In hot pursuit

The use of flexible remedies and procedures to combat fraud

Paul Lowenstein QC and Matthew McGhee, Barristers, 20 Essex Street

In Summer 2018, the Lord Chancellor announced that a new flagship court would be opening in London and be specifically designed to tackle fraud, cybercrime and economic crime. Plans for its opening are underway and it is hoped that the court will be in full service by 2025. Judging by current trends, the new court will be very busy from day one.

Reliable estimates of the prevalence of fraud, especially cyber-fraud, are difficult to assess. What is clear, however, is that such activity is increasing. Earlier this year, for example, Santander announced that it closes 24,000 UK bank accounts per year on suspicion of fraud, of which about 11,000 are suspected of being operated as 'money mule' accounts – ie. operated by fraudsters (who may or may not be the account holder) to conduct illegal activities such as money laundering.

The problem is not just with Santander. Nationwide closes about 12,000 bank accounts per year for similar reasons, of which about 6,000 are suspected 'money mule' accounts. Facebook has also recently taken steps to remove adverts from its platform where fraudsters were offering its users £1,200 in exchange for those users allowing their accounts to be operated as 'money mule' accounts.

In such times, lawyers and judges must recognise the need for the law to respond appropriately. There is no need to reinvent the wheel; well-established processes and remedies can be adapted and applied to the new challenges. In this update, we provide a brief overview of some of the ways in which this has been achieved in recent months.

Development of the 'persons unknown' jurisdiction

In *CMOC v Persons Unknown* [2018] EWHC 2230 (Comm), the High Court confirmed that it has jurisdiction to make worldwide freezing orders against persons unknown. In the case of a cyber-fraud, this enables a victim to freeze the accounts to which sums were sent in the course of the fraud even if the victim does not (yet) know the identity of the account holder.

There is similarly a growing body of cases where *American Cynamid* injunctions are granted against persons unknown who have been involved in gaining unauthorised access to claimant parties' IT systems. Threats are often made to disclose commercially sensitive data unless a ransom payment is made. See *PML v Person(s) Unknown* [2018] EWHC 838 (QB) and *Clarkson Plc v Person or Persons Unknown* [2018] EWHC 417 (QB). In such cases, the respondents are routinely ordered to not disclose the data, and may additionally or alternatively be asked to destroy any copies of the data that they have made (*cf. Bloomsbury Publishing v News Group Newspapers* [2003] 1 WLR 1633).

'Spartacus' (or self-identification) orders may also be made in such instances. A 'Spartacus' order requires the unnamed respondent is ordered to identify him or herself to the Court. Although such 'Spartacus' orders may not be complied with, the threat of contempt proceedings should the respondents later be unveiled may act as a spur to prompt compliance of some individuals.

However, helpful as the 'persons unknown' jurisdiction is, it should not be seen as a magic panacea for any difficulty in identifying the parties to a fraud. In *Cameron v Liverpool Victoria Insurance* [2019] UKSC 6, the Supreme Court explained that there are two kinds of unnameable defendants: defendants who were identifiable but whose names were unknown; and defendants who were anonymous and could not be identified. Claims can only be made against 'persons unknown' in the first category, not the second. The first category covers the defendants/respondents in *PML, Clarkson & CMOC*, where it was plain that there was a conspirator or body of conspirators operating from certain email addresses or bank accounts, but the actual identities were unknown. The second category would include (in the case of *Cameron*) the unknown hit-and-run driver, but also other defendants who are not only anonymous but are also unidentifiable. It seems that the distinction may be between 'persons unknown' who can or cannot be served, whether that be directly or by alternate means.

Facilitate and support investigations

The courts have also shown a willingness to facilitate and support fraud investigations, both by specific orders but also through a general preparedness to apply their procedural powers in a flexible but principled manner.

In facilitating investigations into fraud, the High Court in *CMOC* (*cf.* [2017] EWHC 3599 (Comm)) confirmed that it would make disclosure orders against international banks in foreign jurisdictions to require those banks to provide information about their clients, the holders of the accounts which received the stolen funds, so as to facilitate the fraud investigation and asset tracing exercise. This is an important step forward in facilitating international fraud investigations, given that the decision in *AB Bank v Abu Dhabi Commercial Bank* [2016] EWHC 2082 (Comm) effectively prohibits a victim of fraud from seeking Norwich Pharmacal relief against parties outside of the jurisdiction.

