UK P&I CLUB

L P Bulletin

Wednesday 28 September 2016

Bulletin 1112 - 09/16 – Cyber Fraud - Worldwide

In December 2014 Signum Services circulated loss prevention advice concerning 'invoice' fraud (bulletin 1014 dated 24.12.16.) These types of crime continue to cause problems and it is worthwhile reminding members to be extra vigilant. Members are advised to ensure that these issues are brought to the attention of their accounts departments.

Sometimes termed 'Mandate Fraud' or 'Payment Diversion Fraud' - the method used is generally the same.
Normally a criminal will hack into the victims email traffic, usually where a payment has recently been requested. A short time after the original email is delivered the fraudster will send a follow up message purporting to be the genuine sender. The fraudster will have made an exact copy of the victim's email format and will have slightly altered the email header, often changing just one letter.
The new email will allege that there is some problem with the account to where payment had originally been requested and ask that the payment is now made to a subsidiary account. This will be one that the fraudster had opened earlier. In some cases fraudster can even use 'Photoshop' software to amend the bank details on invoices that may be attached to emails.
The payment will be made and the transaction will often take several days to come to light. Unfortunately, by this time the funds will have been transferred from the fraudsters account through a series of other banks and lost forever.
Victims often wonder how, in the modern era of secure banking, it may be possible for a criminal to open a bank account in another country and have money paid into it.

Fraudsters can open accounts in several ways and there is a wealth of information on the 'dark web' advising criminals on how to do this. Sometimes corrupt employees are recruited by organised crime gangs to open accounts on fake identification. Even honest bank staff may be unable to carry out checks of identification from overseas, because they simply do not know what to look for. For example, a UK employee is likely to spot a forged UK passport, but may struggle with a Romanian one.

This type of crime is made easier to commit simply because there is actually no need for fraudsters to go through the process of opening an account. It is easy enough to obtain or make a utility bill etc. or to intercept one in the post. Once the criminal has stolen enough information about a person's identity and financial affairs he is able to take over their account or to impersonate them. The fraudster will gain access to their account after getting through security online, at a bank branch or call centre, or by teaming up with someone inside the organisation that holds the account.

'IBAN' type transactions are automated. Due to the huge volumes of payments received each day banks do not perform any checks to ensure that the beneficiary name quoted by the remitter matches the beneficiary account holder's name prior to crediting the account. So long as the remitter has provided the correct beneficiary sort code and account number the funds will always automatically credit the beneficiary account, unless the beneficiary account is closed. If the beneficiary account is closed the funds are returned to the remitter.
These fraudsters operate internationally across multiple police jurisdictions, making it very difficult for national law enforcement agencies to combat such crimes and making any post incident recovery of funds virtually impossible.
Bearing all this in mind we advise members to exercise high levels of alertness and to avoid compliancy. We recommend that in all instances where an unusual request for payment of funds is received that staff

double check the veracity of the request. Ideally this will be done by speaking in person with the original sender, so long as you are certain it's not the fraudster you are talking to….!!.
For any further advice please contact Signum Services.

Our Members can also find of interest the following article, recently published by the TT Club:
http://www.ttclub.com/loss-prevention/tt-talk/article/tt-talk-mandate-fraud-133885/

Source of Information

David J. Thompson
Signum Services
Thomas Miller P&I (Europe) Ltd. Department
Telephone: +44 20 7283 5616