinds of disclosure applications against non-parties out of the jurisdiction using the existing gateways.

The problem for claimants is that this shift in approach has not been universally adopted and the result is a patchwork of inconsistent decisions.

Take, for example, decisions under the following gateways:

**a)** Gateway (2) – "claims for an injunction ordering a defendant to do or refrain from doing an act within the jurisdiction". Permission was granted under this gateway for service out of an NPO in Bacon v Automattic Inc [2011] EWHC 1072 (QB) where US companies were ordered to disclose the names, addresses, IP addresses and other information that would identify the wrongdoer. More recently, however, Teare J criticised that decision in AB Bank Ltd v Abu Dhabi Commercial Bank PJSC [2016] EWHC 2082 (Comm) ("AB Bank") and indicated that the gateway was not engaged where the information sought could be provided anywhere in the world – so that there was no need for permission to serve out.[8] Subsequent authorities provide a mixed reception for Teare J's view.[9]

**b)** Gateway (20) – "a claim is made under an enactment which allowed proceedings to be brought and those proceedings are not covered by any of the other [gateways]": In

2 Exchanges have accordingly already been the subject of a number of disclosure applications: see for example, Fetch.AI Limited and another v. Persons Unknown (categories A, B and C) [2021] EWHC 2254 (Comm); Ion Sciences Ltd v Persons Unknown and others (unreported), 21 December 2020 (Commercial Court); and D'Aloia v Persons Unknown and others [2022] EWHC 1723.

3 In Tulip Trading Ltd v Bitcoin Association for BSV [2022] EWHC 667 (Ch), the claimants argued that the core developers of four networks were able to implement a software patch which would enable the claimant to regain control of cypto assets lost following a computer hack. The core developers did not appear to dispute the proposition that they could implement such a patch, which at least raises the question whether developers might have information that could shed light on the identity of the hackers or the location of misappropriated assets.

4 Dicey Rule 23 sets out that, outside the letter of request regime (discussed below), "the court has no power to compel a third party who is outside the United Kingdom to provide documents which are outside the United Kingdom". Dicey, Morris & Collins on the Conflict of Laws, 15th ed.

5 The Siskina [1979] AC 210; more recently reviewed in Broad Idea International v Convoy Collateral Ltd [2021] UKPC 24

6 Used to deploy the letters of request or letters rogatory regime, which is the only recognised exception to the general rule in Dicey Rule 23. This was an important reason why Cockerill J would have declined to exercise the court's jurisdiction to make a disclosure order even if she had held the court had jurisdiction in Nix v Emerdata Ltd [2022] EWHC 718 (Comm).

7 "Contracts, just smarter. Seizing the opportunity of smarter contracts", speech by Sir Geoffrey Vos MR to Lawtech UK, 24 February 2022: https://www.judiciary.uk/wp-content/uploads/2022/02/Speech-MR-to-Smarter-Contracts-Report-Launch-Lawtech-UK-UKJT-Blockchain-Smart-Contracts.pdf.

8 At [17]-[18]. At issue in AB Bank was a mandatory injunction requiring the defendant to provide information verified by a responsible officer

9 It was endorsed in Koza Ltd v Koza Altin Isletmeleri AS [2021] EWHC 2131 (Ch) at [126], but other cases have hinted that the place where documents are located may still be a relevant factor: see comments of Jacob J in Gorbachev v Guriev [2022] EWHC 1907 (Comm) at [108].

ED&F Man Capital Markets LLP v Obex Securities LLC [2017] EWHC 2965 (Ch) ("Obex"), it was held that an application for pre-action disclosure under CPR 31.16 and s.33 of the Senior Courts Act 1981 could come within gateway (20), the applications being "claims" and constituting the bringing of "proceedings". However, this jurisdiction should be treated cautiously in light of the recent, conflicting first instance decisions of Nix v Emerdata Ltd [2022] EWHC 718 (Comm) (where Cockerill J doubted whether Obex had been correctly decided) and Gorbachev v Guriev [2022] EWHC 1907 (Comm) (in which Jacobs J came to the opposite view in relation to an application under r.31.17).

