XXIV BARRISTERS' CHAMBERS

XXIV.CO.UK

Email hacking - who picks up the tab?

Email hacking or business email compromise ("BEC") fraud, as it is more formally known, costs businesses in the UK millions of pounds each year. In 2018 Lloyds Bank reported that the total amount of BEC fraud in the UK had increased by 58% and that 52% of that fraud involved businesses receiving emails that appeared to be from their suppliers. The aim of such emails is to trick buyers into making payments to bank accounts controlled by the fraudsters. Where a BEC attack is successful, an issue arises as to whether liability for the consequent loss should fall on the seller, whose email account may have been hacked, or the buyer, who made the payment to the wrong account. Given the prevalence of this form of fraud and the rate at which it is increasing, there is a surprising dearth of authority in England and Wales regarding liability for losses caused by BEC fraud. This article explores this issue by reference to decisions in other jurisdictions and by reasoning by analogy with other areas of the law.

The contractual position – allocation of risk

Since, one of the primary purposes of a contract is the allocation of risk between the parties, the starting point for any analysis of liability for the loss arising from BEC fraud must be the terms of the contract governing the transaction in question.

Unfortunately, very few commercial contracts presently contain provisions which expressly address the allocation of risk in respect of losses arising from BEC fraud. However, the effect of such a provision was considered by the Superior Court of Justice of Ontario in ***Du v Jameson Bank***, 2017 ONSC 2422. That case concerned a dispute between a bank and its customer over liability for transfers amounting to US$135,000, which were made by the bank on the basis of fraudulent emails sent from the customer's email account (which had been hacked). The court decided that the bank was not liable for the loss resulting from the transfers on the basis that, in the absence of gross negligence or wilful conduct on the part of the bank, the agreement concluded between the parties

STUART ADAIR

allocated the risk of loss arising from "*fraudulent and unauthorized instructions*" to the customer.

Implications of payment to a nominated bank account

Whilst it is rare for a contract to allocate the risk of loss arising from BEC fraud, most contracts will stipulate the manner in which payment is to be made for goods or services. In particular, it is not uncommon for a contract to provide that payment is to be made to the bank account nominated in writing by the seller. Where such a contractual term applies and a fraudster is able to hack the seller's email account and provide fraudulent payment instructions, the following

issues are raised:

· Whether the transfer of funds to the bank account nominated by the fraudster constitutes "payment" for the purposes of the contract; and

· Whether the seller owes a duty of care in respect of the security of its email communications and the payment instructions provided to the buyer

What constitutes payment

In ***Norman v Ricketts*** (1886) 3 TLR 182 a milliner in Bond Street wrote to Mrs Ricketts in Suffolk stating that her account amounted to £142 and "*the favour of a cheque within a week will oblige*". Mrs Ricketts sent a cheque for the full amount by post within the time stipulated, but the cheque was stolen in transit and cashed by the thief. On the milliner claiming payment of the £142 it was held that payment had been made by putting the cheque in the post. Lord Esher MR stated:

> "...if a debtor had to pay his creditor money, as a general rule the debtor must come and pay his creditor. But if the creditor asked him to pay in a particular way, the debtor might do so. If asked to pay through the post, the putting the letter in the post with the money was sufficient. The only question here was whether the plaintiffs asked the defendant in effect to send the money through the post. An express request to send through the post was not necessary. If what the plaintiffs said amounted to a request to send the cheque by post, then there was payment. To answer that question the existing circumstances must be looked at."

The principle laid down in ***Norman v Ricketts*** was applied in ***Thairlwall v The Great North Railway Company*** [1910] 2 KB 509 on the basis that there had been the necessary agreement between the company (acting by its directors) and the shareholders that a dividend would be paid by placing a warrant in the post.

These cases were decided in the late 19th and early 20th centuries in the context of the commercial use of the postal system and it is difficult to see why such principles cannot be applied to email communications, which are the modern equivalent of the post. However, there is a fundamental difference between ***Norman v Ricketts*** and cases of modern BEC fraud. In ***Norman v Ricketts*** there was no doubt that the communication requesting that Mrs Ricketts put a cheque in the post came from the seller. On this basis, a finding that putting the cheque in the post constituted payment, which effectively allocated the risk of the cheque going astray to the seller, makes perfect sense.

