DORSEY
DORSEY + WHITNEY LLP

Hong Kong Email Wire Fraud Epidemic - How to retrieve funds and prevent wire fraud

by Steven C. Nelson and Janet Wong

Related People

- Steven C. Nelson
- Janet Wong

Related Capabilities

- International Arbitration & Litigation
- Financial Services Regulatory
- Privacy & Social Media
- Anti-Corruption
- Asia-Pacific
- China

Over the Lunar New Year period, we observed a spate of email wire frauds (or 'business email scams') which involve funds being wired internationally to bank accounts in Hong Kong. The amounts transferred vary from a few hundred thousand US dollars to millions of US dollars. The most prevalent method of perpetrating an email wire fraud simply occurs by deceiving an accounts manager, or someone else within an organisation with authority to order a wire transfer, to do so. The prevalence of wire frauds in Hong Kong has even prompted the Hong Kong Police to publish a notice on its website warning people to beware of the 'CEO email scam' where fraudsters pretending to be senior management officials of companies send fictitious but artfully-crafted emails to induce staff to transfer company funds to bank accounts controlled by the fraudsters.[1]

What to do immediately after discovering the fraud

1. Contact your initiating bank and seek an immediate reversal of the wire. If that is not possible, ask them to contact the beneficiary bank to notify them of the wire fraud and to request that the account be frozen.
2. File a police report in the jurisdiction in which the funds were transferred. If the money has been wired to a bank in Hong Kong, which seems to be the most common destination, a police report may be filed online here: https://secure1.info.gov.hk/police/eforms/report_cyber_crime_en.php.
3. If the fraud has occurred due to a hacking incident or other IT security breach, as is frequently the case, take steps to ensure the threat has been removed.
4. Seek legal advice in the jurisdiction to which the funds were transferred. If that is Hong Kong, we are glad to advise you on the best legal course of action to recover the funds, which may involve obtaining Court orders to freeze the fraudster's account.
5. We recommend writing a chronology of events that led to the wire fraud and collating copies of the fraudulent emails so that they can be readily sent to the police, relevant banks and lawyers.

Time is of the essence. It is important to carry out the above steps quickly as possible as the fraudsters will try to withdraw or transfer the funds out of the account just as fast as you are trying to stop the process.

Preventing wire fraud

To help prevent a wire fraud, those who have authority to execute wire transfers should be cautioned to be on the lookout for:

- requests ostensibly received from colleagues for transfers to unknown beneficiaries;
- requests for transfers to international bank accounts, especially in Hong Kong, China and Singapore;
- unusual "extremely urgent" requests for payments or other requests to expedite a wire transfer;
- missing information about the transfer, such as the account from which the funds should be transferred, the expense account to which the transfer should be recorded and/or the reasons for the transfer;
- email addresses from a known person which are from a different or unusual email account, bearing in mind that difficult-to-detect changes can be made to a legitimate e-mail address; and
- emails with unusually poor spelling and grammar.

Other ways to reduce the likelihood of falling victim to wire fraud include requiring two people within an organisation to authorise a wire transfer of over a certain amount; or requiring telephone or in-person confirmation of email requests to execute such wire transfers.

For a detailed review of email wire fraud and business email scams, please see our *Guide to Protecting Against Email Wire Fraud Scams and Recovering Funds Wired to Hong Kong* here.

[1] http://www.police.gov.hk/ppp_en/04_crime_matters/ccb/fst.php?msg_id=cct_30