**c)** Gateway (3) – where the party is a "necessary and proper party" to an existing claim. The authorities are unclear as to whether the third party would need to be a necessary and proper party to the existing cause(s) of action as pleaded against the anchor defendant. In AB Bank, Teare J appeared to decide that it was necessary to show that the same causes of action would be advanced against a Norwich Pharmacal defendant in order for the gateway to bite.[10] On the other hand, in Ion Science Butcher J refused to apply Teare J's reasoning in AB Bank to a BTO (without expressly determining whether AB Bank was correctly decided). Instead, he distinguished AB Bank on the basis that it was applied to Norwich Pharmacal relief rather than BTO relief (which was the instant application before him), and that in any event there was power to grant permission for service out of a BTO where there was "hot pursuit", in reliance on Mackinnon v Donaldson, Lufkin and Jenrette Securities Corporation and Others [1986] 2 W.L.R. 453.[11] In Fetch.ai Ltd v Persons Unknown and others [2022] EWHC 2254 (Comm), HHJ Pelling QC recognised the apparent conflict between the approach to NPOs and BTOs in AB Bank and Ion Science but did not seek to resolve it, proceeding instead on the basis that the court had jurisdiction to grant permission for service out of a BTO order but not an NPO.[12]

These cases show that a conflicting body of authority had developed as to whether, when and how an English court will intervene to order a foreign non-party to provide information or documents in support of English proceedings.

## The new gateway 25

The new gateway seeks to address these issues by providing an express basis on which permission to serve disclosure or information applications out of the jurisdiction may be granted. It provides that permission may be granted where:

### Information orders against non-parties

(25) 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.

Accordingly, it appears the gateway will be available:

**a)** For pre-action applications as well as applications after the issue of substantive proceedings where proceedings have been or will be commenced in the jurisdiction;

**b)** In a range of applications (or "claims"), which should include NPOs and BTOs, although there is nothing in the wording to suggest that the gateway is limited to these types of application; and

**c)** Specifically against non-parties, marking an express departure from the traditional position that injunctions against foreign non-parties was an affront to the sovereignty of the foreign state.

Of course, the fact that a gateway for these applications is now clearly available does not obviate the need for claimants to show:

**a)** That in any case an NPO, BTO or other order should be made. An NPO, for example, requires the threshold conditions in Mitsui & Co Ltd v Nexen Petroleum UK Ltd[13] to be satisfied in addition to a discretionary test; and

**b)** That the requirements for service out are all met, namely a serious issue on the merits, a good arguable case in relation to the relevant gateway(s) and that England is the appropriate place to try the claim.[14] However, the case law indicates that these requirements will not be difficult to surmount in a typical cryptocurrency fraud claim.

To take advantage of the gateway it appears that it will also be necessary for a claimant without ongoing proceedings in England to show a good arguable case that the English court will have jurisdiction over the substance of the matter – paragraph (b) of the gateway. The exact meaning of the words 'subject to the content of the information received' in this paragraph are not entirely clear. Presumably the intention is to show that a claimant is not bound to bring proceedings in England, if for example, information received pursuant to the application discloses another available forum which would be more advantageous or appropriate. For example, where the information discloses the domicile of the eventual defendant to the claim.

10 At [19]. In so doing, he expressly departed from earlier authority which held that the gateway was engaged where the information provided by a respondent to an NPO would lead to the identification of the defendants: Lockton Companies International and others v Persons Unknown and Google [2009] EWHC 3423 (QB).

