



To JMB Insurance Clients

Urgent Risk Control Bulletin – Electronic Funds Transfer Fraud Schemes

JMB Insurance would like to alert you of an increasing incidence of fraudulent scams involving Wire Transfers and Automatic Clearing House (“ACH”) disbursements. You and your business partners could be at risk.

Hackers are “spoofing” email domains or are infiltrating corporate email systems and sending fraudulent email communications, purportedly from a known vendor or business partner to a target company. These emails generally contain fraudulent information about a change in electronic remittance protocols, including new banking information with respect to Wire Transfers or ACH remittances. These emails almost always appear to originate from a known contact at a vendor or business partner.

By the time the party remitting funds electronically becomes aware that the request was fraudulent, the funds have already been transferred, typically to an overseas bank. This fraud is often successful because the banking change request appears to be received from a recognized business partner with knowledge of the relationship, and often under the name of someone who is personally known.

We strongly recommend that you immediately institute a risk control practice of verifying all requests received from a client or business partner for transfer of funds to a new or different bank (if not a different bank, a different/new account number at the same bank). Call and speak personally with your contact and confirm that the request is authentic. This will go a long way towards ensuring you are not a victim of this type of fraud.

At JMB Insurance we give considerable thought to the risks and exposures that our clients encounter on an ongoing basis, especially in this fast-moving, constantly evolving and challenging electronic world in which we now live. Please do not hesitate to contact us if you have any questions.