STEAMSHIP MUTUAL

Comprehensive Cover. Exceptional Service.

Payment fraud alerts

December 2019

The hacking of email accounts and the frequency and sophistication of intercepted and fraudulent emails has increased over recent years resulting in payments being made inadvertently to fraudulent bank accounts. Some victims eventually manage to recover their money, while the more unlucky ones are often left with no choice but to abandon any recovery, due to the insubstantial amount and/or costs involved. However, in a recent case in the English Commercial Court dealing with a "payment interception" fraud, K v A [2019] EWHC 1118 (Comm), the defrauded paying party managed to retrieve over US$1million, but also lost US$161,646 due to fluctuations in foreign exchange rates.

Facts:

In K v A, A agreed to sell, and K agreed to buy a bulk cargo on FOB terms with Vicorus SA ("V") as a broker. The contract required 100% net cash payment within 2 banking days to A's bank upon presentation of a commercial invoice and other documents. Upon completion of cargo loading, A sent emails to K via V on 2 Nov 2015 attaching an invoice and subsequently an amended invoice, for US$1.16 million and seeking K's payment to a bank account maintained at Citibank NA, New York branch (the "**Correct Account**"). V's email records showed that the emails with the invoices were apparently forwarded by V to K on the same day, however what K actually received were emails which *appeared* to come from V, containing payment instructions for remittance via Citibank NA's New York branch *in favour of Citibank NA at its London branch* with different account details purporting to identify A as the beneficiary. It emerged subsequently that the London branch account was in the name of "Ecobank" (the "**Fraudulent Account**"), although there is no suggestion of wrongdoing by Ecobank itself.

For another week or so, A and K exchanged several emails, either via V or directly, dealing with various matters. These emails were manipulated in a similar way to the initial invoices, and the fraud went unnoticed for some time.

K had remitted funds on 5 Nov. Subsequently, on 13 Nov, K emailed A asking for an acknowledgement of receipt of the funds saying that its bank had been told by Citibank New York that the latter had had payment confirmed by the London branch. Citibank London had also requested confirmation from the buyer's side of having performed due diligence in respect of the payment *"as last payment for same beneficiary has been recalled because fraudulent"*.

On discovery of the fraud, investigations showed that the funds were still in the Ecobank account, although K's US$ payment had been converted into Pounds Sterling (for reasons which were not made clear in the case). Arrangements were made to recall the funds from Ecobank and reallocate them to the Correct Account. On 24 Nov, Ecobank approved the debit from their account of £674,831 which was less than the original credited sum of £768,372. It is also not clear from the judgment how this discrepancy came about, but Citibank explained that the difference was due to fluctuations in exchange rates. The funds were transferred to the Correct Account on 18 Dec 2015 valued at about US$1 million, leaving a shortfall from the contractual price of US$161,646, for which A commenced arbitration against K.

Arbitration:

The dispute was heard before a GAFTA First Tier Tribunal and thereafter appealed to the GAFTA Board of Appeal. The former's decision was not considered in the Court case because under the GAFTA arbitration rules an appeal to the Board of Appeal operates as a complete *de novo* rehearing.

The GAFTA Board of Appeal ordered K to pay to A US$161,616 plus interest taking the following issues into account:

1. It was an agreed fact that the invoices received by K providing for payment into the London account were fraudulent and that an email account was likely to have been manipulated.
2. There were disagreements as to where the fraudulent email manipulation had taken place (whether at any of or all the offices or servers of A, K and/or V), which party was at fault for the manipulation and whether any party bore vicarious liability. It was impossible to determine where or how the fraudulent manipulations had taken place. The Board proceeded on the basis that it had to identify the allocation of liability based on risk.
3. The Board considered the emails and invoices sent by A to V containing the Correct Account's details as good notice, since V was acting in its capacity as broker and by reliance on the incorporated contractual provision of GAFTA 119 Clause 18 which states "*…A notice to the Brokers or Agent shall be deemed a notice under this contract*".
4. Therefore, K's duty was to ensure transfer of the full contractual price to the account nominated by A. K should bear the risk of receipt of the incorrect bank details which led to payment into the Fraudulent Account.
5. As a result, A was entitled to (a) the difference between the amount eventually received by A into its own bank account, and the amount invoiced for the goods, as it was a consequence of K's payment into the incorrect account; and (b) interest on the disputed sum and also on the full purchase price for the period between the due date and the date when the monies were received into the Correct Account.