In contrast, in a case of BEC fraud the email communication directing that payment be made to a bank account controlled by a fraudster does not come from the seller but from the fraudster, albeit by means of the seller's email account. The key question is whether the contractual term that payment be made to a bank account nominated in writing can equate to the letter from the seller in ***Norman v Ricketts*** and serve to allocate to the seller the risk of the seller's email account being hacked and used to communicate fraudulent payment instructions.

The existence of a duty of care

In ***Young v Grote*** (1827) 4 Bing 253 a husband, Young, who was going away on business left signed blank cheques with his wife for her to fill in to obtain cash to pay employees and any other bills that arose. The wife required £50 2s 3d to pay wages and asked a trusted clerk employed by Young to complete the cheque for that sum. The clerk did so, but in such a way that the figures and words could easily be altered. The clerk subsequently altered the cheque so that it was drawn in the sum of £350 2s 3d, presented it at the bank and absconded with the proceeds. It was held that a customer drawing a cheque owes a duty of care to the bank to take care that it cannot be altered and that, by reason of Young's

negligence, he was liable for the loss suffered.

In ***London Joint Stock Bank Limited v Macmillan*** [1918] AC 777 the facts were very similar to those in ***Young v Grote***. Approving the decision in ***Young v Grote***, Lord Finlay LC stated:

"The ground on which Young v Grote proceeded was, according to the judgment of three out of the four judges, simply this, that if a customer in drawing a cheque neglects reasonable precautions against forgery and forgery ensues, he is liable to make good the loss to the banker and that the fact that a crime intervenes to cause the loss does not make it too remote. Indeed, forgery is the very thing against which the customer is bound to take reasonable precaution...

No one can be certain of preventing forgery, but it is a very simple thing in drawing a cheque to take reasonable and ordinary precautions against forgery. If owing to the neglect of such precautions it is put in the power of any dishonest person to increase the amount by forgery, the customer must bear the loss as between himself and the banker."

Although ***Young v Grote*** and ***London Joint Stock Bank Limited v Macmillan*** were cases dealing with forged cheques and the relationship between a customer and his bank, rather than the position between a seller and a purchaser, there are clear analogies to be drawn. In both cases there is a creditor and debtor relationships and the creditor instructs the debtor to make payment in accordance with written instructions, which have been hijacked and corrupted by a fraudster. On the basis of these authorities, there is clearly a good argument that where a creditor instructs a debtor to make payment in accordance with instructions provided by email, the creditor owes a duty to take reasonable care to ensure that a dishonest person cannot intercept their communications and cause payments to be sent to the wrong bank account. In this regard, it is interesting to note that, in dealing with cases of BEC fraud, courts in the United States have drawn analogies with the law relating to negotiable instruments.

Decisions of the United States Courts

In ***Arrow Truck Sales v Top Quality Truck & Equipment*** 2015 WL 4936272 Arrow agreed to purchase 12 trucks from Top Quality for a price of $570,000. Due to the hacking of the email accounts of both the seller and purchaser, fraudulent instructions were given to Arrow and the purchase price was consequently paid to a bank account controlled by the fraudster. Following a trial, the United States District Court for the Middle District of Florida, Tampa Division, applied by analogy a rule known as the "*imposter rule*", which is derived from section 404(d) of Article 43 of the United States Uniform Commercial Code ("US UCC"), which deals with negotiable instruments and provides that:

"(d) With respect to an instrument to which subsection (a) or (b) applies, if a person paying the instrument or taking it for value or for collection fails to exercise ordinary care in paying or taking the instrument and that failure substantially contributes to loss resulting from payment of the instrument, the person bearing the loss may recover from the person failing to exercise ordinary care to the extent the failure to exercise ordinary care contributed to the loss."

The court had found as a matter of fact that neither party had been negligent in handling their email accounts, but explained the relevance of the "*imposter rule*" as follows:

"The parties informed the Court that they were unable to find a factually similar case. The Court then conducted its own research on the issue and also did not find a factually similar case. However, the Court identified cases in the banking context dealing with third party "imposters" and forged checks that are helpful

to resolve this issue. Under the "imposter rule," the party who was in the best position to prevent the forgery by exercising reasonable care suffers the loss. See, e.g. UCC § 3-404(d); State Sec. Check Cashing, Inc. v. Am. Gen. Fin. Servs., 972 A.2d 882 (Md. App. 2009)."

