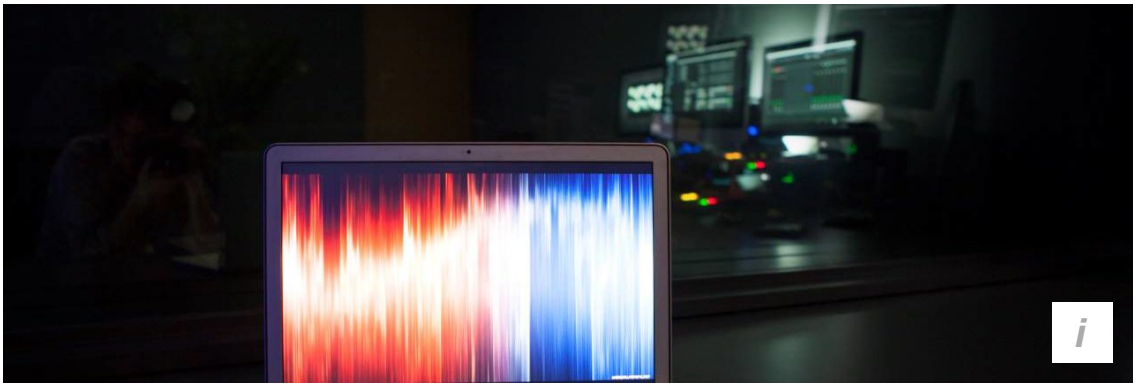
PRACTICAL LAW
DISPUTE RESOLUTION BLOG



FEBRUARY 11, 2020

Asset recovery in cyber fraud cases

Cyber fraud is big business for criminals. It is everywhere. Readers will have been reminded by their banks to be on the lookout for such fraud frequently in the recent past. Cases where the victims of such frauds seek to recover their misappropriated money are becoming increasingly common in the English courts. But the legal remedies in relation to cyber fraud have only developed in the last year or two, and are still not widely understood. In this blog, I share my experience and tips gleaned from obtaining a number of *injunctions* and related orders in recent cyber fraud cases.

by **Philip Hinks**
at 3 Verulam Buildings

Typical cyber fraud attacks

The cyber fraud cases in which I have recently acted typically start with a "business email compromise attack". Anonymous fraudsters succeed in hacking into an email account, and begin sending emails which appear to come from the real account holder. Sometimes, the compromised account will belong to the client, often to one of its senior executives with authority for making payment transfers on the client's behalf. The fraudsters will then proceed to generate a series of fraudulent payment instructions directing transfers to be made to various banks accounts around the world. If those instructions are accepted by the client's bank (a matter which depends on the sophistication of the security systems in place between the client and its bank), the fraud will be perfected, and funds will be paid to bank accounts that have no bona fide connection with the client.

This was the case in *CMOC Sales & Marketing Ltd v Persons Unknown*, in which I acted for CMOC. The email account that was hacked belonged to one of the client's directors, Mr Chen, who was also an authorised signatory to its banking facilities. Over the course of a number of days, fraudsters impersonating Mr Chen sent payment instructions to CMOC's bank. Those instructions were acted upon and transfers totaling approximately US $10 million were made.

In other cases, however, the business email compromise attack is made on a third party, such as one of the client's suppliers. There, the client will receive an email that appears to have come from a regular supply contact, often requesting that payment of a recently rendered invoice be made to a different bank account, perhaps referring to an internal reorganisation to explain the change in banking provider. If that request is accepted (a matter which similarly depends on the security systems applied in the client's payment processes), the fraud will be perfected and funds will be paid to an account having no connection with the supplier.

To remain undetected whilst the fraud is being carried out, the hackers will sometimes change inbox account rules or change the reply-to addresses. As a result, responses querying the payment instructions will be directed to the fraudsters rather than the genuine email accountholders. In CMOC, when finance employees sent emails to Mr Chen querying why substantial sums were being paid to entities with which the company had had no business dealings, the fraudsters responded giving fake, but more or less rational, explanations for the transfers.

Putting the bank on notice?

When a cyber fraud is first discovered, the information available to the victim will be extremely limited, and will typically consist of the account number, sort code and account holder name (which may deliberately resemble the actual supplier). Investigations into email addresses as a means of tracking down the individuals behind the emails are unlikely to assist, as it is common and not difficult to "spoof" an email address (making an email appear to have come from an address other than the actual sender's email address).

The knee-jerk reaction of the victim of a cyber fraud attack is to give notice of the fraud to the banks that have received the proceeds. Receiving banks will be requested to freeze the accounts in question, and to provide information concerning the account holders to the victims. But they have no obligation to do so.

Experience shows that most banks (particularly those located in the UK) that receive notice of a cyber fraud will take steps to prevent further use of the accounts in question for a short period of time whilst investigations are carried out, and will not bring the victim's communication to the account holder's attention, although there remains a risk of tipping off as the bank owes contractual (and possibly statutory) obligations to their account holders that may include the notification of interferences like this. Further, it is highly unlikely that a receiving bank will provide the victim with any information about the accounts that have been credited with the proceeds of the fraud, or the holders of those accounts, until *served* with a *disclosure* order.

Notice to the bank is therefore no real substitute for a disclosure or *freezing order* against the bank.

Disclosure orders under the Norwich Pharmacal and Bankers Trust jurisdictions

The first application that the victim of a cyber fraud attack will probably need to make is for disclosure against the receiving banks (as no cause of action respondents) pursuant to the *Norwich Pharmacal* or *Bankers Trust* jurisdictions. The first of these allows the court to make disclosure orders against innocent third parties who have become mixed up in a wrong; here, against the bank whose accounts have been used to facilitate the fraud. The second allows the making of disclosure orders in support of proprietary claims. Subject to governing law issues, the victim of a cyber fraud may be able to assert such a claim in respect of the stolen funds: *CMOC* at paragraph 77.

