Impersonation Fraud – It Could Happen to You!
By Dennis M. Tsonis, CPCU, Lovitt & Touche

An employee who has authority to process wire transfer requests receives an email from their CEO, requesting them to wire funds for an acquisition they have been working on. Everything appears normal, so the employee makes the request of the bank and the funds are transferred. It then becomes evident that the email from the CEO was not actually sent by the CEO. The bank is contacted but informs the employee that the transfer request they made is not fraudulent, as they have the authority to make such requests. The bank is not responsible for the funds and the company has now suffered a financial loss due to the fraudulent impersonation of the CEO.

Impersonation fraud is nothing new. Everyone has heard of the Trojan horse myth, or probably received an email from a Nigerian Prince who wanted to entrust you to handle his financial matters for a sizable payment. These schemes rely on human emotion and interaction to exploit weakness in our nature to trick us to let down our guard out of a sense of duty, for a reward, or out of complacency. While computers offer greater means to control and automate many processes, when it comes to electronic communications, such as email, they allow criminals the ability to easily impersonate someone of authority to cause us to willingly part with our, or our company's, hard earned money.

A world-wide trend is occurring where businesses are being targeted by organized fraudsters in a number of impersonation scams. According to the Association for Financial Professionals 2014 Payments Fraud and Controls Report, 62% of organizations in the United States were exposed to actual or attempted payments fraud in 2014. Some cases have resulted in multi-million dollar losses and pose significant threats to businesses that fail to take measures to protect themselves.

This type of threat is also known as "Social Engineering Fraud", which is defined as a non-technical method of intrusion hackers use to gain access to buildings, systems or data by using the art of psychology to exploit human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations encounter today.

Impersonation Fraud typically takes two forms: 1) Fake CEO Scams or 2) Vendor/Client Scams. A "Fake CEO Scam" is when the fraudster impersonates the company director, CEO, CFO or similar, and instructs a member of the company's finance department to transfer funds with respect to a discreet and/or sensitive acquisition, either of another business, or commercial property. This typically takes the form of an email that appears legitimate. We have seen a number of these instances recently with our clients. "Vendor/Client Scams" are when someone impersonates a supplier you have an existing relationship with, and provide alternate bank details with respect to a genuine invoice, which may have been altered. Fraudsters also impersonate genuine retailers or wholesalers and place large orders for goods with suppliers

who may or may not have an existing relationship with the impersonated company. The goods are ordered on a credit basis and either delivered or redirected to an address accessible to the suspects, or in some cases, collected directly by the fraudsters. The fraudsters then sell the product, often back into genuine supply chains, or to the public.

With the recent global upsurge in these types of scams, companies of all sizes and sectors are at risk. It is imperative that companies understand this risk and take adequate measures to educate employees on how to identify and avoid the scam AND to transfer this risk to an insurance product in order to avoid potential losses.

The Insurance Services Office (ISO), who writes the standard insurance policy forms that many insurance companies use, has recently introduced new "Fraudulent Impersonation" coverage that is available as an endorsement to a Commercial Crime policy. A number of insurance companies have also come out with their own proprietary coverage forms to address this growing risk. These new policy forms generally include coverage for two types of fraud:

> "Fraudulent Impersonation of Employees" covers losses directly resulting from having, in good faith, transferred money, securities or other property in reliance upon a transfer instruction purportedly issued by an employee, or any of the insured's partners, members, managers, officers, directors or trustees.
>
> "Fraudulent Impersonation Of Customers And Vendors" covers losses directly resulting from having, in good faith, transferred money, securities or other property in reliance upon a transfer instruction purportedly issued by a customer or vendor with whom the you have a written contract, but which transfer instruction proves to have been fraudulently issued by an imposter without the knowledge or consent of the customer or vendor.

Detailed specific applications are required to obtain a quote for this insurance. As is the case with other specialty lines of coverage, completing the application is a good way to see if you already have the right internal controls in place to prevent a claim. If you answer "no" to too many of the questions, you may not be considered an acceptable risk by the underwriter and they won't offer a quote or you won't like the premium.

Here are some of the controls you should consider implementing to reduce your risk for impersonation fraud:

- Have a procedure in place to verify new customers or clients prior to initiating any financial transaction with them. Examples include: a D&B Report or other credit worthiness check, bank account verification (name, address, contact info matching customer file), confirmation of physical address, etc.

- If you accept funds transfer instructions from clients & co-workers over the telephone, email, text message or similar method of communication, prior to complying with the instruction you should authenticate such instructions by calling the customer/co-worker at a predetermined number, sending a text message to a predetermined number, requiring receipt of a code known only to the customer/coworker to confirm identity.
- Verify all vendor/supplier bank accounts by a direct call to the receiving bank, prior to being established in the accounts payable system.
- Confirm all changes to vendor/supplier details (including routing numbers, account numbers, telephone numbers and contact information) by a direct call using only the contact number previously provided by the vendor/supplier before the request was received.
- Send all confirmations of changes requested by the vendor/supplier to a person independent of the requestor of the change, with any changes being implemented only after the vendor/supplier has the opportunity to challenge them.
- Require review of all changes to vendor/supplier records by a supervisor or next-level approver before any change to the record is processed.
- Run exception reports, either automatic, or manually created, showing all changes to the standing data of vendors/suppliers.
- If funds have been paid out as a result of the scam, contact your bank and the beneficiary bank as soon as possible, so that they can attempt to prevent the onward dispersal of the funds.
- Ensure your computer antivirus software is up-to-date and that your staff receives regular reminders and training with respect to the on-going threats from malware and phishing emails, including social network invitations.
- Consider what your business makes publically available, with respect to existing contracts and suppliers. Evaluate whether it is really necessary to publish information of this type in the public domain, given that it is also available to fraudsters.
- Ensure that all of your members of staff are aware of these scams and of the relevant security protocols in place to identify and prevent them.

This can happen to you. Don't be a modern-day victim of the Trojan Horse. Educate your staff, strengthen your fraud prevention policies and consider purchasing insurance coverage for Impersonation Fraud.

Dennis is a Senior Vice President with Lovitt & Touché, Inc., one of the nation's 100 largest insurance brokerages. As their Construction Practice Leader, Dennis leads a team of construction insurance experts in serving the insurance and risk management needs of contractors, A&Es, developers and suppliers. Dennis is also a graduate of the Arizona Builders Alliance – Leadership Development Forum. He can be reached at 602-778-7027 or dtsonis@lovitt-touche.com.