haynesboone

December 31, 2018

Chasing Down the Cyber-Criminals: A Lesson in Innovation

By Ryan Deane

Introduction

Cybercrime is a growing concern for many companies. Major stories about hacked systems or compromised data proliferate the news. Electronic fraud is steadily on the rise. Fortunately, the English courts are demonstrating a willingness to innovate in this area. A good example of how the courts are expanding their armoury to combat these modern challenges is the recent case of *CMOC Sales & Marketing Ltd* v *Persons Unknown and 30 others* [2018] EWHC 2230, which answers the question: how do you pursue defendants in legal proceedings if you don't know who they are?

Background

The claimant ("CMOC") is an English company which buys and sells Nobium, a soft metal predominantly found in Brazil and used in alloys such as special steel and gas pipelines. In October 2017 CMOC discovered that it was the victim of a business email compromise fraud, whereby the perpetrators of the fraud had hacked into its email system and instructed its bank, Bank of China in London, to pay US$6.91 million and €1.27 million to various bank accounts around the world.

The director whose email account was hacked was called Mr Chen. Once the hackers had taken control of the account the fraud was straightforward. The fraudsters looked through Mr Chen's old emails to find a payment instruction to the bank, and fabricated a new instruction which was identical in all material aspects save for the payees' account details and the transferred amounts.

The fraudsters set up certain 'rules' in Mr Chen's email account which diverted emails to a separate account controlled by the fraudsters for screening before being released for Mr Chen to view. This meant that when the accounts department of the company emailed Mr Chen to query the transactions, the email never reached him, and the reassuring reply the accounts department thought was from Mr Chen was actually from the fraudsters.

The emails purporting to come from Mr Chen were all the more believable since they appeared to be copied to other officers of CMOC. In fact, they were not. The fraudsters had created dummy email addresses similar to the officers' actual email addresses, but slightly misspelt, so that one would only notice the difference if actively looking for it. Run your eye over "@cmocinternational.com" and "@cmocintermational.com" to see if you would have noticed anything suspicious.

Highlighting the value of occasionally picking up the phone, someone eventually called Mr Chen to discuss the irregularities, whereupon the fraud unravelled. Mr Chen called the bank and told them to cease all payments, only barely stopping a fraudulent payment of US$3.2 million from being processed.

The stolen funds had been dispersed into a large number of accounts worldwide. To give an idea of the scale of the dispersal, a payment of €1.13 million into one bank account was subsequently transferred into 12 other bank accounts. The amount in one of those 12 bank accounts was transferred into a further 19 bank accounts. There was therefore a vast spider web of bank accounts which CMOC's money had passed through.

Worldwide freezing order against persons unknown

CMOC immediately tried to obtain a worldwide freezing injunction in the English courts to prevent further dissipation of the stolen funds. Although interim freezing injunctions are granted without notice to a defendant, the court ordinarily expects the defendant to be identified. After all, the defendant must be subsequently notified of the injunction so that they are able to contest it, not to mention the need to inform the defendant that breaching the injunction may result in a custodial sentence.

CMOC's difficulty was that it did not know who to serve the proceedings on. There was no cause of action in which the banks themselves could be named as defendants. CMOC had no choice but to ask for a worldwide freezing order against 'persons unknown', defined as:

"(1) any person or entity who carried out and/or assisted and/or participated in the fraud; and

(2) any person or entity who received any of the monies misappropriated from CMOC (including the traceable proceeds thereof) other than in the course of a genuine business transaction with a third party."

Mr Justice Waksman, sitting in the High Court, granted the injunction in these terms, noting that, as far as he was aware, it was the first occasion on which such an order had been made.

He explained that other types of injunctions against persons unknown had previously, if rarely, been granted by the courts. The most well-known example is the case of *Bloomsbury Publishing Group Limited and JK Rowling* v *News Group Newspapers Ltd and Others* [2003] 1 W.L.R. 1633, which concerned an application for an injunction against those responsible for removing copies of an unpublished Harry Potter book without authority and offering them for sale to the press. Giving the judgment of the court, Sir Andrew Morritt VC remarked:

"the description [of the defendant] *used must be sufficiently certain as to identify both those who are included and those who are not. If that test is satisfied then it does not seem to me to matter that the description may apply to no one or to more than one person or that there is no further element of subsequent identification whether by way of service or otherwise."*

The novel aspect of CMOC's application was that it was for a freezing injunction. Mr Justice Waksman saw no reason in principle why the courts' jurisdiction should not be extended to include this type of injunction. Indeed, there were good reasons to extend the principle. A primary freezing injunction is needed to act as the springboard for the grant of ancillary relief in respect of third parties, including, most importantly, orders that the recipient banks reveal the identities of the relevant account holders.

