TWENTY ESSEX

At last! A new jurisdictional gateway permitting service of third-party disclosure orders out of the jurisdiction

Paul Lowenstein KC and Sam Goodman

Paul Lowenstein KC and Sam Goodman discuss their role in developing new disclosure gateway 25 and what this means for international fraud litigation.

The Courts in England and Wales are rightly seen as the gold-standard jurisdiction for complex, international fraud and asset-tracing litigation. However, for a while now, fraudsters engaged in rapid cross-border cyber and money transfer frauds have been outpacing developments in the legal system, making the process of tracing, securing and enforcing against assets difficult and expensive, and sometimes impossible.

The difficulty in most international transfer fraud cases is that the victim does not know what has happened to their assets (be they money, crypto or something else), or who received them and what has subsequently become of them. The fraudsters operate under the cloak of secrecy afforded by digital systems and very often the only clue as to what has become of the assets are faint traces on a pseudonymous blockchain. There may sometimes be a hint of who has taken them in an IP address or an anonymous email account.

It is frequently possible, with the help of experts, to conduct some form of tracing exercise which will generally reveal basic information, such as (1) that the assets have been divided into small parcels and transferred across the World, before being "cashed-out" at banks or cryptocurrency intermediaries such as exchanges and/or (2) that a particular email address used in the fraud is associated with an accountholder at a particular bank or exchange and/or (3) perhaps that a company implicated in the fraud, almost inevitably established in an offshore jurisdiction with well-developed secrecy laws, was set up and managed by a particular corporate services agent.

At that stage, if they are to obtain any form of effective redress, the victim requires (1) disclosure (2) from the relevant intermediary bank, exchange, financial institution, corporate services agent or otherwise (3) of the information/records/documentation held by the intermediary regarding the accountholder or customer implicated in/connected to the fraud by the basic information. For example, they will likely hold Know-Your-Client (KYC) and Anti-Money Laundering (AML) documentation containing information about the true identity of the fraudster and details of their address, passport, utility bills and of other linked accounts or wallets.

When this sort of information is held by a party within England and Wales, there is usually no problem satisfying the English Court that it should exercise its substantive jurisdiction to make a disclosure order against an innocent third-party bank, financial institution, exchange, financial institution, or corporate services agent likely to hold information that could assist in unravelling the fraud. There are a number of well-established jurisdictions for such an order, such as Norwich Pharmacal, Bankers Trust and CPR 25.1.g.

The difficulty has always been when there is an international element to the transfer fraud, since the target for disclosure will almost inevitably be

located outside England and Wales. This in turn gives rise to questions concerning the Court's *territorial* jurisdiction because the Court is therefore being asked to make an order against an innocent party located abroad. In practice, these issues arise in almost every transfer fraud case in which we have been involved.

For some time, there has been great uncertainty about which, if any, of the CPR Practice Direction 6B jurisdictional gateways for service out could apply to an application for disclosure from an overseas respondent. The position became more difficult for victims of international transfer fraud following *AB Bank Limited v Abu Dhabi Commercial Bank* [2016] EWHC 2082 (Comm) which decided that certain of the jurisdictional gateways which might allow an order for service out of an international *Norwich Pharmacal* disclosure application (such as the 'necessary or proper party' gateway) could not in fact be used. Whilst (with respect to the Judge) we consider *AB Bank* was wrongly decided, first instance judges subsequently dealing with *ex parte* applications for international *Norwich Pharmacal* disclosure have understandably considered themselves to be bound by it.

We therefore, in stages, developed a solution, persuading the Court (1) that the *AB Bank* obstacle could be confined to the applications made under the *Norwich Pharmacal* jurisdiction (2) that the *Bankers Trust* jurisdiction (which only applies where the Claimant has a proprietary claim) is different in nature, because the Court acts to safeguard trust property and is ordering disclosure in respect of the very same property that is the subject of the substantive claim (3) that the CPR Part 25.1(g) jurisdiction, also being ancillary to a main claim, equally escaped the *AB Bank* restriction. Most importantly, with regard to the proprietary jurisdiction, we argued that for jurisdictional/service out purposes, a respondent to a *Bankers Trust* application could properly be described as a "necessary or proper party" within the meaning of gateway 3.1(3) and (4) that the relevant anchor claimant for jurisdictional purposes could be 'Persons Unknown'.

Thus, in circumstances in which: (1) the matter is urgent (2) there are no realistic alternatives for the victim and (3) the relevant property was originally located in England (such that this jurisdiction can be described as the *forum conveniens*), we have persuaded the Court that it can and should make an extraterritorial order relying on gateway 3.1(3): see *CMOC v Persons Unknown* [2017] EWHC 3599 for the first example of a money case and *Ion Science Ltd v Persons Unknown* (unreported) 21 December 2020 (Commercial Court), the first application in a crypto claim.

