Chasing Down the Cyber-Criminals: A Lesson in Innovation

December 31, 2018

RELATED PRACTICES International Arbitration

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.

© 2026 Haynes and Boone, LLP

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.

To read the full publication, please click on the PDF linked below.

Chasing-Down-the-Cyber-Criminals-A-Lesson-in-Innovation.PDF

© 2026 Haynes and Boone, LLP