Surge in wire transfer fraud leaves victims looking to banks for redress

9 June 2016

Fraudsters targeting businesses is not a new phenomenon. In its January 2010 report, the National Fraud Authority estimated that approximately £5.4bn had been lost to corporate fraud in the UK during 2008 (please see page 26 of the Report). This figure does not include frauds suffered by SMEs and so the actual losses suffered by UK businesses are likely to be higher than this.

However, 2016 has so far seen a surge in fraudulent activity in the business sector, with fraudsters levelling scams against both small businesses and multi-million pound corporations. One increasingly common scam that has recently emerged is "Business Email Compromise". The FBI has estimated that this scam alone has cost businesses globally around $2.3bn. High profile victims of the scam have included US grain supplier Scoular, who were duped into wiring $17.2m to an offshore bank account. This type of scam suggests that there are two key developments emerging in fraud cases: (1) the fraudsters are becoming even more sophisticated in their methods of obtaining "legitimate" cash; and (2) they are using the financial system (banks and other financial institutions) to do so.

Business Email Compromise scams

Essentially, the fraudster tricks an unsuspecting employee into making a wire transfer payment by means of an attack on an email account. Whilst the execution of the fraud can have a number of different fact patterns, it is effectively perpetrated by the fraudster either compromising or impersonating an email address, and using this to convince an employee to make the payment for a perceived legitimate business reason. For example, the employee may get an email from the fraudster, who has been able to compromise the CEO or CFO's email address, requesting an urgent bank transfer to be made. Alternatively, the fraudster could impersonate a supplier purporting to notify the business of a change of bank for payment purposes. In some circumstances, invoices sent via email have been intercepted and the account details altered, leaving the business none the wiser that the fraud has taken place at all, until they are contacted by the (genuine) supplier – who will have been expecting the (genuine) payment.

Generally, the money is then transferred through multiple bank accounts, sometimes using foreign exchange platforms, before ultimately being withdrawn and dissipated. This makes the tracing of the funds extremely difficult.

Any comments or queries?

Parham Kouchikali
Partner
+44 20 3060 6189
parham.kouchikali@rpc.co.uk

Obtaining information to identify the fraudster

Banks will often cite client confidentiality as a reason for not providing account-holder details to victims of fraud, creating a delay in obtaining vital information concerning the fraud. However, a Norwich Pharmacal Order (a form of disclosure order available against third parties) can be a useful tool in compelling the bank, that has become mixed up or otherwise facilitated the wrongdoing, to provide documents or information connected to the wrongdoing. This can assist the victim in "following the money" and in identifying the fraudster.

If the ultimate fraudster is found, it may be possible to obtain a freezing injunction to prevent the dissipation of their assets. In order to obtain a freezing injunction, the fraud victim would need to demonstrate a substantive cause of action for which there is a good arguable case, as well as the existence of the assets, and that there is a risk of dissipation of those assets. It must also be shown that the English Court has jurisdiction and the applicant must be prepared to provide an undertaking in damages. If the injunction being sought is to specifically freeze the funds that have been transferred as part of the fraud, there is no need to establish a risk that the assets will be dissipated. When the fraudster's assets are located outside of the jurisdiction, it may be possible to obtain a worldwide freezing order although enforcing such an order may be complicated and time consuming depending on the location of the assets.

Potential claims against financial institutions that facilitated payments

But what if the ultimate fraudster cannot be located, the assets are no longer traceable or are in a jurisdiction where recovery would be, at best, extremely difficult? Often this is the real problem for victims of such a fraud: they are simply too late and the party against whom there is legal redress is either unidentifiable or, in the best case scenario, has long got rid of the proceeds of the fraud and has no assets against which meaningful enforcement action can be taken. In such circumstances, the claimant will have to think about other potential defendants. A claim against banks and other financial institutions that the money has passed through is an attractive proposition. Such entities have deep pockets, are heavily regulated and regularly scrutinised for their customer due diligence and money laundering procedures.

In order to establish which claims may be brought against banks and other financial institutions, it is first necessary to determine the scope of their obligations and duties.

Duties to customers

Banks owe duties of care to their customers. For example, a bank is under a duty to comply with the terms of its customer's mandate. However, the precise scope of the duty will depend upon the contractual relationship between the bank and its customer, as well as other factors such as usual banking practice.

Recently, the Court of Appeal held in *Tidal Energy Ltd v Bank of Scotland*[1] (by a majority) that banks are not required to check that the name on the account corresponds to the account number and sort code when executing a CHAPS transfer. Similarly, in *Abou-Rahmah v Abacha*[2] it was held that the bank was not negligent for failing to notice that the account to which the payment should be made was "Trust International" rather than the fraudster's account under the name "Trusty International". These cases demonstrate that a bank will not be in breach of the duty of care owed to its customers for failing to check that the name of the beneficiary matches the account details set out in the instructions to the bank. This is particularly relevant in the context of Business Email Compromise scams, as quite often the fraudster will give the name of a legitimate business (for example the genuine supplier's name) but provide a different account number and sort code.

