SOMETHING ROTTEN IN THE STATE OF SHIPPING

WHAT YOU NEED TO KNOW ABOUT MANDATE FRAUD AND THE FRAUDULENT REDIRECTING OF PAYMENTS

A recent shipping review lists fraud, as well as theft and corruption, as the joint second highest risk to the shipping sector, ranked only behind that of market developments, such as market volatility[1].

This briefing focuses on the fraudulent redirecting of invoice payments, Mandate Fraud, and covers what it is, how to respond and how it may be combated.

What is Mandate Fraud?

The doctoring or the giving of fraudulent payment instructions so that funds are redirected from the intended recipient and instead to the fraudster.

1 Allianz Safety and Shipping Review 2017

“We at HFW have seen a recent example of both genuine parties being kept in the dark by the fraudster, through the sending and intercepting of emails from hacked email accounts. This, combined with the use of emails sent from fake email addresses, created an elaborate and convincing deception.”

Who is at risk?

You are.

The potential threat is significant. All companies in the shipping industry are inevitably required to make payments to third party suppliers of goods or services on a daily basis. The amounts too may be significant, if relating to charter hire payments, a ship purchase or brokerage commissions.

How does it happen?

At its most basic, the scam may involve the sending of fake invoices from a company that purports to have provided services, such as those required in port, but in fact has not. BIMCO helpfully keeps a log of companies reportedly issuing such fake invoices[2].

There are also instances of fraudulent payment instructions being sent from an email address very similar to that one used by the company providing the services to which the payment is to be made. The deception is simple but can be very difficult to spot. The fraudster need only set up a domain name similar to that of the party receiving the funds so that payment instructions can be sent. That email may appear to come from some external and known organisation or even from someone senior within your company authorising a payment (i.e. “I am at a meeting today, please settle the attached invoice immediately..”).

More sophisticated is the fraudster deploying the hacker’s toolkit: the use of phishing, malware and viruses, to enable access to and control over email accounts. Hackers are looking to gain access to your computers and data, capture keyboard strokes (potentially compromising passwords on other systems) or intercept network traffic. Successful infiltration of your or a third party supplier’s computer systems may allow a fraudster to give or manipulate payment instructions by email so they appear to come from an authorised person, such as someone in a supplier’s accounts department that you may have dealt with previously.

We at HFW have seen a recent example of both genuine parties being kept in the dark by the fraudster, through the sending and intercepting of emails from hacked email accounts. This, combined with the use of emails sent from fake email addresses, created an elaborate and convincing deception.

Alarmingly, there is also a reported instance of a virus automatically altering the text of an email to include different bank account details[3].

What to do when Mandate Fraud is discovered?

The fraud can be difficult to uncover and may remain unnoticed until the genuine third party chases for payment, funds having already been diverted by the fraudster.

Upon discovering the fraud, rapid steps are required in order for you to have any chance of successfully tracing and recovering paid funds. Immediate steps should include the following:

- Notifying your bank to try and ‘stop’ the payment
- Notifying the recipient bank to put them on notice of the fraud
- Requesting the recipient bank to notify any other bank it has been instructed to send funds on to
- Notifying your genuine contractual counterpart to alert them that there may have been a security breach – this should be done over the telephone
- Notifying your insurers
- Referring to your ‘crisis response’ team. This team will include your

2 https://www.bimco.org/search-result?term=Fraud

3 http://www.bbc.co.uk/news/technology-40685821

lawyers, and potentially cyber-risks experts/those with specialist IT skills in order to assess if the company's cyber-security has been compromised

- Notifying Action Fraud in the UK, if appropriate, who may then take up matters with the National Fraud Intelligence Bureau (NFIB)
- In appropriate cases, urgent court applications may be required

Having in place a protocol of response in advance is recommended as an important element of good risk management.

How can the English courts help following the discovery of Mandate Fraud?

The English Courts have powerful weapons at their disposal in order to try and uncover information and recover extorted funds.

