



# Case Alert

## Georgia Federal Court Rules Commercial Crime Policy Covers Fraudulent Wire Transfer

Losses resulting from cyber fraud have become all too common in everyday business. While many think of “hackers” when it comes to cyber risk, another danger lurks behind everyday communications: the risk of your corporation suffering a substantial monetary loss from a fraudulent e-mail. For example, a single scam email, purportedly from an executive requesting a transfer or wire of corporate funds, could leave you uninsured for the loss under a commercial crime policy.

In August of 2016, however, a Georgia Federal Court ruled in favor of the policyholder in such a situation. In *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, No. 1:15-cv-04130 (RWS) (N.D. Ga. Aug. 30, 2016), the Court ruled that the commercial crime insurer, Ironshore Indemnity, Inc. must cover a \$1.717 million loss suffered by its insured, Principle Solutions Group, because of a wire transfer triggered by a fraudulent e-mail.

Principle’s controller received an e-mail from a person purporting to be one of their managing directors instructing the controller to work with a fictional attorney to ensure that a wire for an international acquisition be done as soon as possible. Because Principle’s bank required more than an e-mail to wire funds from Principle’s account, the controller enabled the approval function on Principle’s online account to verify the capability to wire internationally in different forms of currency. The controller then instructed another Principle employee to create the wire instructions, which was approved by the controller. Principle

then wired \$1.717 million to a bank account in China. The money was then stolen from that account and Principle was unable to recover those funds.

Principle tendered the loss to Ironshore seeking coverage under its commercial crime policy. The commercial crime policy provided coverage for specifically-defined categories of crimes, one of which was “Computer and Funds Transfer Fraud.” Ironshore denied coverage for the loss. Principle filed suit, contending that the loss was covered under the commercial crime policy because the policy provided coverage for losses “resulting directly from a ‘fraudulent instruction’ directing a ‘financial institution’ to debit [Principle’s] ‘transfer account’ and transfer, pay or deliver ‘money’ or ‘securities’ from that account.” Principle argued that its loss resulted directly from the fraudulent e-mail that appeared to have been from its director. Ironshore argued that the loss did not result “directly” because additional information for the wire was conveyed to Principle by the fake attorney after the initial fraudulent e-mail, after which Principle’s employees set up and approved the wire transfer.

The Court found the language of the insurance provision to be ambiguous because it was subject to two reasonable interpretations. It was reasonable for Principle to interpret the language of the commercial crime policy to provide coverage even if there were intervening events between the fraud and the loss. Ironshore’s interpretation, that the provision required an immediate link between the injury and cause, was also reasonable. The Court noted that

“[i]f some employee interaction between the fraud and the loss was sufficient to allow [Ironshore] to be relieved from paying under the provision at issue, the provision would be rendered almost pointless and would result in illusory coverage.”

As corporations continue to rely on electronic communications to facilitate their business practices, the risk of sustaining a substantial loss from a fraudulent e-mail is ever-present. Policyholders should

exercise extreme caution when it comes to situations like the one at issue and be sure to effectively communicate the nature of the loss to their insurers in order to maximize the ability to obtain insurance coverage.

For more information, or if you require assistance in dealing with a similar situation, please contact Phillip A. Perez at [pap@sdvlaw.com](mailto:pap@sdvlaw.com) or (203) 287-2118.