AmWINS Group, Inc.

CLIENT ADVISORY

ENDORSEMENTS THAT PROTECT YOUR CLIENTS FROM SOCIAL ENGINEERING LOSSES

In recent years, hackers and cyber-thieves have been developing new techniques to infiltrate insureds' bank accounts. Early phishing scams were fairly easy to spot: a request from a Nigerian prince or a link purported to take you to your bank's customer service center were tell-tale signs of suspicious email traffic. It was recommended to never click on the link and delete the email immediately. In response to the masses becoming more aware of these red flags, thieves have countered with more sophisticated attacks, such as CEO Fraud, also known as **Social Engineering Fraud**. Social engineering is defined as "psychological manipulation of people into performing actions or divulging confidential information." [1]

HERE ARE SOME EXAMPLES OF WHAT CEO FRAUD OR SOCIAL ENGINEERING FRAUD MIGHT LOOK LIKE:

Example #1

An email, purportedly from the CEO, is sent to the firm's accounting department authorizing an urgent payment to a new vendor with a bogus bank account number. Not wanting to disappoint the CEO, the amount is transferred only to find out the CEO never requested any new vendor payments. Hackers might follow a CEO or CFO's social media posts to see when they are traveling to make verbal confirmation more difficult for the target.

Example #2

After months of monitoring transactions from accounts payable to a foreign vendor, hackers create a fake email address that is similar to that of the foreign vendor. They then use the fake email address to inform an accounts payable representative that the bank account number has changed and to please send payment to the new account number. Often, the company will only be aware of these fraudulent payments when the real vendor follows up for payment. By then the money is unrecoverable.

As of April 2016, the FBI has estimated that CEO Fraud has cost businesses $2.3 billion. In an effort to recoup these losses, insureds are looking to their crime policies for reimbursement for their losses. Specifically, they are looking to the **Funds Transfer Fraud** *("The company shall pay the parent organization for direct loss of money sustained by an insured resulting from funds transfer fraud committed by a third party")* and **Computer Fraud** *("The company shall pay the parent organization for direct loss of money sustained by an insured resulting from computer fraud committed by a third party")* insuring agreements.

Unfortunately, under the CEO Fraud scenario, funds are transferred willingly, with the insured's knowledge; therefore, claims are declined under the Funds Transfer Fraud insuring agreement. Similarly, under the Computer Fraud insuring agreement, the carrier can argue that coverage has not been triggered as the fraudulent payment instructions came into the company via email, *and email by its nature is an authorized entry*. Another method used is the **Voluntary Parting Exclusion**, which excludes coverage when an insured willfully parts with title to, or possession of, any property.

(continued on next page)

CONTACT

To learn more about how AmWINS can help you place coverage for your clients, reach out to your local AmWINS broker or marketing@amwins.com.

ENDORSEMENTS THAT PROTECT YOUR CLIENTS FROM SOCIAL ENGINEERING LOSSES

(*continued from previous page)*

Cyber carriers are beginning to offer policy enhancement endorsements that affirm sublimited coverage for CEO Fraud or Social Engineering Fraud. The wording to look for which confirms coverage may look similar to this:

> *"The Insurer will pay the **Insured Entity** for **Social Engineering Fraud Loss** resulting directly from a **Social Engineering Fraud Event**, in excess of the applicable retention and within the applicable Limits of Insurance.*
>
> *It is a condition precedent to coverage under the **Social Engineering Fraud** Coverage that the **Insured** attempted to **Authenticate** the **Fraudulent Instruction** prior to transferring any **Money** or **Securities**."*

How we do we address this increasing risk as an industry? Traction is gaining and more carriers are beginning to extend coverage by endorsement, albeit under sublimits, in both Crime and Cyber lines. Even these small improvements show signs of progress in the industry. By discussing this issue with insureds, retail agents and brokers can provide added value by urging them to educate their employees and set protocols for verifying large or frequent transfers.

This article was co-authored by Brandyn Surprenant and Mikkel Vogele of AmWINS Brokerage in Chicago, Illinois.

[1] https://en.wikipedia.org/wiki/Social_engineering_(security)