Service by Facebook Messenger and WhatsApp platforms

As CMOC's investigations continued, and the banks supplied information about the relevant account holders, particular defendants were able to be identified. This process would culminate in 30 defendants being identified for service of proceedings to recover the stolen monies.

Some of those defendants were identified only by conversations they had with other defendants on Facebook Messenger or WhatsApp, two private messaging services. This meant that these were the only methods of service available to CMOC to serve proceedings against those defendants. The question was whether sending a message on these platforms would be sufficient to act as proper service of legal proceedings.

Mr Justice Waksman held that in the circumstances these forms of service would be allowed. He took comfort from the fact that each service showed the sender of the message when the message had been received and

read by the addressee. He stressed that he was not setting any particular precedent, but was exercising his discretion to proactively consider different forms of alternative service which are justified in the circumstances of the case. This indicates the willingness of the courts to apply established principles more flexibly in situations where little is known about potential defendants due to the nature of their fraud.

Having carried out thorough investigations to identify 30 defendants and having frozen dozens of bank accounts, CMOC finally brought an action against those defendants to recover the money. One of the defendants remained 'persons unknown', as defined above, so that CMOC could apply to the court to have the judgment enforced against any defendant subsequently identified as falling within that definition.

The defendants

The defendants in the trial on liability were identified by their proximity to the accounts that the stolen monies were originally paid into. Thus, the holders of the bank accounts into which money was paid from the CMOC account were called "Level 1 payees", the recipients of payments from the Level 1 payees were called "Level 2 payees", then "Level 3 payees".

A "receiving defendant" was defined as a defendant who received CMOC monies, either directly or indirectly, which included all Level 1, 2 and 3 payees. A "participation defendant" was one who, due to their connection with the receiving defendants, was alleged to have been involved in the fraud. Most of the participation defendants were directors of one of more of the receiving defendants. "Perpetrators" referred to persons, currently unknown, who devised the original plan to hack Mr Chen's email and actually carried out the fraud.

CMOC made a variety of claims against the defendants. Those claims were: (1) a proprietary claim involving the use of tracing; (2) a claim for compensation for dishonest assistance; (3) a claim in damages for unlawful means conspiracy; (4) a claim in knowing receipt; and (5) a claim in unjust enrichment.

None of the defendants were represented at trial, leaving the claimant with an obligation to fairly present its claims to the court. That duty is less onerous than the duty of "full and frank disclosure", which parties making without notice applications must comply with, but the represented party must still draw to the attention of the court any factual or legal points that might be of benefit to the unrepresented party.

Proprietary claim

CMOC made a proprietary claim against all receiving defendants. The law treats stolen money as trust property held by the thief as a fiduciary. This means that if exactly the same money that was stolen can be identified, whoever currently holds that money will also hold it on trust for whomever it was stolen from. This claim was therefore automatically successful against all the defendants with bank accounts which still held some of the stolen money.

However, the disadvantage of this method of recovery is that when stolen monies are transferred into bank accounts with other funds this 'mixes' the money, and the traceable proceeds become limited to what is known as the "lowest intermediate balance" in the account. The effect of this is that the more the money is funnelled through bank accounts and mixed with other money, the less the claimant can recover. Given that CMOC's money had been mixed with money in so many different accounts, the judge found that CMOC could only recover a fraction of the total amount stolen by way of a proprietary claim.

Dishonest assistance

A claim for dishonest assistance was brought against the perpetrators of the fraud and the participation defendants.

Liability for dishonest assistance arises where a person acts dishonestly as an accessory to a breach of trust. Mr Justice Waksman had already established the stolen money was transferred in breach of trust for the proprietary claim. The remaining issues were whether the defendants assisted the breach of trust, and whether they did so dishonestly.

