

Mississippi Court Rules That Email Phishing Claims Are Not Covered By Computer Transfer Fraud Or Funds Transfer Coverage Provisions

04.23.20



(Article from *Insurance Law Alert*, April 2020)

For more information, please visit the [Insurance Law Alert Resource Center](#).

A Mississippi federal district court ruled that losses stemming from wire transfers initiated by spoofed emails were not covered by Computer Transfer Fraud or Funds Transfer coverage provisions. *Miss. Silicon Holdings, LLC v. AXIS Ins. Co.*, 2020 WL 869974 (N.D. Miss. Feb. 21, 2020).

An employee of MSH, a manufacturing company, received an email purportedly from one of its suppliers, directing it to change banking information for future payments. In accordance with that email, the MSH employee electronically changed the information and initiated a wire transfer in the amount of \$250,030. Another MSH employee authorized the transfer and following a confirmation call from the bank, a third MSH employee verbally authorized the transfer. A second payment of \$775,851.13 was made, following the same three-step authorization process. Shortly thereafter, MSH discovered that the emails were fraudulent and that the funds had been sent to hackers' bank accounts. Axis Insurance paid MSH the \$100,000 limit under a Social Engineering Fraud clause. MSH returned payment and filed suit, alleging it was entitled to coverage under the Computer Transfer Fraud and Funds Transfer provisions. The court granted Axis Insurance's summary judgment motion, finding that neither provision encompassed the underlying claims.

The Computer Transfer Fraud provision covered loss "resulting directly from Computer Transfer Fraud that causes the transfer, payment or delivery of Covered Property . . . without the Insured Entity's knowledge or consent." Computer Transfer Fraud, in turn, was defined as "the fraudulent entry of Information into or the fraudulent alteration of any Information within a Computer System." The court ruled that the losses did not "result directly" from the fraudulent emails. The court explained that while the emails "set in motion a series of events which ultimately led to the loss," the affirmative conduct of the MSH employees was responsible for the account change and wire transfer.

In addition, the court ruled that there was no Computer Transfer Fraud coverage because the transfers did not occur without MSH's "knowledge or consent" given that three employees explicitly authorized and effectuated the wire transfers. The court rejected MSH's contention that coverage was intended to apply to transfers that were known to MSH, but made unwittingly, as the result of fraudulent information.

For the same reason, the court rejected coverage under the Funds Transfer Fraud provision, which included the same "without the Insured

Entity’s knowledge or consent” language. In refusing to interpret “knowledge or consent” phrase to implicitly require knowledge based on “true facts and circumstances,” the court distinguished the Social Engineering Fraud provision, which expressly covered transfers made knowingly, but as the result of false information. That provision stated: “The Insurer will pay for loss resulting” from the payment or transfer of money 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.”

Authors and
Contacts

[Bryce Friedman](#)
Partner
bfriedman@stblaw.com
[+1-212-455-2235](tel:+12124552235)

