HFW LITIGATION

JANUARY 2020

EMAIL PAYMENT FRAUDS – STAYING ONE STEP AHEAD

Email payment frauds are becoming more elaborate and can have a heavy financial cost for those that fall victim to them. In this briefing, we examine what businesses can do to prevent themselves becoming a victim to these frauds and to recover money paid out if they do fall victim to such a fraud.

"If money is paid out to a scam account, recovery is still possible in various jurisdictions, provided that you act very promptly."

What is happening?

The majority of businesses now send their invoices for payment by email, making them and their invoices vulnerable to exploitation by increasingly sophisticated fraudsters who operate online. We are observing an increase in the number of instances where email accounts operated by the fraudsters make urgent requests for payment into bank accounts that are operated or controlled by the fraudsters. The emails sent by the fraudsters often attach counterfeit invoices or payment instructions that closely mirror previous legitimate requests (for example, amended payment account details may be the only initial discernible difference between the new fraudulent invoice and an old invoice that was valid).

Often, these fraudulent payment requests are sent by email, marked as urgent and "from" a key contact, such as the CEO or CFO. This is primarily done with the purpose of bypassing the internal scrutiny that an everyday payment request may be subject to.

Money paid into the fraudulent bank account is invariably dissipated into other bank accounts, which are often located in other jurisdictions in an attempt to prevent recovery. A direct consequence of incorrectly paying monies to the fraudsters is that the contractual counterparties remain unpaid. This can have both significant legal and commercial consequences.

In the recent English Commercial Court judgment in *K v A*[1], a buyer who had fallen foul of an email scam and paid to the correct bank but the wrong account was found to be in breach of contract for failure to pay for the goods it had purchased.

How can you identify a suspicious payment request?

The best protection against fraudulent emails is to identify them prior to making payment. They will often appear genuine at first glance but there are measures, which we have outlined below, which, if actioned, can increase your chances of identifying a fraudulent email:

- Check the covering email / attached invoice carefully –
  - Is the email address of the sender different from the sender's email signature?
  - Has the suspicious email been sent from a third party email account (e.g. Hotmail or Gmail) instead of the usual (and correct) company email address?
  - Is there a link in the suspicious email that would not normally be included, which leads you to another screen or portal where you are required to enter login or other requested details?

If any the above questions can be answered in the affirmative then the email in question should be treated with suspicion and you should notify your internal IT point of contact to confirm the source of the email.

- Review previous invoices / payment requests sent by the alleged requesting party –
  - Do the payment details / addresses differ from the previous invoice / payment request?
  - Are there any repeated paragraphs, incorrect names, errors or typos in the relevant email or physical addresses?

If either of the above questions can be answered in the affirmative then please follow the advice provided under (a) above.

- Implement and follow a set of internal procedures –
  - Ensure that any request is reviewed and approved by more than one person.
  - Ensure that the provenance of the invoice is verified by a method other than by email e.g. telephone.

1 [2019] EWHC 1118 (Comm)

- Provide updates and training to employees on cyber security.

(Please speak to HFW if you would like guidance on drafting appropriate internal cyber policies.)

- Work with your IT department to ensure that -
  - Your organisation's "*spam*" email filter is catching emails that originate from improper or unusual email addresses outside your organisation.
  - You have satisfactory cyber security procedures in place, e.g. two factor authentication.

What if you have been the victim of an email fraud?

If money is paid out into a fraudulent account, recovery is still possible in various jurisdictions, provided that you act promptly. We focus below on recovery in the UK and in Switzerland:

UK & Switzerland –

- Do not delay! You are in a race against time before the misappropriated funds are dissipated.
- Notify your bank immediately.
  - **UK:** Banks are able to notify each other of potential fraudulent activity, which may ensure that a temporary freeze is placed on the recipient account. This can be done by email or phone.
  - **Switzerland:** Funds can be frozen without the need for any intervention by a Court or authority by giving detailed notice to your bank together with explanatory evidence detailing that fraudulently misappropriated funds have been deposited in an account held with that bank. Provided that the evidence is compelling, the bank will usually freeze the relevant funds and prevent the fraudsters from dissipating the funds further.
- Instruct solicitors to apply to Court and obtain an order freezing the account to prevent any further dissipation.

HFW London has recently acted successfully to recover over GBP 2 million in misappropriated funds from a frozen bank account following a fraud perpetrated using a malicious link in an email through the Commercial Court.

The process in Switzerland is driven either by prosecutors, who are able to freeze assets related to criminal proceedings through a criminal freezing order, or by civil courts through an urgent attachment order. Both orders can be obtained at short notice. However, the need to act quickly is again paramount.

HFW Geneva gives regular advice to its clients in this regard, and has recently acted successfully to obtain an attachment order over a Swiss bank account, for a claim worth approximately USD 26 million.

Additional measures available in the UK

- At the same time as applying for the freezing order under (3) above, you can also apply for a *Norwich Pharmacal* order compelling disclosure of the bank account details into which the fraudulent payment has been made (including the name and address of the account holder and details of the funds remaining in the account and any subsequent transfers). This may aid any later recovery actions.
- Finally, if the funds have been transferred to accounts overseas you can apply to the Court for a worldwide freezing order (WFO) against those accounts. The Commercial Court has recently expanded the interim remedies available to claimants by granting the first WFO against "*persons unknown*".[2] This will assist claimants where there are difficulties in identifying unknown cyber criminals.

For further information, please contact:

ANDREW WILLIAMS
Partner, London
T +44 (0)20 7264 8364
E andrew.williams@hfw.com

PATRICK MYERS
Associate, Geneva
T +41 (0)22 322 4808
E patrick.myers@hfw.com

ALIX BOSSON
Associate, Geneva
T +41 (0)22 322 4815
E alix.bosson@hfw.com

2 CMOC Sales and Marketing Ltd v Persons Unknown & 30 Ors [2018] EWHC 2230

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our Dispute Resolution capabilities, please visit www.hfw.com/Dispute-Resolution

hfw.com

Americas | Europe | Middle East | Asia Pacific