By definition the perpetrators had assisted the breach of trust because they instigated the breach in the first place by setting up the fraud and giving effect to it by ensuring the removal of the trust monies from CMOC. This was clearly dishonest because they knew there was no basis for removing the money.

What about the participation defendants that had received stolen money and were alleged to have been involved in the fraud, but in respect of whom there was no evidence they had perpetrated it? The judge noted that there was no evidence that any of these defendants gave any consideration for receipt of the monies, they had not repaid any monies despite being put on notice of the claim and despite CMOC's demands, they had been served with injunctions but had not given any disclosure, and they had been served with proceedings but had not filed any defence.

Mr Justice Waksman said that these facts, taken together, indicated that on the balance of probabilities the defendants had dishonestly assisted in the breach of trust. In particular, for the Level 1 payees, receiving the money directly from CMOC, there was no suggestion that they received the money for an innocent purpose, nor could any innocent purpose be imagined. It was therefore inconceivable that they did not know they were assisting in a fraud and were part of a fraudulent conspiracy.

For the Level 2 and 3 payees, the judge found that their ownership and/or association with the Level 1 payees meant that they must have had the requisite knowledge and involvement as well. All of these defendants were dishonest because they knew of the fraud, made no attempt to repay on demand, and undoubtedly assisted in the speedy onward transmission of the monies. Mr Justice Waksman confirmed that it was irrelevant that there was no evidence that the participating defendants knew the identity of the victim of the fraud, noting the dicta of Lord Millet in *Twinsectra Ltd* v *Yardley* [2002] 2 A.C. 164:

"It is obviously not necessary that he should know the details of the trust or the identity of the beneficiary. It is sufficient that he knows that the money is not at the free disposal of the principal. In some circumstances it may not even be necessary that his knowledge should extend that far. It may be sufficient that he knows that he is assisting in a dishonest scheme."

CMOC's claim for dishonest assistance against the perpetrators and the participating defendants therefore succeeded in full.

Unlawful means conspiracy

This claim was also made against the perpetrators and the participating defendants, on the basis that they had conspired to use illegal means to injure CMOC. For unlawful means conspiracy there must be: (a) a combination or understanding between two or more people, (b) an intention to injure another individual or separate legal entity, (c) concerted action consequent upon the combination or understanding, and (d) use of unlawful means as part of the concerted action.

These requirements were clearly met in the claim against the perpetrators. They had conspired to use unlawful means, including deceit, breach of trust, and theft, with the intention to injure CMOC, and had taken the relevant 'concerted action' by carrying out the fraud.

As for the participation defendants, Mr Justice Waksman held that, similarly to the claim in dishonest assistance, it could be properly inferred from the same facts that they had all acted together to give effect to the fraud. Their aim was to enrich themselves, which would inevitably cause injury to CMOC. That was sufficient to satisfy the intention to injure. Their participation in the fraud by receiving the stolen monies and passing them on constituted the required concerted action.

All of the perpetrators and participation defendants were therefore liable to CMOC in damages in both dishonest assistance and unlawful means conspiracy. It was however important for CMOC to succeed in a claim against the receiving defendants, so that they could recover the money that had been frozen in those defendants' bank accounts. The proprietary claim could only trace a fraction of the stolen money into those accounts. CMOC advanced two claims for this purpose: unjust enrichment and knowing receipt.

Unjust enrichment

CMOC claimed that each of the receiving defendants had been unjustly enriched, and should pay back the money under the laws of restitution. The relevant requirements for a claim in unjust enrichment are that the defendant was enriched, the defendant's enrichment was at the expense of the claimant, the enrichment was unjust, and there are no defences available to the claim.

At first sight one can be forgiven for thinking that these requirements were obviously satisfied. The receiving defendants had been enriched, and the enrichment was clearly unjust, and there were no defences available. There was, however, a problem with the requirement that all the receiving defendants were enriched at CMOC's expense. The problem arose in the form of a recent judgment of the Supreme Court, *Investment Trust Companies* v *Revenue and Customs Commissioners* [2018] A.C. 275, in which Lord Reed affirmed the general rule that a defendant can only be enriched at the claimant's expense if there has been a direct transfer between the two parties.

