TEMPLARS
NIGERIA | GHANA

19 August 2024

TEMPLARS ThoughtLab

Business Email Compromise: Strategies for Prevention & Incident Response

Introduction

Case Study: The Costly Email

Imagine that you are the CFO of a growing commodities trading company that regularly processes large payments to suppliers across the globe. One day, you receive an email from what appears to be the CFO of a supplier company urgently requesting the transfer of the purchase price of the last supply to a new bank account. Given the urgency and your company's delay in paying the invoice, you authorise the transfer without a second thought. A week later, the real CFO inquired about the status of their invoice only for you to discover that the first payment request was fictitious. By then, the USD400,000 has vanished, transferred to an account set up by cybercriminals who had successfully compromised the CFO's email. The company now faces not only a significant financial loss but also potential legal action from stakeholders questioning the adequacy of the company's internal controls.

This scenario highlights the real and growing threat of Business Email Compromise (BEC), an internet email scam that targets businesses and corporations that typically conduct business over the internet and complete payment for goods and services via bank wire transfers. The United States Federal Bureau of Investigation (FBI) has described BEC as the "$26 Billion Scam".

Typically, a victim (usually a member of a business' finance department) would receive an email request from a vendor or supplier to make an expected payment but instructing that the payment be made into a different bank account. Once the victim pays into the fraudulent bank account, the scammers immediately withdraw or transfer funds and disappear. The scam would usually not be noticed until after the legitimate creditor makes another request for payment. At this point, both businesses typically resort to the courts to determine the parties' liability.

Key contacts

Augustine B. Kidisil
Managing Partner and Head,
Dispute Resolution (Ghana)
augustine.kidisil@templars-law.com

Paa Kwame Larbi Asare
Senior Associate,
Dispute Resolution (Ghana)
paakwame.asare@templars-law.com

The scam is usually successful because of the social engineering tactics of the scammers. First, the email would typically come from an email that is closely similar (with slight variations) to the legitimate email address. Second, the scammers might send spear phishing emails to trick victims into revealing confidential information that lets fraudsters have access to company accounts, and data that provides the details scammers need to carry out the BEC scheme. Third, the fraudsters may use malware software to infiltrate company networks and gain access to legitimate email threads about billing and invoices.

What does it mean for your business when you are a victim of a BEC scheme?

The consequences of a BEC can be severe, involving financial losses, legal liabilities, and reputational damage. A business' legal liability depends on that business' involvement in the transaction where a BEC scam has occurred.

For the payer, it is likely that they may be liable to the legitimate creditor to make a second payment to meet their outstanding contractual obligations despite the previous fraudulent payment. In a BEC case of Riepco Ltd v. Zen Petroleum Mali & 5 Others (Suit No. CM/BDC/0417/2018) (delivered by the Commercial High Court, Accra, on 22nd December 2020), the scammers intercepted an email thread between a vendor (Riepco) and a purchaser (Zen Petroleum) and provided the purchaser with new bank details different from the details provided by the vendor. The purchaser paid to the fictitious bank account and sent the SWIFT advice to the vendor. The vendor who received the SWIFT advice did not verify payment and then delivered the goods. About 48 hours later, both parties discovered the fraud when the vendor noticed that the bank account details were wrong, and it had not received payment.

The Ghanaian High Court held that once the vendor had part-performed its contractual obligation for the delivery of lubricants, the purchaser was obliged to pay the contract sum to the vendor although the purchaser had already wired the contract sum to the scammers.

However, the decision of the Ghanaian High Court is not a principle of general application in all courts in Ghana. Being a High Court, its decisions on questions of law are merely persuasive to other Superior Court Judges. For lower courts though, the decisions of the High Court are binding. In that regard, it is useful to add that in other jurisdictions, the courts have considered the duty of care that a creditor may owe to a debtor when providing banking details via email. Considering the prevalence of the BEC scheme, it has been suggested that the vendor owes a duty to the purchaser to issue a fraud alert providing a warning on the risk of a BEC scheme and a two-factor authentication procedure for confirming banking details. One may, therefore, foresee circumstances where a payer may be absolved of the duty to pay the vendor if the vendor did not take adequate measures to communicate payment details in a secure way. The vendor's duty of care has been held to be one of ordinary care and not a heightened threshold.