In ***Beau Townsend Ford Lincoln Inc v Don Hinds Ford Inc***, 759 Fed. Appx. 348 Beau Townsend agreed to sell 20 Ford Explorer vehicles to Don Hinds for a price of US$736,225. However, a fraudster hacked the email account of Beau Townsend and instructed Don Hinds to make payment to a bank account under the fraudster's control. At first instance, the district court granted summary judgment to Beau Townsend on the basis that Don Hinds was in breach of the parties' agreement because it had not paid Beau Townsend for the vehicles. However, having reviewed earlier US authorities, including ***Arrow Truck Sales v Top Quality Truck & Equipment*** and ***Bile v RREMC LLC*** 2016 WL 4487864, the United States Court of Appeals for the Sixth Circuit set aside summary judgment, concluding that the district court had taken "*an overly simplistic view*" and "*failed to adequately analyze this complex issue*". It concluded that there would have to be a trial to determine which party "*was in the best position to prevent the fraud*". In coming to this conclusion, the court referred to the "*imposter rule*", derived from section 404(d) of Article 3 of the US UCC, and also to section 406 of Article 3 of the US UCC, which provides that:

"[a] person whose failure to exercise ordinary care substantially contributes to... the making of a forged signature on an instrument is precluded from asserting [that] forgery against a person who, in good faith, pays the instrument".

It is interesting to note that section 406 of Article 3 of the US UCC echoes the principle underpinning the decisions in ***Young v Grote*** and ***London Joint Stock Bank Limited v Macmillan***.

Decisions of the Canadian Courts

Determining which party was in the best position to prevent the fraud is really just another way of asking which party was properly to be regarded as being responsible for the loss resulting from the fraud and this approach resonates in the decision of the Supreme Court of British Columbia in ***Opus Consulting Group Ltd v Ardenton Capital Corporation***. In this case the plaintiff supplied computer hardware to the defendant buyer and issued two invoices for the total sum of CAN$186,000. The buyer requested electronic payment instructions and the seller provided such instructions by email. However, less than an hour later the buyer received another email, purporting to come from the same person and providing instructions to make payment to a different bank account. The seller had obtained a "pre-judgment garnishing order" and the buyer applied to set that order aside. Mr Justice Mayer set aside the order for technical/ procedural reasons (lack of full and frank disclosure), but added that, even if he had not set the order aside on that basis, he would have done so on the basis that it would be just to do so. He continued:

"[14] ... In that respect I am satisfied that Ardenton has an arguable defence being that Opus was responsible for the issuance of the fraudulent wire transfer instructions.

[15] The question of whether Opus is responsible for not protecting its email system as is alleged, and other potential failings, or whether Ardenton is responsible for complying with a questionable second set of wire transfer instructions in my view qualifies as a serious question to be tried. To be clear, I am not making any findings of fact with respect to the parties' relative responsibilities, either in contract or in negligence. That is a matter to be determined at trial."

St. Lawrence Testing and Inspection Co. Ltd v Lanark Leeds Distribution Ltd, 2019 CanLii 69697 was a decision of Deputy Judge Shane A. Kelford in the Ontario Small Claims Court in Perth and concerned a misdirected payment of CAN$7,000 made pursuant to a settlement agreement. An unknown fraudster hacked the email account of a paralegal employed by the plaintiff's lawyers and sent the defendant fraudulent payment instructions. After considering the decision in ***Du v Jameson Bank***, the deputy judge stated the issue for determination to be to be whether a creditor (Victim A) is liable for the resulting loss where a computer fraudster assumes control of Victim A's email account and causes the debtor (Victim B) to make payment to a bank account controlled by the fraudster. At paragraph 57 of his judgment he answered this question as follows:

"In my view, the answer is "no", unless:

a. Victim A and Victim B are parties to a contract which (i) authorizes Victim B to rely on email instructions from Victim A and, (ii) assuming compliance with the terms of the contract, shifts liability for a loss resulting from fraudulent payment instructions to Victim A;

b. There is evidence of willful misconduct or dishonesty by Victim A; or

c. There is negligence on the part of Victim A."