However, whilst this workaround was successful in a number of cases, it had several drawbacks. First, it required a Claimant to initially issue a claim against Persons Unknown so that there was a relevant anchor defendant for jurisdictional purposes. This necessitated the payment of a large court fee before the victim knew if they were going to get any useful information about the real identity of the fraudster. Second, in the crypto sphere, *Ion Science* and the cases which have followed it were decided *ex parte*. Since this means that these decisions have no precedential value it has been necessary in every case to spend significant time (and therefore cost) preparing to persuade judges from first principle that such disclosure orders can be served out of the jurisdiction. Third, the only victims which it helped were those with a proprietary claim. This excluded many claimants who did not have a proprietary claim but who nevertheless had suffered loss through transfer fraud committed by anonymous wrongdoers.

After discussions following Sam's talk at the launch of 'CFAAR' (the Cryptocurrency Fraud and Asset Recovery network) about some of these problems and the threat they posed to this jurisdiction's status as the premier forum for litigating fraud disputes, Sir Geoffrey Vos, MR, invited us to join a sub-committee of the Civil Procedure Rules Committee that had been established to consider revisions to the jurisdictional gateways. We were asked to consider and, if we felt appropriate, to propose a new disclosure gateway for that committee to review. We proposed an entirely new disclosure gateway, and both the sub-committee and the main Civil Procedure Rules Committee agreed. The resulting sub-committee report, containing our draft gateway, can be found in Annex A - CPRC Service Sub-Committee Paper. Other gateway changes have been made. These are discussed by our colleagues Charles Kimmins KC and Josh Folkard in their commentary, found here.

The text of new gateway 25 – which comes into force on 1 October 2022 as CPR PD 6B Para 3.1(25) – reads as follows:

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) the claim or application is made 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 rule 6.32, 6.33 or 6.36.

It is worth emphasising three points. The first is that the gateway is not strictly limited to the service out of applications

aimed at uncovering what has become of property. It is extends to applications to uncover the identity of a "defendant or potential defendant". Thus, whilst not all *Norwich Pharmacal* applications will be able to pass through the gateway, at least one core basis for seeking Norwich Pharmacal relief (to find out who has wronged the victim) will do so. Second, the drafting ensures that the Court will only grant relief where the proceedings or intended proceedings have been/ are to be commenced in England and Wales (whether by service here or by service abroad with permission). This prevents the gateway from being used as a 'springboard' by victims wishing to use the English court to obtain information for litigation proceeding abroad. Third, although the genesis for this new gateway was our experience of cyber-fraud cases, in fact there is no requirement for a cyber-fraud to have occurred, or indeed for any fraud to have occurred.

One question which is often raised in relation to extra-territorial disclosure orders is whether they will be effective. Why should any bank, exchange, financial institution or corporate services agent in another jurisdiction comply with them? This is where London's position as a global financial centre makes all the difference. Firstly, such orders are frequently registered or recognised, where necessary, by the local court of the foreign respondent. Secondly, it is often not necessary to expend the cost of registration/recognition, because a respondent disobeying an English disclosure order may become exposed to the risk of imprisonment, fine or asset seizure should they or their directors move assets or travel into England. Thirdly, such a respondent will also suffer the public reputational consequences of having committed a contempt of court in England. So, whilst compliance cannot be guaranteed, we expect that orders which pass through the new gateway are likely to be taken seriously. Certainly, our experience is that orders made using the *CMOC / Ion Science* method were generally – although not universally – complied with.

We consider that new gateway 25 cements this jurisdiction's reputation as the leading forum for international fraud litigation. We have already been instructed to make applications for service out of disclosure orders using this new rule and we look forward to developing the principles surrounding the Court's exercise of its new jurisdiction. As ever, there remain important issues to be resolved by Judges. Examples include: (1) the proper form of such disclosure orders (2) whether, in a non-urgent case, the Court will agree to make both the order for permission to serve out and the order for immediate disclosure at the same time, or if it will require the respondent to be served first with an 'in principle' order, but to delay the production of documents until after an on-notice hearing and (3) the introduction and refinement of safeguards for an innocent disclosure respondent which is called on to provide information about their customer/client who appears to have defrauded the victim.

As developed in the CMOC litigation, such safeguards in the disclosure order might (a) stipulate an early on-notice return date (if required) or (b) include exceptions to clarify that the foreign respondent is not required to do anything that is either illegal under its local law and/or which contravenes its contractual relationship with its customer/client or (c) require the respondent to gather the information immediately but not to disclose it until after they have had a chance to be heard at an on-notice return date.

In the meantime, we are confident that new gateway 25 has and will make life easier for the victims of fraud to obtain meaningful redress.

This article does not constitute, and should not be relied upon as, legal advice. The views and opinions expressed in this article are those of the authors and do not necessarily reflect the position of other members of Twenty Essex.

Paul Lowenstein KC

Paul is a leading commercial silk in domestic and international litigation and arbitration. A highly experienced courtroom advocate, he has expertise in high-profile, heavy, and sensitive commercial, civil fraud, financial, and international disputes of all kinds.

Read his online bio ›

Sam Goodman

Sam specialises in complex, high-value commercial litigation and arbitration. Sam has a particularly strong civil fraud & asset recovery practice, having been instructed in several multibillion dollar international fraud disputes over the last couple of years.

Read his online bio ›