- A Norwich Pharmacal Order (NPO) is a form of disclosure order that may be used to obtain information in order to trace assets or bring proprietary claims. It is helpful when wrongdoing has taken place and the applicant does not know the identity of the wrongdoer but can identify a third party who can provide information i.e. the fraudster's bankers
- A Freezing Order is an order that prevents a party from disposing of or dealing with assets in order to preserve property, here the funds in the fraudsters' bank account. It may be possible, in appropriate cases, to obtain a "worldwide freezing injunction" intended to apply to assets in countries outside of the English court jurisdiction. For example, if a global bank is involved, service of an English court 'worldwide' Freezing Order might be sufficient to freeze a foreign bank account

The target of these orders will be the fraudster's bankers, who must be formally served with the orders obtained and other formal documents. The applicant will also be required to give certain undertakings to the court.

In a recent case handled by HFW these tools enabled us to successfully block a fraudsters' bank account and, ultimately, to recover the funds. It is important to bear in mind that each case is different, with different factual considerations. While it is critical to take all possible steps as fast as possible, there is never a guarantee of success.

Importantly, very urgent court applications, such as those following a fraud, may be made in the English courts outside of normal court hours. If a payment to a bank account outside of the English jurisdiction is involved, it may be appropriate to try and obtain relief from the local court where the bank account is located, subject to the remedies available there. For example, we have in the past obtained a 'Rule B' garnishment in New York over a fraudster's bank account, leading to the recovery of funds.

What can you do to minimise the risks of becoming a victim?

A bill of lading has been referred to as the keys to the floating warehouse.

Without proper precautions and security measures in place, access by a hacker / fraudster to a corporate email account could be regarded as being given the keys to the safe.

However, the threat may be reduced through employing tested best practice control and risk management protocols. These can include the following:

- Ensuring that payment instructions and bank account details are checked by telephone with an officer of the intended recipient company, especially for larger payment amounts. This should be done using a phone number or contact already known to you, rather than relying on a number or a web link included within the email exchange
- To always query changes in payment details, again orally, by telephone using 'known' contact details
- For larger transactions, for payment details to be potentially provided directly in person by an individual from the recipient company, carrying with them appropriate identification
- Payment requests to be verified internally by more than one individual, such approval requiring the use of a hardcopy signed document, signed by multiple authorised signatories
- Agreeing with your Bank a pre-arranged financial limit for payments, so that any payment request exceeding the set limit triggers a telephone call from your Bank to obtain oral confirmation that the payment may proceed
- To consider the use of disclaimers, in contractual documents or in the standard texts of emails, making clear that changes or amendments to bank details by suppliers will require phone confirmation, preceding any invoice payment
- Ensure that email security settings are in place to minimise the likelihood that emails may be intercepted or email systems compromised. At a basic level this should include the use of long and complex passwords, and 'two factor access' ("2FA"), particularly for any web based access
- Never leave paper copy invoices unattended
- Educate your staff to be vigilant against the risks of Mandate Fraud and when or how it may arise

The most important protection of all is for you and your colleagues to remain alive to the risks of deception and to be on constant alert for anything unusual or different arising in relation to payment requests. Tell-tale signs might include changes in the language, grammar or spelling used in an email by a familiar supplier or counterpart, or differences in the appearance of an invoice sent compared to that seen previously.

If there is any doubt, always err on the side of caution and seek verification with your counterpart by telephone.

Wider risk management

This briefing has focused on controls and processes specific to reducing the risk of Mandate Fraud and having a clear plan for dealing with any fraud that occurs. This will of course need to be part of a wider risk management plan, including assessment of your company's cyber-security and risk exposure together with cyber-security experts. It is critical to ensure that your staff are regularly trained on the risks and your IT security is up to date. The importance of cyber-security cannot be overstated – cyber criminals target any business which is not properly protected. It is recommended that all businesses engage cyber specialists to review exposure and suggest remediation plans. Useful benchmarks are the government-backed Cyber Essentials and Cyber Essentials Plus accreditations. You should also review your company's insurances to check whether they are sufficient to cover any losses and legal expenses as a result of Mandate Fraud.

For more information, please contact the authors of this briefing:

PAUL DEAN
Partner, London
T +44 (0)20 7264 8363
M +44 (0)7770 951092
E paul.dean@hfw.com

RORY GROUT
Senior Associate, London
T +44 (0)20 7264 8198
M +44 (0)778 9716 335
E rory.grout@hfw.com

HFW has over 500 lawyers working in offices across Australia, Asia, the Middle East, Europe and the Americas. For further information about our shipping capabilities, please visit hfw.com/shipping

hfw.com