Further Appeal to Court:

K challenged the Award in the English Commercial Court on various grounds available under the Arbitration Act, including that:

1. The Board made an obvious error of law in holding that K had an obligation to ensure payment into A's account at Citibank NA (s.69 "Appeal on Point of Law"). K's obligation, it was argued, was only to pay the fund to A's bank, which was A's agent to receive payment regardless of any account details.

   The Court rejected this argument, deciding that to fulfil a payment obligation transfer instructions should have been accompanied by the account details notified by the seller. It is "commercially impossible" to make a payment without specific bank details including an account name and number, regardless of the fact that technically any payment to a bank account is a payment to the bank of which the customer is a creditor. Upholding K's argument would lead to "a commercially absurd result". Permission to appeal under s. 69 was therefore rejected.
2. The Tribunal's decision of holding V to be K's agent and that notification to V of A's bank account details constituted a notification to K by reliance of clause 18 of GAFTA 119 was seriously irregular because, as accepted by the parties, neither party had raised agency arguments in their submissions and K had been deprived of an opportunity to address the point (s. 68 "Challenging the Award: Serious Irregularity"). Furthermore, it was a substantial injustice for the Board to hold K responsible for the risk which eventuated in A not receiving the price in full, and for making up the difference resulting in the outcome that K's payment obligation ended up being more than the contractual price. Alternatively, the Board's decision was wrong and constituted an error of law (further ground of appeal under s. 69).

The judge decided to remit this matter for reconsideration by the GAFTA Board of Appeal, as he was satisfied that for s.68 purposes, it is sufficient if the Board might well have reached a different view. K was not required to prove that if K had had the opportunity to address its arguments to the Board, the result would necessarily or even probably have been different.

HIGHLIGHTS:

Despite the successful challenge under section 68 of the Arbitration Act, the only relief K was granted was a remission to the GAFTA Board of Appeal to reconsider the Board's reliance on a contractual term with the benefit of submissions from the parties on the point.

This case emphasises the importance of exercising due diligence before remitting payments. The judgment makes it clear that the responsibility for ensuring payments are made to the correct account lies squarely with the paying party, not the payee.

Preventive measures:

Precautionary measures should be taken to ensure payment into the correct bank account. These may include a clear specification of account details in the contract, and verifying (by phone calls instead of emails) and checking the authenticity of any subsequent apparent change of account details.

A number of the Club's members have been affected by frauds of this type, but after contacting the Club immediately on discovering the fraud, and subject to being able to take prompt steps against the bank in the relevant jurisdiction, it has been possible in some of these matters to recover these monies if still in the account to which they had been remitted.

Unless sufficient time is allowed for checking / vetting account details, complications can arise in charterparty contexts as an owner will normally have the right to exercise liens on cargo / hire / freight, suspend performance and/or withdraw the vessel in default of timely hire and/or freight payments. Furthermore, time charter clauses such as 11(d) of NYPE 2015 given the owner the right to suspend performance immediately once hire is outstanding, without the need to tender any grace period notice. It is, therefore, important that hire payments be arranged sufficiently in advance to avoid adverse consequences where there appears to have been a change in account details, so that there is ample time to make necessary verification / checking.

So far there is no proforma charterparty form containing provisions allocating the risk of payment fraud. The newly published "BIMCO Cyber Security Clause 2019" does not purport to address payment fraud but rather situations where a party's own "Digital Environment" is affected by a cyber security incident and that incident affects the ability to perform contractual obligations. As the drafting sub-committee explains, "*[payment fraud] risk will not be greatly reduced through a contractual clause. The fraud is successful mainly due to poor verification and authorisation procedures in companies and can be avoided by tightening internal procedures….*" (see https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/cyber-security-clause-2019).

For a more general discussion of digital risks, including links to Guidelines on Cyber Security and Club Circulars, see the article available on the Steamship website and App and Sea Venture 31 "Cyber Security and Data Protection" https://www.steamshipmutual.com/publications/Articles/cyber-security-data-protection062019.htm

Article by Fiona Li

Syndicate Manager (Claims)

Eastern Syndicate