An application for disclosure against the banks can usually be justifiably made without notice to the banks (and, therefore, at speed) because of the risk that if notice were given, they would be obliged to bring that interference to the account holders' attention. For the same reason, the application should ideally seek a non-disclosure (or "gagging") order against the banks, preventing them from communicating with the account holders for a period of time. Regard should be had to the Practice Guidance on Non-Disclosure Orders [2012] 1 WLR 1003 and, in particular, the requirement that they be put in place for no longer than is strictly necessary. A formulation should be arrived at in the order sought to avoid there being a return date of the disclosure order (in circumstances where disclosure is to be provided within 24/48 hours), while at the same time permitting the banks to apply to vary or *set aside* the order on short notice.

When disclosure is received from these banks, and as further investigations and other applications are made by the victim, it may become necessary to extend the non-disclosure relief to other banks or recipients. Experience shows that the proceeds of a cyber fraud will often be paid on through a series of other accounts shortly after they were credited to the immediate receiving accounts. It may, therefore, be the case that in chasing the money around the world, several rounds of disclosure from several tiers of receiving banks are required before funds or non-bank recipients are located/identified at the end of the money flow tree. In *CMOC*, disclosure orders against three tiers of recipients were obtained before substantial funds were identified; in other cases that I've acted in, traceable proceeds have been identified after fewer rounds of disclosure.

Where subsequent disclosure orders are required in short order, it is preferable (if circumstances allow) for those applications to be listed before the same judge who granted the initial relief. In those cases, the relief sought is the logical continuation of the asset tracing exercise that has already been put in motion, and later hearings are typically shorter and less contentious. In *CMOC*, there were a total of 14 hearings and seven paper applications in the nine months between the discovery of the fraud and *trial*, many of which were determined by Waksman J, who granted the initial injunctive relief.

Overseas banks

It is often the case that the proceeds of the fraud will have been credited to accounts with banks located outside England and Wales. This presents two substantial obstacles for the victim.

First, where the receiving bank must be *served outside* the jurisdiction (that is, where the bank has no English branch at which service may be effected), the only available jurisdictional gateway for the service out of a claim for Norwich Pharmacal disclosure is the "necessary or proper party" ground in *Practice Direction 6B.3.1(3)*: *AB Bank v Abu Dhabi Commercial Bank*. Hence, a prima facie case will need to be made out as to why the receiving banks are necessary or proper parties to the victim's claim. In *CMOC*, all of the receiving banks against which disclosure orders were obtained were located outside the jurisdiction.

Second, most overseas banks will, understandably, refuse to comply with an English disclosure order unless and until that order is recognised, or similar relief is obtained, in their local jurisdiction. The form of order sought should include carve-outs permitting non-compliance by banks located outside the jurisdiction, where to do so would amount to a contravention of local laws. Care should therefore be taken to ensure that the *cross-undertakings* offered by the victim to the court do not (as is standard in applications for freezing order relief) place restrictions on the taking of steps to enforce the order overseas, and to ensure that local counsel are engaged to act swiftly when the English disclosure order is granted.

Freezing orders against cyber fraudsters and other fund recipients

In addition to finding out where the stolen funds have gone and who is behind the bank accounts that received those funds, what can the victim do to ensure that whatever's left of the proceeds is effectively frozen?

As discussed above, the mere giving of notice of the fraud to the receiving banks may cause them to impose internal restrictions on future dealings with affected accounts. However, the victim will have limited visibility on, and no control over, such restrictions, which may well be temporary in any event. When all is said and done, a disclosure order is no substitute for a freezing order.

Following *CMOC*, it is now established that *worldwide freezing orders* and (if a proprietary claim is available) proprietary injunctions may be ordered against cyber fraudsters, notwithstanding that their identities are currently unknown to the victim. The important consideration here is to ensure that the description given for the persons unknown is sufficiently certain to allow assessments to be made in due course as to whether someone falls within the class (and is therefore subject to the injunction) or outside of it, and for the persons themselves to know. In many cases, that description will take its flavour from the receiving accounts about which some information is already known, for example, persons unknown (being the holder(s) and authorised signatory(ies) to the account held at XYZ Bank with IBAN number 123). In *Cameron v Liverpool Victoria Insurance Co Ltd*, the Supreme Court observed that there has been a significant increase in the "persons unknown" jurisdiction in recent times, with the main contexts for its exercise being "abuse of the internet, that powerful tool for anonymous wrongdoing; and trespasses and other torts committed by protesters, demonstrators and paparazzi" (at paragraph 11).

Service on cyber fraudsters and other fund recipients

But how does one serve the persons unknown?

It will almost always be the case that an order for *alternative service* is required under *CPR 6.15* or *6.37(5)(b)(i)*. A "good reason" to allow such service to take place will not be difficult to find; the overarching consideration being the victim's inability to effect proper service in accordance with the CPR. But where to serve? In cyber fraud cases, the only realistic solution will often be service on the fraudsters at the banks that received the proceeds of the fraud, with those banks being invited (albeit not compelled) to pass the same to the account holders. That method was approved by the court in *CMOC*, and has since been adopted in other cyber fraud cases in which I have appeared.

As and when disclosure is received from the banks, the victim will have access to all manner of KYC information gathered by the banks concerning the account holders, including physical addresses, email addresses and telephone numbers. One can at that stage seek to shore up the position on service by more conventional methods, as well as use that information to seek to identify further assets and information about the fraudsters.