Cyber Scams, Injunctions and Tracing Fraudulent Funds Transfers

The recent High Court case of *Foglia v Family Officer Ltd & Ors* [2021] EWHC 650 (Comm) (22 March 2021) demonstrates the important interaction between legal remedies and IT technical expertise to discover the necessary evidence to trace stolen funds and expose fraudulent scams relating to email spoofing and social engineering fraud. In this context, the term 'social engineering' refers to fraudulent scams where the victim is manipulated into disclosing passwords or other confidential information or transferring funds. The case further illustrates how the English Courts have been adapting traditional legal remedies to these evolving cyber risks.

The Background

The Claimant was the victim of a fraud which misappropriated €15 million from a bank account in the Cayman Islands. The account held funds through a fiduciary nominee, Unione Fiduciaria (**UF**). The unidentified fraudster conveyed payment instructions to the Cayman Islands bank, impersonating an authorised signatory of UF by telephone calls and by fax. The misappropriated funds were sent to a bank account in England held by the First Defendant (**TFO**) which was wholly owned by the Fourth Defendant, Mr Cerri.

The Claimant obtained a series of non-party disclosure orders against various third parties, such as the banks and financial institutions to trace the funds and identify the perpetrators. The Claimant also obtained a series of freezing and proprietary injunctions against initially "Persons Unknown" and, after identification, the Defendants. As a result of these Court orders, the Claimant recovered approximately €11.5 million of the €15 million that had been stolen from the Defendants and third-party recipients of the proceeds of the fraud.

To recover the remaining amount of approximately €3.5 million (plus interest and costs), the Claimant advanced proprietary claims and claims in knowing receipt, dishonest assistance, and unjust enrichment against the Defendants. Thereafter, the Claimant made an application for summary judgment on the basis that the Defendants had no real prospect of successfully defending these claims at trial. The High Court's judgment was handed down in relation to the Claimant's summary judgment application.

In his defence against the summary judgment application, Mr Cerri argued he was "set up" by unknown person(s) who carried out the fraud on the Claimant. He believed the €15 million received by TFO belonged to an Italian businessman named Mr Antonio Aloschi.

Mr Cerri contended that the Claimant could not identify how he could have known details of the Claimant's financial affairs, or those of Mr Aloschi, and how he had any of the information necessary to engineer the payment of €15 million out of the Claimant's bank account.

Mr Cerri's explanation for payments which he caused TFO to make out of the €15 million received was that they represented investments he was making pursuant to an agreement between himself and Mr Aloschi.

In view of the evidence regarding the spoofed emails, Mr Cerri accepted that he had no agreement with the real Mr Aloschi, but he contended that he did not know at the time that the emails that he had received from Mr Aloschi were spoofed (i.e. that the sender's email address purporting to be from Mr Aloschi was forged). He also pointed to certain handwritten notes from his notebooks as proof of negotiation of the alleged agreement.

The Decision

The Court rejected Mr Cerri's explanation for his innocent receipt and use of the proceeds of the fraud, on the following basis:

(i) **The Phone Mast Evidence**: this evidence obtained pursuant to Norwich Pharmacal Orders made against Vodafone and Revolut Bank demonstrating, as was accepted by Mr Cerri, that:

- the phone handset and SIM card associated with the mobile number that was used to make the fraudulent payment calls were purchased using a bank card belonging to a junior employee of TFO and, on the day before that purchase, Mr Cerri transferred £200 to the account of that employee; and

- the fraudulent caller's location, when the call was made, was less than 100 metres from TFO's office.

Mr Cerri contended that the handset and SIM were given to a representative of Mr Aloschi before the scam calls were made. He also argued the unknown fraudster might have operated close to his office, either coincidentally, or because there was an intent to implicate him. As a result, in view of these arguments, the Court accepted the phone mast evidence was not in and of itself capable of sustaining a summary judgment application without a trial.

Further, in relation to the phone mast and other tracing evidence, Mr Cerri also argued that there was a "clash of improbabilities". If Mr Cerri were the real fraudster, he would not have made the scam calls from such proximity to his office and would have arranged for the Claimant to pay the funds into a bank account with which he had no connection. As a result, Mr Cerri contended that in view of this alleged "clash of improbabilities" and unknowns which remained in the case, the Court should not grant summary judgment. However, the Court was unconvinced by this argument because it presupposed a level of information by Mr Cerri (as the real fraudster) in relation to the way in which funds may be traced.

(ii) **The Spoofed Emails**: these were emails relied upon by Mr Cerri to evidence his alleged agreement with Mr Aloschi, that, it transpired, were manufactured by a Czech website. In addition, Mr Cerri failed to produce reliable copies "in native format" of two of the spoofed emails that contained earlier emails sent by Mr Cerri. As a result, the Court held that the spoofed email evidence was consistent with Mr Cerri either being the fraudster or conspiring with the fraudster.

(iii) **Cui bono?:** the alleged 'investments' that Mr Cerri claimed to have been making on Mr Aloschi's behalf with the misappropriated monies, in reality consisted of paying off debts owed by Mr Cerri and his companies. Further, there was no due diligence carried out by Mr Cerri in respect of Mr Aloschi before the funds were received. Therefore, the Court held that, if, as alleged by Mr Cerri, the unknown fraudster was impersonating Mr Aloschi and Mr Cerri was innocent, it would be odd for this fraudster to enter into an agreement which only benefitted Mr Cerri. The alleged agreement allowed the purportedly innocent Mr Cerri to use a portion of the funds for his own benefit (and not the fraudster's).

In conclusion, the Court held that the spoofed emails defied any innocent explanation. In any event, taken together, the mobile phone evidence, emails, and payments to Mr Cerri, comprised a body of evidence which justified the conclusion that any innocent explanation was fanciful. As a result, the Court granted summary judgment to the Claimant.

In reaching this decision, the Court noted how CPR 24 empowers the Court to give summary judgment in respect of a claim if it considers that a defendant has no real prospect of successfully defending it, and where there is no other compelling reason why the claim should be disposed of at trial.

Despite this type of unusual application for summary judgment in a fraud claim on the merits, the Court further held that the standard of proof for granting summary judgment against the Defendants is neither the criminal standard, nor the normal civil burden of proof as if the application for summary judgment was a trial. Instead, the correct standard of proof is that, bearing in mind the possibilities for further evidence, the Defendants' "…*prospects of success are truly fanciful as opposed to real*". The Court added that the *"…approach of looking to see if any honest explanation is possible, at the pleading stage, is almost certainly a sound cautionary check".*

Commentary

This case demonstrates the importance placed by the Courts on highly technical IT evidence in cases of cyber fraud, such as email spoofing and social engineering scams, where technology is at the forefront of evidence gathering. It also illustrates the interaction between IT technical investigatory techniques that will determine the appropriate follow-up Court applications for specific injunctions to trace assets and to identify perpetrators. Furthermore, the Court held that Mr Cerri's failure to provide IT evidence, namely, any reliable copies "in native format" showing the origin of emails sent by Mr Cerri to UF, was fatal to Mr Cerri's defence.

By Celso De Azevedo

36 Commercial
www.36commercial.co.uk
clerks@36commercial.co.uk
Tel: +44 (0)20 7421 80512

Celso De Azevedo is a highly experienced international cyber, reinsurance and commercial dispute resolution barrister and qualified New York Attorney. He is regarded as a leader in the fields of high value international litigation and arbitration.