LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, JULY 28, 2017
PERSPECTIVE

Groundbreaking cyber insurance decision

By Peter S. Selvin

Consider the following two scenarios resulting in identical losses, but potentially two entirely different insurance coverage outcomes:

In the first instance, a thief hacks, or gains unauthorized entry, into an insured's computer system and causes that computer system to execute a bank transfer to the thief's offshore account.

In the second instance, a thief utilizes a process called "spoofing," in which an authentic looking, but fraudulent, email is created to trick the insured into wiring funds to the thief's offshore account. The "spoofing" process in essence tricks the insured's email server into recognizing the fraudulent email as one that actually originated from the insured's client or other trusted source.

Computer fraud policies often provide coverage in the first scenario because in that instance the thief had actually obtained access to the insured's computer and had "used" that computer, in the words of typical policy language, "to fraudulently cause a transfer of [] property from inside [the insured's premises] to … a person outside those premises."

By contrast, in the second scenario, the courts have been generally unreceptive to finding coverage because an insured's acting on, or treating as genuine, a fraudulent email directing the payment of funds has not been thought to be the equivalent of the "use of a computer" in a manner that fraudulently "caused" a transfer of money or other property. As stated by one court, "[t]o interpret the computer-fraud provision as reaching any fraudulent scheme in which [a computer] communication was part of the process would … convert the computer- fraud provision to one for general fraud." *Apache Corp. v. Great Am. Ins. Co.,* 662 Fed. Appx. 252, 258 (5th Cir. 2016); *see also Taylor & Lieberman v. Federal Insurance Company*, 2017 WL 929211 (9th Cir. 2017).

It is believed that the *Medidata* decision is the first which extends the concept of computer 'use' or 'violation' to the practice of 'spoofing.

A recent case decided by the U.S. District Court for the Southern District of New York, however, creates greater opportunities for policyholders to secure coverage in connection with the second scenario. In *Medidata Solutions, Inc. v. Federal Insurance Company*, CV-00907 (S.D.N.Y. July 21, 2017), the court ruled that a "spoofing" incident, which resulted in an insured wiring money overseas, was covered under the insured's computer fraud policy even though the thief had not gained access to or directly used the insured's computer system.

In *Medidata*, the insured, a company that provided cloud-based services to scientists conducting clinical research, used Google's Gmail platform for company emails. In context of the company's possible acquisition, the company's finance department received an email purportedly from the company's president stating that an attorney named Michael Meyer would be contacting the finance department. The email message purportedly from the company's president contained the president's name, email address and picture in the "From" field, but it was a fraudulent "spoof."

On the same day, the company's finance department received a phone call from a man who held himself out to be Meyer, who demanded that a wire transfer be processed for him. The company's finance department advised that it needed further authorization to process Meyer's request in the form of a further email from the company's president requesting the wire transfer. The finance department thereupon received an email from the company's president which, as before, contained the president's email address in the "From" field and a picture next to his name.

Based on this subsequent, authentically appearing email, the finance department wired approximately $4.7 million to a bank account that was provided by Meyer. To state the predictable, the man purporting to be Meyer was a thief and the company's $4.7 million was lost.

Medidata had an "Executive Protection" policy which included a coverage section for computer fraud. Like many such policies, the operative policy language required "the fraudulent (a) entry of Data into … a Computer System; [and] (b) change to Data elements or program logic of a Computer System." Invoking this language, Medidata's insurer denied coverage for the loss because there had been no "fraudulent entry of Data into Medidata's computer system." In addition, the insurer argued that the subject emails containing the false information were sent to "an inbox which was open to receive emails from any member of the public" and thus entry of the fictitious emails "was authorized."

The district court disagreed. As Medidata successfully argued, the address in the "From" field of the spoofed emails constituted "data" which was entered by the thief posing as Medidata's president. The thief accomplished this by entering computer code into the fraudulent email which caused Gmail to "change" the hacker's email address to that of Medidata's president.

Indeed, the court in *Medidata* noted that direct hacking into an insured's computer is only "one of many methods a thief can use" and that the fraud perpetrated on Medidata was "achieved by entry into Medidata's email system with spoofed emails armed with a computer code that masked the thief's true identity. The thief's computer code also changed data from the true email address to Medidata's president's address to achieve the email spoof." For this reason, the court concluded that Medidata's losses were a direct cause of a computer violation and granted summary judgment to Medidata against its carrier.

It is believed that the Medidata decision is the first which extends the concept of computer "use" or "violation" to the practice of "spoofing." As the arsenal of techniques utilized by cyber-criminals change and expand, this is a useful precedent for policyholders seeking to obtain coverage for losses in this context.

Peter S. Selvin *is a member of TroyGould, PC where he practices in the areas of civil litigation and insurance coverage and recovery.*


SELVIN