AIG

Payment diversion frauds...

...including supplier bank detail frauds, fraudulent payment instructions and fraudulent bank communications

There are different versions of payment diversion frauds. The main three are supplier bank detail frauds (often referred to as "mandate fraud"), fraudulent payment instructions and fraudulent bank communications.

Firstly, in relation to mandate fraud, a fraudster contacts an employee, usually in the accounts payable department, pretending to be from one of the company's suppliers. The fraudster advises that the supplier's bank details have changed and asks the employee to update the company's records. There are several ways in which fraudsters can initiate false payment instructions. These include hacking into email communications between professionals and their clients or sending false email instructions directly to a company's bank.

Finally, a company may receive communications from a fraudster purporting to be their bank. The fraudster has normally obtained certain details of the company's confidential bank account information and therefore appears credible. This leads an employee to reveal further bank account security details thus enabling the fraudster to make unauthorised online payments.

How do they do it?

The fraudsters behind supplier bank details or mandate frauds typically use publicly available information, including publicly announced contracts, to target supplier accounts on which large payments are likely to be made. Companies' own websites and social media sites can provide details of relevant employees to target as well as supplier names. Information can also be gleaned from telephone calls to unsuspecting employees to obtain information about their procedures or details of contacts.

Frauds involving fraudulent payment instructions often involve fraudsters hacking into the email account either of the Insured or one of their clients or customers. In instances where fraudsters send false email payment instructions directly to the bank, they often obtain and amend a company's similar genuine request to satisfy the bank's procedures. This may be done by accessing old email correspondence with the bank or by using information obtained online. In these instances, if the company can show that they did not send the instruction to the bank, then the bank has prima facie acted in breach of the mandate from the company. In most jurisdictions it is therefore the bank that will sustain the loss, rather than the account holder.

As for fraudulent bank communications, the fraudster dupes a company's employee by providing certain confidential information which leads them to believe that the fraudster is credible. It is not clear how this information is obtained; it is most likely a combination of IT or security breaches, internet research, or possible collusion by a bank employee, although this is rarely proven. Payment diversion frauds including supplier bank detail frauds, fraudulent payment instructions and fraudulent bank communications

What are the common factors that should be looked out for?

If letters or emails are sent to the company, they may have the company logo at the top, often readily available on the internet, but not be on official headed paper.

The letters or emails often contain false contact details so that if the Insured call or email to confirm the change they will contact the fraudsters rather than the genuine supplier. Furthermore, the letters or emails are sometimes written in poor English.

Finally, the address of the recipient bank is often in a location which has no apparent connection with the payee.

If pretending to be from a company's bank, the fraudster may telephone saying that there is a problem with the bank account or with a payment that the company is trying to process. They do so to elicit confidential details from the company such as security details or codes.

Before sending fake instructions to a company, a fraudster will often make so called "pretext" telephone calls to the company to try and get information which will then be used to increase their chances of success. This includes asking for names or direct telephone numbers of people in the accounts payable department, or the supplier reference number for a particular supplier.

How can they be prevented?

There are several steps that businesses can take to prevent these types of frauds, for example:

- Forewarn staff to ensure that those in accounts departments and with responsibility for making payments or accessing the company's bank accounts are familiar with these fraudulent schemes.
- Have a clean desk policy so that important information is tidied away daily when employees are not at their desk.
- Emphasize the importance of following company procedures at all times.
- Before any payment is made to a supplier's new bank account, telephone them to confirm the changes to their bank details.
- Perform a periodic review of changes to supplier bank details.
- Do not accept calls from withheld numbers purporting to be from the bank.
- Record the caller's details including their name and telephone number and call them back.
- Ensure dual control is in place whereby the same employees cannot both post and approve transactions on the banking system.
- Implement a formal data security policy as part of the employee handbook to draw attention to the data that should not be shared by telephone or email. The policy should be regularly reminded to employees by way of training.

AIG®

ASL

ASL are specialist loss adjusters. They have worked closely with AIG and their clients for many years investigating the full spectrum of crime claims including stock losses, employee fraud and social engineering frauds.