HINSHAW

Alerts

Computer Fraud and Funds Transfer Fraud Coverages Not Triggered by Social Engineering Phishing Scam

March 2, 2020
Insights for Insurers: Cyber Coverage

A Mississippi federal district court became the latest to rule that Computer Fraud Transfer and Funds Transfer Fraud coverages were not applicable to losses resulting from an email phishing scam. In *Miss. Silicon Holdings, LLC v. Axis Ins. Co., 2020 U.S. Dist. LEXIS 29967 (N.D. Miss. 2020),* Mississippi Silicon Holdings, LLC (MSH) had fallen prey to spoofed emails and wired more than $1 million to fraudsters instead of a legitimate MSH vendor. Three MSH employees approved both of the wire transfers at issue before MSH learned that hackers had infiltrated its computer system and impersonated an authentic vendor.

MSH tendered a claim for the loss to Axis Insurance Company, which determined that the loss was covered by the Social Engineering provision of the management liability policy issued to MSH, but not by the Computer Fraud Transfer and Funds Transfer Fraud coverage grants. Axis then mailed MSH a check for $100,000, the full limit of the policy's Social Engineering coverage. MSH returned the check and instituted coverage litigation, alleging the loss fell within all three of the Axis coverages at issue.

Relevant Coverage Grants

The parties did not dispute that MSH's claim was covered by the policy's Social Engineering Fraud provision, which stated:

The Insurer will pay for loss of **Money** or **Securities** resulting directly from the transfer, payment, or delivery of **Money** or **Securities** from the **Premises** or a Transfer Account to a person, place, or account beyond the **Insured Entity's** control by:

a. an **Employee** acting in good faith reliance upon a telephone, written, or electronic instruction that purported to be a **Transfer Instruction** but, in fact, was not issued by a **Client**, **Employee** or **Vendor**; or

b. a **Financial Institution** as instructed by an **Employee** acting in good faith reliance upon a telephone, written, or electronic instruction that purported to be a **Transfer Instruction** but in fact, was not issued by a **Client**, **Employee** or **Vendor**.

Attorneys

Scott M. Seaman

The parties did dispute, however, whether or not the following coverages also applied to MSH's claim:

Computer Transfer Fraud

The Insurer will pay for loss of or loss from damage to **Covered Property** resulting directly from **Computer Transfer Fraud** that causes the transfer, payment, or delivery of **Covered Property** from the **Premises** or **Transfer Account** to a person, place, or account beyond the **Insured Entity's** control, without the **Insured Entity's** knowledge or consent.

Funds Transfer Fraud

The insurer will pay for loss of **Money** or **Securities** resulting directly from the transfer of **Money** or **Securities** from a **Transfer Account** to a person, place, or account beyond the **Insured Entity's** control, by a **Financial Institution** that relied upon a written, electronic, telegraphic, cable, or teletype instruction that purported to be a **Transfer Instruction** but, in fact, was issued without the **Insured Entity's** knowledge or consent.

Both of those coverages were subject to a $1 million policy limit.

Computer Transfer Fraud Coverage

AXIS contended that this coverage was not implicated because "nothing 'entered' into or 'altered' within [MSH's] Computer System . . . directly caused the transfer of any Money." Instead, three MSH employees caused the transfer. Because the fraudulent emails did not themselves manipulate MSH's computer system, a "Computer Transfer Fraud" did not directly cause the transfers. MSH urged the court to instead apply a proximate cause test and find that the fraudulent emails were the dominant and efficient cause of the loss.

Focusing on the term "directly" in the coverage grant, the court rejected MSH's argument and stated:

While the Court recognizes and appreciates MSH's argument in favor of a 'proximate cause' standard, it cannot be ignored that the provision itself specifically requires that the fraudulent act directly cause the loss. And it further cannot be ignored that MSH's employees, not the fraudulent emails themselves, actually initiated the transfer. If a proximate cause standard or some other more expansive coverage was intended, that language undoubtedly could have been included in the Policy. However, it was not.

In addition, the court held that the requirement for the transfer to take place "without the **Insured Entity's** knowledge or consent" was not satisfied. In doing so, the court rejected MSH's assertion that a more logical reading of the requirement would be that MSH had to have actual knowledge of material facts, such as the transferee's true identity, or consent to the transfer in light of the true facts and circumstances. The court held that the policy provision was clear and unambiguous, and MSH provided no legitimate reason to impose a heightened requirement into the policy, other than its own desire to modify the policy terms.

Further, the court noted, the policy's Social Engineering Fraud provision "cleary authorizes coverage when an employee relies on information that is later determined to be false or fraudulent. In contrast, the Computer Transfer Fraud provision, rather than specifically extending coverage when employee in good faith relies upon fraudulent information and inflicts a loss, specifically states that coverage is only available when the loss occurs 'without the insured entities knowledge or consent.''

While explaining that it need not look beyond the four corners of the Axis policy to decide the coverage questions at issue, the court favorably cited the Fifth Circuit's analysis of a computer fraud provision in *Apache Corp. v. Great American Ins. Co., 662 F. App'x 252 (5th Cir. 2016)*:

Here, as in *Apache*, the transfer of funds was initiated and authorized by an employee of MSH. And as noted by the Fifth Circuit in *Apache*, an application of a 'computer fraud' insurance provision in circumstances where in employee explicitly authorizes the subject transfer in response to an email would effectively convert all provisions of this type into general fraud provisions, especially considering that a large percentage of fraudulent schemes will likely involve a computer in one

way or another. Like the Fifth Circuit in *Apache*, this Court declines such an expansive interpretation of this type of provision, particularly considering the Policy's clear and unambiguous language to the contrary.

Ultimately, MSH's position, similar to the argument made by the plaintiff in *Apache*, ignores the plain and unambiguous language and intent of the subject provisions and should not be traditionally sanctioned.

The court also held that the Funds Transfer Fraud coverage was not triggered because the three MSH employees had knowledge of, and consented to, the transfers. The court found no legitimate basis to accept MSH's argument that the policy required those MSH employees to know that the spoofed emails were fraudulent at the time of the transfers.