Circular Ref No.:PNI1805

Date: 16 March 2018

Dear Sir or Madam,

Subject: Email Fraud Alert!!!

Email fraud cases have been noted and reported very frequently recently, where fraudsters pretend themselves to be claim handlers of either Club, member, correspondent or broker, etc. requesting to remit funds to their designated bank account in disguise. They either hack into the email correspondences of a claim and then take up from a certain point writing to Club or member who is guardlessly ready to pay a payment following the normal sequence of claim handling, sending from a disguised email address and providing a fake bank account. Sometimes, they even make up a claim out of blue sending emails to Clubs or members, disguised as correspondent, cargo owner or insurer, or other claimants. In other cases, they pretend to be any of the above parties spreading emails with virus-bedded attachments, in order to hack into the receivers' email systems.

The fraudsters are so professional with these tricks and familiar with the shipping and insurance business that from time to time there are unfortunate victims to these predators. As such, we consider it necessary to call on high attention and caution to these fraud activities to avoid losses or troubles.

E-mail Address of Fraudsters
They usually imitate the e-mail address by adding extra letters or copying some part of the real ones. Below are some examples:
pni.sh.huatai-serv.com@list.ru
smartq_adrnin_hkg.qbe.com@list.ru
chenxiuyun.tnzconsult.com@list.ru
However, it is worthwhile to point out that in some cases though rare, they would somehow disguise the sending email address to be identical to the real one, so as to catch readers off guard.

Bank Account

Fraudsters will nominate a bank account to receive the payment pretending as the intended fund receiver. They either write secretly to the paying party in disguised email addresses, or they would send out an email after the real bank account has been sent out by the intended fund receiver, alleging that there has been a problem (such as auditing) with the previously sent bank account and that the fund should be sent to their nominated new account.

Recommendations

Email fraud rampancy has become an increasingly serious problem in shipping industry. To protect the interests of our clients, we would like to draw the attention of the readers to the following:

1) Please check the email addresses of the senders. Most of the fraud emails are sent from addresses that are different from the real ones, which can usually be easily detected. By doing this, you will be able to screen most of the fraud emails.

However, please note that even if the email address appears correct, it doesn't mean that the email is one hundred percent safe; that's why the following points are even more important.

2) When payment or remittance is to be made, extra care should be taken. Please make sure that you will telephone the intended receiving party in person to verify the bank account, should account details be found suspicious, especially when the fund is requested to be remitted into a revised bank account.

For the sake of caution, please find our one and only bank account details as follows for your record, which remains unchanged:
Beneficiary: Huatai Insurance Agency & Consultant Service Ltd.
Name of Bank: Bank of China, Beijing Jin Rong Jie Sub-branch
Address of Bank: 27 Jinrongjie, Xicheng District, Beijing, China.
Account No.(USD): 342856024291
Swift Code: BKCHCNBJ110

3) If possible please increase the security level of the email settings including password, logging record monitoring, etc. and update the anti-virus systems timely.

In fight against these rampant email fraudsters, we are upgrading our email security system, calling on serious caution from each and every member of our team, and also, issuing this circular to alert you of this issue, in the hope that with our combined effort and attention, no one of us will fall prey to these fraud again.

Any queries, please feel free to contact us.

Best regards

Yu Limin
President