For a vendor (or a person in the position of a creditor), it is unlikely that the Ghanaian courts will award interest or damages for breach of contract against a payer who is a BEC victim. For instance, in the Riepco Ltd v. Zen Petroleum Mali case, the High Court held that the payer was not liable to pay interest on the outstanding contract sum. The Court reasoned that the non-payment to the vendor was not a deliberate wrongful act by the purchaser as both parties had been negligent. The court found that the payer was

negligent because they ought to have verified the accurate bank details via telephone call when they received conflicting bank details. Conversely, the Court found that the vendor was negligent when the vendor failed to double-check the fictitious SWIFT advice before delivering the goods under the contract. As a result of the vendor's contributory negligence and the absence of deliberate wrongful conduct by the payer, the Court refused the vendor's request for interest and damages for negligent misrepresentation.

A paying bank, in limited circumstances, may also be found liable to their customer for a fraudulent payment. Generally, a paying bank owes a duty of care (ordinary prudent banker) to its customer to refrain from executing a payment order if the banker is put on notice as to the circumstances which lead the banker to believe that there is a possibility that the customer might be defrauded. For a bank to be held liable, the courts would consider very narrow circumstances as to whether the information provided to the bank would lead an ordinary banker to suspect the possibility of a fraud.

What can you do to avoid falling victim to a BEC scheme?

The following strategies may help mitigate the risk of falling victim to a BEC scheme and may also improve your litigation chances if the scheme occurs.

1. **Issue a fraud alert when sending banking details for payment**. For businesses who are expecting wire payments for goods or services, issue a fraud alert together with the banking details warning the payer of the risks of BEC and providing a secondary method of verification (two-factor authentication).
2. **Always confirm banking details via telephone conversation with the issuing officer**. This is especially significant where the payer has received two different banking details for the same transaction.
3. **Train employees on the risks of BEC schemes.** Employees should be trained on social engineering tactics and the actions that can be taken to mitigate BEC risks such as how employees should respond to suspicious email requests, email links, and spoofed email addresses.
4. **Deploy a credible cybersecurity defence program for your computer systems**. This should provide adequate protection against malware software and phishing attempts. Recently, the FBI Internet Crime Complaint Centre issued a public service announcement which reported that the FBI IC3 has received an increase of BEC complaints involving the use of virtual meeting platforms to instruct victims to send unauthorized transfers of funds to fraudulent accounts. Thus, a secure computer system should mitigate the risks of being hacked in similar fashion.

You are already a victim; what are your options in response?

We recommend three (3) strategies below as BEC incident response.

5. **Communication**. Inform relevant stakeholders within and outside the organization about the email compromise. Internally, IT, legal, compliance and management teams should be informed immediately and appropriate cybersecurity protection measures taken to ensure the compromise is contained. Externally, inform regulators who are required to be notified by law and notify clients/customers who may be directly affected by the email compromise. This ensures transparency and trust with stakeholders.

6. **Recovery of wrongful payment from fraudsters**. Generally, a person who makes a payment under a mistake of fact is entitled to the recovery of that sum of money. Practically, this may involve immediately issuing instructions to the paying bank to reverse a payment transaction or suing in the courts for recovery. However, this option is not always available or suitable for victims for various reasons. Firstly, although SWIFT payments are not instant, it takes a while for victims to realize the fraud. Thus, to boost your chances of recovery, one must act quickly within 24 hours to reverse the transaction. Secondly, litigating in the courts can be more cumbersome where the identity of the fraudsters is unknown, or the receiving banks are outside the jurisdiction.
7. **Legal action against defaulting payer**. A vendor who has not received payment may initiate legal proceedings against the payer although that payer may have already wired the contract sum to the scammers. The decision of the courts will revolve around questions of contract law and negligence.