The decision in ***St. Lawrence Testing and Inspection Co. Ltd v Lanark Leeds Distribution Ltd*** appears to incorporate a presumption that the seller is not liable for the losses unless certain conditions are met, rather than an open-ended determination of where responsibility for the losses lies. In this regard it appears to be out of kilter with the decisions of the United States courts and the Supreme Court of British Columbia.

Contributory negligence

Where a duty of care is owed in tort alone or there are parallel duties in both contract and tort, section 1(1) of the Law Reform (Contributory Negligence) Act 1945 will apply and permit the apportionment of loss by the reduction of the claimant's damages where he "*suffers damage as the result of his own fault and partly of the fault of any other person*". This provision will not come into operation unless the court determines that there is fault on the part of both parties which has caused damage.

In the context of competing arguments regarding which party was responsible for the loss resulting from a BEC fraud, there is ample scope for findings of contributory negligence. Matters amounting to contributory negligence might include a failure to notice and respond to warning signs in fraudulent emails, such as poor English or inconsistencies with earlier emails, or a failure to check or confirm payment instructions by telephone. In particular, a failure on the part of a buyer to follow its own written policies and procedures might be regarded as contributory negligence.

English decisions on BEC fraud

As stated in the introduction to this article, there is a surprising dearth of authority in England and Wales regarding liability for losses resulting from BEC fraud. The writer has only been able to identify two reported decisions which are directly on the point.

Sell Your Car With Us Ltd v Sareen [2019] BCC 1211 concerned an application by the company for an injunction restraining the presentation of a winding up petition by Mr Sareen. The facts were that Mr Sareen had sold a Maserati Levante car through the company and, under the terms of their contract, the company was obliged to pay him £51,800. However, a third party fraudulently intercepted the email exchanges between the company and Mr Sareen and, purporting to be Mr Sareen, directed the company to send £30,000 of the sum due to an account controlled by the fraudster. Mr Sareen served a statutory demand

and threatened to present a winding up petition. The company contended that the debt was disputed on substantial grounds. The grounds relied on were breach of an implied term that Mr Sareen would take reasonable care over the security of his email communications and an implied misrepresentation by Mr Sareen that he had reasonable control over the security of his email communications.

ICC Judge Burton found at paragraph 51 of her judgment that:

> "...the company was alone responsible for sending money to an unauthorised account on instructions received from an unknown third party. The cross-claim, which it asserts, has no prospect of success and falls below the threshold required for me to consider it to be serious, genuine or substantial."

It is notable that the decision of ICC Judge Burton was in remarkably similar terms to the decision of the district court which was set aside in B***eau Townsend Ford Lincoln Inc v Don Hinds Ford Inc.*** However:

- It does not appear that any of the authorities referred to above were cited in argument before ICC Judge Burton. Indeed, from what is said in the judgment, it does not appear that the arguments advanced on behalf of the company went much beyond mere assertions that (a) there must be an implied term in the contract and (b) the company had no reason to believe that the emails it received were not from Mr Sareen; and

- It was material to the ICC Judge's finding that the company was "*alert*" to the risk of fraud and had included in its terms and conditions a procedure which customers were required to follow to change their email contact details. However, the company failed to spot a very small difference in the email address used by the fraudster and failed to follow its own anti-fraud procedures.

J Brazil Road Contractors v Belectric Solar Ltd 2018 WL 01993147 is a decision of HHJ Simpkiss on an appeal from the decision of a district judge. The facts are that the email account of J Brazil was hacked and emails apparently emanating from J Brazil's email account caused Belectric Solar to pay monies due to J Brazil to a bank account controlled by a fraudster. As HHJ Simpkiss states at paragraph 12 of his judgment, the argument advanced before the district judge had been that the email address was the "ostensible agent" of J Brazil and that Solar was entitled to rely on it as such. Counsel tried to raise before HHJ Simpkiss a new estoppel point that had not been argued before the district judge but was not permitted to do so. At paragraph 18 of his judgment HHJ Simpkiss said:

> "District Judge Suh and Deputy District Judge Adams have both approached this on the basis that this is not an agency case. In the circumstances of having rejected one ground of appeal, this is a hacked email and the person communicating through it is neither the claimant nor the claimant's agent. Both the claimant and the defendant are innocent victims of this scam. An email account cannot be an agent."