11 A case which incidentally did not concern service out of the jurisdiction at all but dealt with the court's subject matter jurisdiction to make an order which although properly served on a defendant in the jurisdiction would require the defendant to produce the documents from outside of the jurisdiction through a foreign branch

12 At [30]. A similar approach was taken by Trower J in D'Aloia v Persons Unknown and others [2022] EWHC 1723 and Danisz v Persons Unknown and Huobi Global Ltd [2022] EWHC 280 (QB), where Ion Science was followed in relation to service out of a BTO against a cryptocurreny exchange

13 [2005] EWHC 625 (Ch) at [21], namely: (i) a wrong by an ultimate wrongdoer, (ii) the NPO is necessary to enable an action to be brought against the ultimate wrongdoer and (iii) the NPO defendant must have been "mixed up" in so as to have facilitated the wrongdoing and be able or likely to be able to provide the information necessary to enable the ultimate wrongdoer to be sued

14 Per the requirements in VTB Capital v Nutritek International Corp & Ors [2012] EWCA Civ 808 at [99]-[101].

## How much further is the new gateway likely to get claimants?

Undoubtedly gateway 25 brings advantages. It resolves the uncertainty created by recent, inconsistent authorities as to when disclosure or information orders could be served out. In this way, it will help to prevent genuine claims being stifled at the outset by technical jurisdictional rules.

However, we think there are at least three points that claimants should bear in mind.

First, as the case law develops it will be interesting to see how the court addresses the question of the appropriate forum for the granting of relief i.e. the third limb of the test for permission for service out. Will the court simply take the approach that where it is has determined it has jurisdiction over the substance of the matter, it is also the most appropriate forum to grant interim disclosure relief? Will it take a more nuanced approach considering factors such as the availability of an alternative forum, the enforceability of any order and the English court's ability to compel compliance? Where the same or equivalent relief is not available in the respondent's home jurisdiction does that automatically make England the most appropriate forum? The recent case law concerning the service out of BTOs has largely not dealt with the question of appropriate forum and appears to have taken the former approach although no doubt the position would be approached differently in a fully contested application.

Second, the new gateway is not a panacea for the problems faced by victims of cyber or cryptocurrency frauds. After all, even if a claimant has an NPO or BTO, what happens if the third party simply refuses to comply? Can they be compelled to produce information? This will depend on the local enforcement regime, although it is typically very difficult to enforce an interim or non-money judgment in the absence of a mutual recognition and enforcement treaty. If the order cannot be enforced, claimants may need to consider whether the foreign courts can be looked to for equivalent relief. Helpfully, NPOs in support of foreign proceedings are now available in the BVI[15] and the Cayman Islands.[16] There is also judicial support for the existence of the jurisdiction in Jersey[17], Guernsey[18], and the Isle of Man.[19] The US also provides a similar regime.[20]

Third, consider the limitations of the scope of the new gateway 25. It applies only to applications seeking information as to the identity of a defendant (so that a claim may be brought against them) or seeking information as to what has become of property (so that it may be traced). Broader disclosure applications will not come within the gateway and thus will either need to progress through the established regime for letters of request (which can be slow and technically cumbersome) or via the less certain route of service out of applications under CPR r.31.16 / s.33 SCA 1981. It is notable that the Civil Procedure Rules Committee rejected the introduction of a broader gateway allowing service of applications on non-parties to the litigation at the same time as they were considering gateway 25.[21]

In any case, the new gateway 25 is a welcome signal from the English courts that in the borderless world of cryptocurrency, it will not allow fraudsters to exploit the difficulties associated with international litigation to their advantage.

15 See, for example, K&S v Z&Z BVIHCM(COM) 2020/0016. The law has now been put on a statutory footing under s.3(5) of the Eastern Caribbean Supreme Court (Virgin Islands) (Amendment) Act 2020

16 See, for example, Essar Global Fund Ltd and Essar Capital Limited v Arcelormittal USA LLC (CICA, unreported, 3 May 2021).

17 See New Media Holding Company LLC v Capita Fiduciary Group Limited [2010 JLR 272]

18 See Equatorial Guinea (President) v Royal Bank of Scotland International & Ors (Guernsey) [2006] UKPC 7 (27 February 2006).

19 See Templeton v Bradford & Bingley (ORD 2010/93 Judgment of Deemster Corlett) 21 January 2011

20 Under section 1782 of Title 28 United States Code

21 See the Minutes of the Civil Procedure Rule Committee: Annual Open Meeting, 13 May 2022, paragraph 69