There were exceptions to this rule where the apparent direct recipient was disregarded in favour of the 'true' recipient, such as when an agent passed money on to a principal, or where the direct recipient is interposed as part of a sham transaction. Even if, however, one of those exceptions applied, a claim in unjust enrichment would not survive against the direct recipient, as it would in effect be transferred to the 'true' recipient. Only one 'level' of recipient could ever be enriched at the claimant's expense.

This was a major hurdle in a situation where CMOC's money had been transferred to Level 1, 2 and 3 payees. CMOC could elect to claim against Level 1 payees on the basis that they had been directly enriched, but that would preclude them from claiming from Level 2 and 3 payees. Alternatively, CMOC could claim, say, that Level 1 payees were acting as agents for Level 2 payees, and claim that the latter were the true direct recipients of the money at CMOC's expense, but that would preclude them from claiming against the Level 1 payees.

Mr Justice Waksman held he was bound by the rule approved by the Supreme Court and held that the claim in unjust enrichment was successful only against the Level 1 payees. While that might have been the correct result based on authority, the application of the rule in this context seems arbitrary and unprincipled. It is perfectly sensible to say that each of the Level 1, 2 and 3 payees were enriched at CMOC's expense. One would simply have to avoid double recovery in the normal way when claiming that the same amount had been transferred to

more than one party. It is clear from the judgment in *Investment Trust* that the Supreme Court was not contemplating this kind of scenario when they approved the general rule. Indeed, if similar facts reached the Supreme Court it is difficult to imagine that they would not carve out a further exception to the rule for chain transactions effecting a fraud, where multiple persons involved in the fraud could properly be said to be enriched at the claimant's expense.

Knowing receipt

This claim was made against all receiving defendants. It was important for CMOC to establish liability under this claim because only a fraction of the stolen money was recoverable under the proprietary and unjust enrichment claims against the same defendants.

The requirements for establishing liability in knowing receipt are: (i) there should be assets held under a trust or fiduciary duty; (ii) there has been disposal of those assets in breach of trust or fiduciary duty; (iii) there has been a beneficial receipt of those assets by the defendant; and (iv) the defendant had sufficient knowledge to render it unconscionable for him to retain the assets. Again, on these facts the first two requirements were met because stolen monies are held on constructive trust for the owner.

As for the third requirement, the judge held that there was no evidence to displace the assumption that each of the relevant defendants received the CMOC monies beneficially. It had not been asserted, for example, that any defendant was in truth receiving the monies only as an agent or nominee.

As for knowledge sufficient to render it unconscionable for the defendant to have received the CMOC monies, Mr Justice Waksman reaffirmed that the core facts were themselves sufficient to establish unconscionable receipt. The irresistible inference was that the receiving defendants knew perfectly well that the monies transferred into their accounts were trust monies in the sense that they had been fraudulently obtained by illegal hacking. Again, whether they knew the actual identity of the victim, the true underlying beneficiary of the trust monies, was in this context immaterial.

In addition, there were other features relating to certain receiving defendants that supported the required level of knowledge. In particular, many defendant companies shared the same directors, those companies had suspiciously low share capital for their purported activities, and there was no evidence that these companies carried on any real trading or business.

Overall, the judge considered that the claims in knowing receipt against all the receiving defendants had clearly been made out. Each was therefore liable to restore the payment which it received. With this result CMOC had been successful in its claims against all the defendants in the claim, whether perpetrators, participating or receiving.

To top it all off the judge expressed his displeasure towards the defendants by awarding compound interest to CMOC in its claims against all the defendants: for the claim in knowing receipt against the receiving defendants, and for the claim in dishonest assistance against the participating defendants. This was in fact a final innovation in the case, because, while compound interest is normally granted in claims of knowing receipt, it is not for claims in dishonest assistance. Mr Justice Waksman considered that he could see no reason in principle why the two claims should be treated differently, as they were both a form of accessory liability to a trustee's breach of fiduciary duty.

Conclusion

Although CMOC was successful in at least one claim against each defendant, it now faces the arguably more difficult task of enforcing the judgment against assets held in various offshore jurisdictions around the world. Nevertheless, as criminals come up with increasingly innovative ways to defraud companies by electronic means, it is reassuring to know that the English courts are demonstrating their willingness to innovate in turn to ensure these persons unknown face the consequences of their unlawful conduct.