Although not permitting the new estoppel case to be argued, the judge went on to consider whether an argument based on estoppel had any merit and concluded it did not. In particular, he stated in his judgment that for an estoppel to arise there would have to be a representation and none had been pleaded. Again, it would appear that none of the authorities or arguments referred to above were put to the court and that such arguments as were advanced were not supported by authority.

Agency by estoppel

It is not quite correct to state that for ostensible authority to arise by estoppel a representation is required. As the authors of Bowstead and Reynolds on Agency explain

at paragraphs 2-103 to 2-104 of the 21st edition, agency can arise by estoppel in the absence of any representation by the principal:

> "The courts have also, however, sometimes been willing to see an estoppel based merely on the breach of duty of care by the negligence of a person in facilitating, or failing to take reasonable steps to prevent, situations in which a third party might be led to assume that a person was authorised, even though there was no manifestation that this was so."

It might, therefore, be argued that where the negligence of a seller has allowed a fraudster to take control of the seller's email account and provide fraudulent payment instructions to the buyer, the seller will be estopped from denying that those instructions were provided on its behalf. In ***Beau Townsend Ford Lincoln Inc v Don Hinds Ford Inc*** the United States Court of Appeals for the Sixth Circuit considered that an agency by estoppel argument might be relevant if "*Beau Townsend had failed to exercise ordinary care in maintaining its email server*". However, since both a duty of care and negligence appear to be essential requirements of such an estoppel, it is difficult to see the advantages of such a claim over a straightforward claim in negligence.

Conclusions

In conclusion, it is clear that parties engaging in commercial transactions ought to be taking steps to protect themselves from losses resulting from BEC fraud by:

- Ensuring that their standard terms and conditions and/or the contracts they enter into deal with the allocation of the risk of such losses;

- Reviewing the security of their own email accounts; and

- Putting in place written policies and procedures to minimise the risk of payments being made to fraudulent accounts.

Such steps will not only reduce the risk of such losses being incurred, but also minimise the risk of them being found to be negligent or contributorily negligent in the event that such losses are incurred.

The terms of the contract governing the transaction in question will be key to determining which party will bear any losses resulting from BEC fraud. In the absence of dishonesty or wrongdoing on the part of one of the parties, a term expressly allocating the risk of such losses to one or other party will generally be determinative of the issue. Even if the contract is silent on the allocation of risk, the provisions relating to payment will provide a start point for consideration of any tortious or contractual duties that the parties might owe to each other in relation to emailed payment instructions or the payments themselves.

Whilst there might be an argument that the principle laid down in ***Norman v Ricketts*** applies where a contractual term requires the buyer to make payment to a bank account nominated by email, the courts are more likely to see such a term as giving rise to a duty of care owed by the seller to the buyer in respect of the integrity of its email account and the payment instructions provided by means of that account.

There is, in any event, a strong argument that the principle laid down in ***Young v Grote*** should be applied to payment instructions provided by email. In other words, a seller providing payment instructions to a buyer by email owes the buyer a duty of care to take reasonable precautions to prevent fraud. Such an approach would be consistent with the approach of the United States courts in ***Beau Townsend Ford Lincoln Inc v Don Hinds Ford Inc*** and ***Arrow Truck Sales v Top Quality Truck & Equipment***, which have also drawn on the law relating to cheques to inform their decisions on this issue. Furthermore, through the application of section 1(1) of the Law Reform (Contributory Negligence) Act 1945, such

an approach would allow the court to balance the respective responsibilities of the parties for the losses suffered.

Ultimately, the task of the court is to determine where responsibility for the losses resulting from the BEC fraud should lie. As both the United States courts and the Supreme Court of British Columbia have made clear, this will generally require a trial to determine the facts of the case. Such a trial will inevitably address how the email account in question was hacked, the security procedures in place to prevent hacking and the procedures of the paying party to verify the authenticity of payment instructions. It would not generally be appropriate to determine such issues on a summary judgment application.