

Eleventh Circuit Rules That Crime Policy Covers Email Phishing Scheme Resulting In Fraudulent Wire Transfer

12.19.19



(Article from *Insurance Law Alert*, December 2019)

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

The Eleventh Circuit ruled that a “fraudulent instruction” provision of a commercial crime policy covered loss stemming from an email phishing scheme. *Principle Solutions Grp., LLC v. Ironshore Indem., Inc.*, 2019 WL 6691509 (11th Cir. Dec. 9, 2019).

A hacker posing as a Principle Solutions executive sent an email to the company controller. The email stated that the company had been secretly working on a corporate acquisition that would involve a \$1.7 million wire transfer to a specific account. The email instructed the employee to await further information from an attorney. Several minutes later, someone purporting to be that attorney sent detailed instructions regarding the wire transfer. The employee then provided necessary information to Wells Fargo in order to effectuate the transfer, including a confirmatory phone call. It was later discovered that the emails were fraudulent. The money was never recovered.

Principle sought coverage under a provision for “loss resulting directly from a fraudulent instruction directing a financial institution to . . . transfer, pay or deliver money or securities.” When the insurer denied coverage, Principle sued for breach of contract. A Georgia district court ruled in Principle’s favor and the Eleventh Circuit affirmed.

The insurer argued that it had no obligation to provide coverage because the loss did not involve a “fraudulent instruction,” defined as “an electronic or written instruction initially received by [Principle], which instruction purports to have been issued *by an employee*, but which in fact was fraudulently issued by someone else without [Principle’s] or the employee’s knowledge or consent” (emphasis added). The insurer argued that this provision did not apply because the wiring instructions were not sent by a hacker purporting to be the Principle executive (the first email), but rather came from the fraudster pretending to be the attorney (the second email). The court rejected this contention, noting that the two emails, considered together, constituted a “fraudulent instruction.”

The court also rejected the insurer’s assertion that the loss did not “result directly” from the fraudulent instruction. The insurer argued that “directly” requires an “immediate” link between the fraudulent instruction and loss, and that several intervening steps occurred between the fraudulent email and the actual wire transfer, including the confirmation phone call with Wells Fargo. Dismissing this argument, the court held that “resulting directly from” requires proximate causation (not immediacy), and that the employee’s interactions with the impersonating attorney and with Wells Fargo did not constitute intervening acts sufficient to break the causal chain. The court also rejected the contention

that proximate causation was a question for a jury, finding that under the factual record presented, the only reasonable conclusion was that the loss “resulted directly from” the fraudulent instruction.

Notably, in another cyber coverage case also governed by Georgia law, the Eleventh Circuit declined to endorse a “proximate cause” interpretation of the policy term “resulting directly,” and instead held that it requires a consequence that follows “straightaway, immediately, and without intervention or interruption.” As discussed in our [May 2018 Alert](#), when it considered that case, *Interactive Communications International, Inc. v. Great Am. Ins. Co.*, 2018 WL 2149769 (11th Cir. May 10, 2018), the Eleventh Circuit held that financial losses did not “result directly” from computer fraud because of a time lapse and intervening steps between the fraud and the loss.

Numerous courts, interpreting specific policy provisions in accordance with governing jurisdictional law, have reached different conclusions as to whether coverage is available for wire transfer losses initiated by fraudulent emails. Such decisions turn largely on whether the factual record establishes a sufficient connection between computer use and the loss-causing event. See [July/August 2018 Alert](#); [March 2017 Alert](#); [November 2016 Alert](#).

Authors and
Contacts

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

