trowers & hamlins

Legal update ——— December 2018

Dispute Litigation & Resolution
Tracing the proceeds of cybercrime

One of the challenges in pursuing cybercriminals relates to the speed at which funds that have been misappropriated can be transferred to accounts in foreign jurisdictions which can obstruct the process of tracing and freezing the money. The recent case of CMOC Sales and Marketing Ltd v Persons Unknown [2018] EWHC 2230 (Comm) has confirmed that it is possible to secure worldwide freezing injunctions against 'persons unknown' to assist with this issue.

Background

CMOC Sales & Marketing Limited (CMOC) is an English company whose parent company, CMOC Mining USA, is based in Phoenix, Arizona. Both companies are subsidiaries of CMOC Limited based in Hong Kong. In October 2017 CMOC became a victim of a cybercrime.

A total of US$6.91 million and €1.27 million were transferred out of the bank account of CMOC in a total of 20 separate transactions. A number of email accounts of CMOC were hacked into by the perpetrators and the key email account of CMOC that was hacked was the account of Mr Chen, who was a company director and an authorised signatory for the company. CMOC had two authorised signatories for the Bank of China accounts in London. Both Mr Chen and the other authorised signatory were based in Arizona.

As and when payments were required to be made the relevant members of the company would approve them and they would then be sent to Mr Chen by email, accompanied by a payment instruction on a blank company letter head (which had been pre-signed by both signatories). Mr Chen would then review the electronic copy of the payment instruction before personally sending it to the Bank of China in London for payment.

The perpetrators were able to hack the account of Mr Chen to the extent that they posed as Mr Chen and sent emails to the Bank of China (in London) to request that bank transfers were made. The details of the transfers were attached to each email in the same way as they would have been had Mr Chen sent the request himself. Accordingly the debits from the account of CMOC were made as instructed. It was clear to the Court how the bank had seen this as a genuine payment request.

The first sign of a potential issue was when emails from another director of CMOC were located in Mr Chen's recycle bin. It was later established that this had been due to a rule that had been set up by the perpetrators and linked to Mr Chen's inbox. However, at the time the issue was noted as a glitch and Mr Chen's email account was recreated by the internal IT team. At a later stage two employees queried payment instructions that had been processed as neither of them had any recollection of the payments being authorised. These emails were intercepted by the perpetrators and were therefore never seen by Mr Chen. The perpetrators replied to the concerned employees as if they were Mr Chen and noted that 'Mr Chen' was involved with an acquisition with CMOC Mining USA and this was the reason for the payments. As this response was received, allegedly from Mr Chen, neither of the employees made any further enquiries. The books for CMOC were also amended electronically to reflect these fictitious payments. The perpetrators also went one step further to make their emails seem believable by copying into the emails other directors of the company, but their email addresses were typed in a slightly different way which upon a quick glance would not be noticed and would therefore be perceived to be a genuine email. For example, the email addresses used by the perpetrators ended with cmocintermatlonal.com instead of cmocinternationa l.com.

The Proceedings

The first pre-trial hearing took place on 23 October 2017 and numerous applications were also made on paper. The difficulty with this fraud was not the fraud itself as this aspect was straightforward, but the identity of those who had committed the fraud. At the first hearing a worldwide freezing order was granted against persons unknown. The persons unknown were then categorised into groups which included any person or entity who

Published by
Trowers & Hamlins

Trowers & Hamlins LLP
3 Bunhill Row
London
EC1Y 8YZ

t +44 (0)20 7423 8000
f +44 (0)20 7423 8001

www.trowers.com

carried out, assisted with or participated in the fraud and any person or entity who received the misappropriated funds from the Claimant (this excluded those that received funds following a genuine business transaction). Once the persons unknown had been categorised the process of attempting to trace the fraudsters began. Disclosure orders were ultimately obtained and revealed that payments had been made to 50 different banks across 19 different jurisdictions.

The proceedings ultimately continued with no engagement from any of the defendants. No acknowledgments of service were filed, and no defence or evidence was filed by any of the defendants. Despite this it was essential for the Court to still carry out and conclude a fair presentation of the case.

The claims made by the Claimant included the following:

1. a proprietary claim involving the use of tracing;
2. compensation for dishonest assistance;
3. damages for unlawful means conspiracy;
4. a claim for knowing receipt; and
5. a claim for unjust enrichment.

