Privacy and Data Security Alert: Insurance Coverage for Social Engineering Attacks

February 4, 2016

Social engineering attacks have evolved to become one of the greatest cyber threats to businesses. From humble beginnings like the infamous "Nigerian prince" scams, these attacks have grown into sophisticated assaults based on the psychological manipulation of people to take action or disclose confidential information. Social engineering attacks are varied and those that are email-based often fall in a category called "phishing". Unlike hacking, these attacks exploit humans, not computer systems.

The most recent social engineering attack is called the "Business E-Mail Compromise" (BEC) or "CEO fraud." This scam lures a corporate employee to transfer funds via ACH or wire to an account held at another bank (either domestic or foreign). These funds are then typically immediately transferred to accounts at yet other banks that are located outside the U.S. or withdrawn. The instruction to the corporate employee is typically sent by a fraudster posing as the CEO or other senior corporate executive.

Last year, for example, Ubiquiti Networks, a manufacturer of networking technology, reported to the SEC that it had been the victim of a criminal fraud. The company said that the "incident involved employee impersonation and fraudulent requests from an outside entity targeting the Company's finance department." The fraud resulted in the transfer of $46.7 million held by a Hong Kong subsidiary to other overseas accounts held by third parties. The company recovered $14.9 million but is still pursuing recovery of the remaining $31.8 million.

Last August, the FBI warned that BEC is "a growing financial fraud that is more sophisticated than any similar scam the FBI has seen before and one—in its various forms—that has resulted in actual and attempted losses of more than a billion dollars worldwide." The FBI reported that since the beginning of 2015 there has been a 270 percent increase in identified BEC victims. The FBI warning noted that "the criminals often employ malware to infiltrate company networks, gaining access to legitimate e-mail threads about billing and invoices they can use to ensure the suspicions of an accountant or financial officer aren't raised when a fraudulent wire transfer is required."

It is important for all businesses to adopt appropriate internal controls to help reduce the risk of unauthorized wire or ACH funds transfers. Most basic is assessing whether emailed instructions for funds transfers are appropriate without a secondary level approval or other form of internal confirmation. Of

course, such confirmation should not be by email to the person purportedly originating the instruction. Businesses should also discuss security procedures that are available at their financial institutions. There will typically be options available requiring additional approval based on the amount of a transfer instruction or the recipient of the payment.

Victims of social engineering fraud usually make claims under the computer fraud or funds transfer fraud coverages in their crime or fidelity bond policies. Insurers are resisting these claims on the grounds that the loss was caused by a social engineering ploy (to which computer use was, at most, incidental), not a computer fraud. The results so far have been mixed, as illustrated by two recent cases.

In *Apache Corp. v. Great American Ins. Co.*, 2015 WL 7709584, (S.D. Tex. Aug.7, 2015), an Apache accounts payable employee received a call from a fraudster claiming to be an employee of a vendor who did work for Apache. The caller requested that the vendor be allowed to change its account information where payment was sent for services rendered. The Apache employee told the imposter that the request had to come on the vendor's letterhead. A few days later, Apache accounts payable received an email with an attachment on the vendor's letterhead requesting the change in account information. The request was routed to another Apache employee who called the number on the letterhead to verify the information in the email. Once the information had been verified, the change request was made. Thereafter, $2.4 million was directed to the "new" account.

After discovering the loss, Apache made a claim under the "Computer Fraud" coverage in its crime policy. The computer fraud section covers loss of money "resulting directly from the use of any computer to fraudulently cause a transfer" of money from inside the premises to a person or place outside those premises. Apache argued that the fraudulent email sent by the fraudster qualified as computer fraud under the policy. The insurer argued that because of the human intervention that took place between the fraudulent email and the actual loss, the language "resulting directly from" removed the loss from coverage under the policy. The court disagreed with the insurer and held that despite "human involvement" that followed the fraud, the loss still resulted directly from computer fraud (*i.e.,* the email requesting Apache to disburse payments to a fraudulent account).

The Court of Appeals of New York came to a different conclusion in *Universal American Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*, 37 N.E.3d 78, 16 N.Y.S.3d 21, 25 N.Y.3d 675 (2015). Universal, a health care insurer offering Medicare Advantage plans, used a computerized billing system that allowed health care providers to submit claims directly to the system. The majority of the claims were processed, approved, and paid automatically without manual review. Universal suffered $18 million in losses for payment of fraudulent claims for medical services that were never performed. Universal made a claim under the "Computer System Fraud" rider on its financial institution bond. The rider provided coverage for any "loss resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program into, or (2) change of Electronic Data or

Computer Program within the Insured's proprietary Computer System …." The court concluded that "fraudulent" modifies "entry" or "change" of electronic data or a computer program. The word placement of "fraudulent" before "entry" or "change" means that the rider only provided coverage for a violation of the integrity of computer system through deceitful or dishonest acts (*i.e.,* hacking). The rider therefore did not cover losses resulting from fraudulent content submitted to the computer system by authorized users.

As these cases demonstrate, coverage for a social engineering loss will depend on the policy language and the facts surrounding the loss. Policyholders therefore need to carefully scrutinize all coverage grants and vigorously pursue claims where appropriate.

Some insurers offer limited coverage for social engineering attacks by way of endorsements to crime policies or cybersecurity policies (variously called "Fraudulent Instruction Coverage," "Payment Instruction Fraud," "Deception Fraud," or "Social Engineering Fraud").

Unfortunately, this coverage is usually subject to a low sublimit, so the full policy limits are not available for this type of loss. There may be other restrictions, such as an exclusion for any fraudulent instruction that was not verified with the requestor using an "Out-Of-Band Authentication." So, for example, if the request comes in by email (band one), the recipient would need to move the verification to the next tier by either texting the person who sent the email (band two) or calling him or her directly (band three) to verify the information.

As noted above, it is important for businesses to employ appropriate internal controls. In particular, if the policyholder does not utilize Out-Of-Band Authentication (and many don't), there may be no coverage at all. As always, it is very important that the policyholder fully understands the scope of coverage and exclusions in order to avoid surprises when a loss occurs.