HINSHAW

Alerts

Fifth Circuit Affirms No Computer Transfer Fraud Coverage for Phishing Scam

February 8, 2021
Insights for Insurers

The Fifth Circuit has affirmed a district court ruling that a crime policy's Computer Transfer Fraud coverage did not apply to losses incurred in connection with an email phishing scam. See *Mississippi Silicon Holdings LLC v. Axis Insurance Company* (5th Cir. 2021). As we discussed in a prior alert, employees of the insured silicon manufacturing company were tricked by fraudsters posing as a vendor into transferring over $1 million to the fraudster's bank account.

The policy's Computer Transfer Fraud provision applied to loss "resulting directly from Computer Transfer Fraud that causes the transfer, payment, or delivery of Covered Property from Premises or Transfer Account to a person, place, or account beyond the Insured Entity's control, without the Insured Entity's knowledge or consent."

The district court held that the policy's Social Engineering coverage, with a $100,000 limit, was triggered by the claim, but the Computer Transfer Fraud provision, with a $1 million limit, did not apply because the transfers were sent by the insured's employees, and the fraudulent emails did not manipulate the insured's computer system. In affirming the lower court's decision, the Fifth Circuit focused on fact that the transfers were made with the knowledge of the insured's employees. The court stated:

> The policy means what it says: Coverage under the Computer Transfer Fraud provision is available only when a computer-based fraud scheme causes a transfer of funds without the Insured's knowledge or consent. Here, three ... employees affirmatively authorized the transfer; it therefore cannot be said that the fraud caused a transfer without the company's knowledge. Had [the insurer] intended, as [the insured] suggests, to only protect against employee collusion, it could have limited the provision to transfers that occur "without the Insured Entity's knowledge of or consent to the Computer Transfer Fraud." Rather than include such language, however, the agreement plainly limits coverage to instances in which the transfer is made without knowledge or consent.

The court contrasted the policy's Social Engineering Fraud provision, which applies where, as here, "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." Consequently, the insured's recovery was limited to the $100,000 Social

Attorneys

Scott M. Seaman

Engineering limit.

Because the court based its decision on the "simpler grounds" concerning the knowledge of the insured's employees under the Computer Transfer Fraud provision, it declined to address the "complicated question" of whether the insured's loss "result[ed] directly from" the fraudulent scheme, noting that some courts interpret that phrase as implying a proximate cause standard, while others consider whether the loss "flows straightaway, immediately, and without any intervention or interruption."