Proprietary claim
The proprietary claim was successful. Where the Claimant was aware of the balance held by the defendant it was ordered that CMOC was entitled to a declaration that stated that the defendant holds the sum on trust for CMOC and there was also to be an order for the sum to be paid out to CMOC. Where the amount traced to the defendant was not known it was stated that the order should be that the traceable proceeds of the monies owed to CMOC are held on trust for CMOC.

Dishonest assistance and unlawful means conspiracy
The claims for dishonest assistance and unlawful means conspiracy were considered together by the Court. In respect of the claims made by the Claimant the defendants were split into different categories. The first category is described as the receiving defendants. This includes the defendants who received the payments either directly or indirectly. The second category of defendants was described as participation defendants. There was some overlap between the two groups of defendants. In respect of this claim the Judge concluded that all of the participation defendants were liable to pay to CMOC the full amount of funds that had been appropriated from the company by way of the fraud.

Knowing receipt
The knowing receipt claim was successful against all of the relevant defendants. Some defendants were excluded as there was no evidence available that they had received any of the CMOC funds.

Unjust enrichment
The unjust enrichment claim initially failed against all of the defendants (except those that were also excluded in the knowing receipt claim as set out above as the unjust enrichment claim was not made against them in any event) however, at the time of the Judgment, Counsel for the Claimant requested an opportunity to elect which defendants the unjust enrichment claim was made against. The Judge allowed the Claimant to elect a group of defendants for this claim to apply, given there had been no engagement from the defendants and therefore no party was prejudiced by this decision. The group of elected defendants were referred to as the Level 1 payees as they all directly received monies from CMOC. The unjust enrichment claim therefore only succeeded against the Level 1 payees.

All claims against the defendants, except for unjust enrichment, succeeded as originally pleaded by the Claimant. The Court also awarded costs on an indemnity basis for the Claimant due to the lack of engagement from any of the defendants. The Court felt it was just for the Claimant to be compensated fully for all of the costs that had been incurred by the Claimant in the pursuit of the claim. In respect of the costs incurred in relation to the work carried out by the Claimant to pursue defendants outside of the jurisdiction the costs could not be recovered but they were able to be recovered as an additional sum of damages as the costs were incurred by the Claimant in an attempt to mitigate their losses.

What made this claim any different?

The unusual aspect of this claim relates to the granting of the worldwide freezing order against persons unknown. Whilst there is case law for injunctions to be granted against persons unknown (for example, in trespass cases) this was the first claim of its type where the concept was extended to freezing injunctions. The practical application meant that if CMOC could show that a particular account fell into one of the classes, the account could be frozen without going back to court to seek a further injunction (or to vary the existing injunction). This undoubtedly maximised the prospects of recovering misappropriated funds and is likely to have saved costs overall.

As well as this the Courts also allowed service to take place by alternative methods to assist the Claimant in being able to serve the claim on Defendants that were reluctant to engage. Albeit the Court did note that no precedent was to be set, service was allowed to take

place by use of Facebook messenger and WhatsApp messenger.

In addition to the use of alternative methods of service, the Courts also allowed the Claimant to utilise a data room as a way to provide the vast background documentation to the number of defendants and banks that became involved with this matter. The claim had to be first served upon the defendants by a court approved method before the Claimant was then able to serve the documentation by way of the data room, but in respect of the banks that were added to the proceedings the Claimant was allowed to serve the claim and the documentation by way of a link to the data room. It is unclear as to how many of the defendants utilised the data room due to the lack of engagement from them as a collective, but the Court did note that the banks that were joined to the proceedings as "no cause of action defendants" found the data room particularly helpful and none of them required hard copies of the documentation to be provided to them by post or for copies to be sent to them by email. This method of service was approved by the Court based on the circumstances of this particular claim and was deemed to be an *"innovative feature of this litigation"*.

Closing remarks

This case is a welcome development in the fight against cybercrime and will assist victims in recovering misappropriated funds or assets. The importance of acting swiftly, following the discovery of an incident, remains paramount.

Trowers & Hamlins are experienced in advising organisations and individuals following the discovery of a cyber fraud incident. Please get in touch with the writers to discuss the judgment or how we may be able to assist you.

For more information please contact

Mark Kenkre
Partner
t +44 (0)121 214 8863
e mkenkre@trowers.com

Christopher Recker
Associate
t +44 (0)121 214 8842
e crecker@trowers.com

Hannah Jakeman
Solicitor
t +44 (0)121 214 8875
e hjakeman@trowers.com