Although it was a case of breach of confidence, not fraud, *Hyperama v Poulis* [2018] EWHC 3483 (QB) is a useful reminder to parties of another investigative tool – the so-called 'doorstep delivery-up' order, a less-Draconian form of search order. The key difference is that the applicant is not entitled to conduct the search him or herself (by their lawyers), but rather attends (without entering) the respondent's property unannounced to demand immediate delivery-up of documents or other evidence. The Judge in *Hyperama* conducted a succinct review of doorstep delivery-up orders and confirmed that an *"elevated standard of whether [the court has] a high degree of assurance that [the applicant] will be able to establish its claims at trial"* applies in doorstep delivery-up orders, albeit that this is a slightly lesser standard than required for a search order (ie. *"extremely strong prima facie case"*).

The courts have shown willingness to develop the procedural flexibility necessary to deal with cyber-fraud cases in a proportionate manner. For example, a final injunction against a cyber-blackmailer has been made without a hearing where it was clear that nobody would appear at court to contest the application: *Clarkson*. The authors are also aware that, in ongoing cyber-fraud investigations, the Court has been willing to consider return dates (and even initial *ex parte* applications) for freezing orders as paper applications. In *CMOC*, the judge permitted service by Facebook Messenger, WhatsApp

Paul Lowenstein QC

messenger and by access to a data room, among other means, commenting that *"the court will consider proactively different forms of alternative service where they can be justified in the particular case."*

Post-judgment freezing orders

A post-judgment freezing order is a powerful tool to assist in enforcement – particularly where a claimant needs to enforce its judgment abroad and the English Court can be persuaded to grant a worldwide freezing order.

In *Michael Wilson v Emmott* [2019] EWCA Civ 219, the Court of Appeal recently confirmed that post-judgment freezing orders can be more readily granted than pre-judgment freezing orders – indeed, a post-judgment freezing order may be granted irrespective of whether an earlier application for a freezing order was made. In *Michael Wilson*, the applicant sought to remove the wording in the standard form freezing order which permits the respondent to use the frozen assets for transactions in the *"ordinary course of business"*. The Court explained that there is no presumption that this exception be removed in a post-judgment freezing order, but that its removal was equally not a remedy of last resort. In *Michael Wilson*, the Court of Appeal agreed to exclude that exception on the basis that the respondent's conduct demonstrated that it was attempting to avoid paying the judgment debt, not that the respondent was unable to do so.

Conclusion

The courts are ready to engage with victim claimants to assist them in seeking recourse against the perpetrators of fraud. There is a broad array of possible remedies and procedures available, and judges have shown a willingness to adapt existing tools to meet new challenges. Critically for litigants, it is important to build the trust of the Court.

This means that litigants should be frank when seeking to expand existing doctrine or to extend a remedy into a difficult area. It also means being scrupulous in ensuring proper compliance with procedural requirements – including in respect of full and frank disclosure. There have been several high-profile recent cases (eg. *Punjab National Bank v Srinivasan* [2019] UKHC 89 (Ch)) where freezing and other orders have been set aside for material non-disclosure. This can result in otherwise-valid relief being refused, adverse costs orders being made and often the entire litigation derailed.

In the context of cyber-fraud, particularly cases where defendants/respondents may not engage with proceedings, proper compliance with procedure has an additional incentive – future enforcement. It would be a pyrrhic victory for a claimant to obtain an English judgment on a cyber-fraud case, but when seeking to enforce that judgment against the foreign-domiciled fraudster the local courts refuse to enforce the judgment on the basis that the claimant failed to follow proper procedure to the prejudice of the fraudster.

A final note on Brexit: At time of writing, there is no certainty as to the outcome of the UK's negotiations to exit the EU. As it stands, there is therefore no certainty as to how UK judgments and orders may be enforced abroad in EU jurisdictions. It is likely that some form of mutual recognition will be granted between UK jurisdictions and EU jurisdictions, but at the time of writing parties must work on the basis that they will lose the benefits of the Recast Brussels Regulations. This may pose its own challenges to cross-border enforcement, particularly in cases of cyber-fraud where speedy domestication abroad is often essential if the locally-obtained relief (eg. freezing orders) is to be effective.

Matthew McGhee