

Ninth Circuit Rejects Coverage Under Computer Fraud Provision For Fraudulent Wire Transfer Claims

03.29.17



(Article from *Insurance Law Alert*, March 2017)

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

As discussed in previous Alerts, courts have rejected policyholder attempts to obtain coverage for cyber-related losses under computer fraud and other similar policy provisions. In *Apache Corp. v. Great American Ins. Co.*, 2016 WL 6090901 (5th Cir. Oct. 18, 2016), the Fifth Circuit ruled that a computer fraud provision does not cover claims arising out of the transfer of funds to criminal accounts because a fraudulent email was only one part of a chain of events that caused the loss, and the loss therefore was not caused “directly” by computer use. See [November 2016 Alert](#). Similarly, in *Universal Am. Corp. v. Nat’l Union Fire Ins. Co. of Pittsburgh, PA*, 2015 WL 3885816 (N.Y. June 25, 2015), the New York Court of Appeals ruled that coverage for the “fraudulent entry” of data is limited to losses caused by unauthorized access into the policyholder’s computer system and does not encompass losses caused by an authorized user’s submission of fraudulent information into the computer system. See [July/August 2015 Alert](#).

This month, the Ninth Circuit, applying similar reasoning, ruled that an insurer does not owe coverage for losses arising out of wire transfers that occurred as a result of fraudulent emails. *Taylor & Lieberman v. Fed. Ins. Corp.*, 2017 WL 929211 (9th Cir. Mar. 9, 2017). The court reasoned that coverage was not available under a computer fraud provision because “sending an email, without more” does not constitute an unauthorized “entry into” a computer system, as required by the coverage grant. The court explained that the emails that instructed the policyholder to effectuate the wire transfers do not amount to trespass into a computer system. The court also held that the fraudulent emails are not an “introduction of instructions” that “propagate[d] themselves” through the computer system, explaining that those policy terms refer to malicious computer codes and other similar intrusions.

In addition, the court ruled that there is no coverage under a forgery provision that protects against loss “resulting from Forgery or alteration of a Financial Instrument by a Third Party.” The court rejected the policyholder’s contention that under the “last antecedent rule,” the words “financial instrument” only limit coverage for an alteration, and that a forgery need not be of a financial instrument. Instead, the court concluded that under a “natural reading of the policy,” forgery coverage extends only to forgery of a financial instrument (and not to a fraudulent email). Finally, the court ruled that there is no funds transfer fraud coverage because that provision requires transfers to be made “without an Insured Organization’s knowledge or consent.” Here, the policyholder knew about the wire transfers and in fact directed the transfer of funds after receiving the fraudulent emails.

Authors and Contacts

[Bryce Friedman](#)

Partner

bfriedman@stblaw.com

+1-212-455-2235