1. [2014] EWCA Civ 1107.
2. [2007] 1 All ER (Comm) 827 CA.

Another significant problem is that often the victim of this kind of fraud is not the customer of the bank through which funds have passed before being siphoned out. This adds a level of complexity to the analysis.

Regulatory obligations

The current legislative framework requires banks and other financial institutions to, amongst other things, put into place policies and procedures to help them detect fraud and other financial crime and to prevent their services from being used for money laundering or terrorist financing. This includes by way of carrying out risk-sensitive customer due diligence checks to identify their customers (including their beneficial owners); verify their identities; and find out more information to enable them to understand the purpose and intended nature of the relationship.

Against this regulatory background, it may be possible for civil claims to be brought against banks for failing to carry out appropriate anti-money laundering and customer due diligence checks when the proceeds of fraud are transferred through their accounts.

Potential claims that may be brought

The first potential claim that could be brought against a bank is a claim for unjust enrichment. This claim is quite attractive as it does not, on the face of it, require any wrongdoing on the part of the bank. Rather, the cause of action arises out of restitution by virtue of the fact that the bank has received a benefit that it should never have received. The requirements to establish this cause of action are: (1) an enrichment or receipt of a benefit; (2) the enrichment is unjust; and (3) the enrichment was at the expense of the claimant. However, the difficulty is that if the money has already left the fraudster's account (which often happens very quickly) then the bank will likely be able to rely on the defence of "change of position", as it no longer has the money. Whilst a bank will be precluded from relying on this defence if it can be established that the bank acted in bad faith, this will be extremely difficult to prove.

Other claims that may potentially be brought are claims in equity for dishonest assistance or knowing receipt of trust property. The difficulty in these types of claims is that it is necessary to either prove that the bank was dishonest or that it had knowledge that the property was trust property and has been transferred in breach of trust. Effectively, a bank would have had to have been involved in the fraud, or to have known that there was a real chance that the funds were the proceeds of money laundering and still turned a blind eye to this. There is some judicial support to suggest that a bank could be found liable for knowing receipt when money is transferred through its accounts. In *Abou-Rahmah v Abacha*[3] Lord Justice Rix opined that given that money laundering is such a serious crime, he could not see "why a bank which has, through its managers, a clear suspicion that a prospective client indulges in money laundering, can be said to lack that knowledge which is the first element in the tort." In short, if there is evidence of dishonesty for the purposes of dishonest assistance or the requisite knowledge for knowing receipt, these claims can be considered. However, any such evidence is likely to be circumstantial (often obtained as part of the Norwich Pharmacal Order for disclosure of information about account opening and money laundering processes) and obtaining further information from the bank is likely to prove difficult.

Conclusion

Victims of wire transfer fraud are struggling to get redress because tracking down the ultimate fraudsters and getting the funds back is usually not a realistic option. Most organisations' insurance policies also do not provide cover for this type of fraud as there is no "cyber-attack" in the classic sense on the organisation's IT infrastructure. What they are faced with is a 21st century variation of one of the oldest scams – making payments to those who are not genuine. It is argued that given the exposures, banks need to be held to higher standards to ensure that this type of fraud is not facilitated through their systems.

3. [2007] 1 All ER (Comm) 827 CA paragraph 37.

About RPC

RPC is a modern, progressive and commercially focused City law firm. We have 79 partners and over 600 employees based in London, Hong Kong, Singapore and Bristol.

"... the client-centred modern City legal services business."

At RPC we put our clients and our people at the heart of what we do:

- **Best Legal Adviser status every year since 2009**
- **Best Legal Employer status every year since 2009**
- **Shortlisted for Law Firm of the Year for two consecutive years**
- **Top 30 Most Innovative Law Firms in Europe**

We have also been shortlisted and won a number of industry awards, including:

- **Winner – Law Firm of the Year – The British Legal Awards 2015**
- **Winner – Competition and Regulatory Team of the Year – The British Legal Awards 2015**
- **Winner – Law Firm of the Year – The Lawyer Awards 2014**
- **Winner – Law Firm of the Year – Halsbury Legal Awards 2014**
- **Winner – Commercial Team of the Year – The British Legal Awards 2014**
- **Winner – Competition Team of the Year – Legal Business Awards 2014**
- **Winner – Best Corporate Social Responsibility Initiative – British Insurance Awards 2014**

Areas of expertise

- Banking
- Commercial
- Commercial Litigation
- Competition
- Construction
- Corporate
- Employment
- Insurance
- Intellectual Property
- Media
- Outsourcing
- Pensions
- Private Equity
- Real Estate
- Regulatory
- Reinsurance
- Tax
- Technology

Tower Bridge House
St Katharine's Way
London E1W 1AA
T +44 20 3060 6000

Temple Circus
Temple Way
Bristol BS1 6LW
T +44 20 3060 6000

11/F Three Exchange Square
8 Connaught Place
Central Hong Kong
T +852 2216 7000

12 Marina Boulevard
#38-04 Marina Bay Financial Centre Tower 3
Singapore 018982
T +65 6422 3000