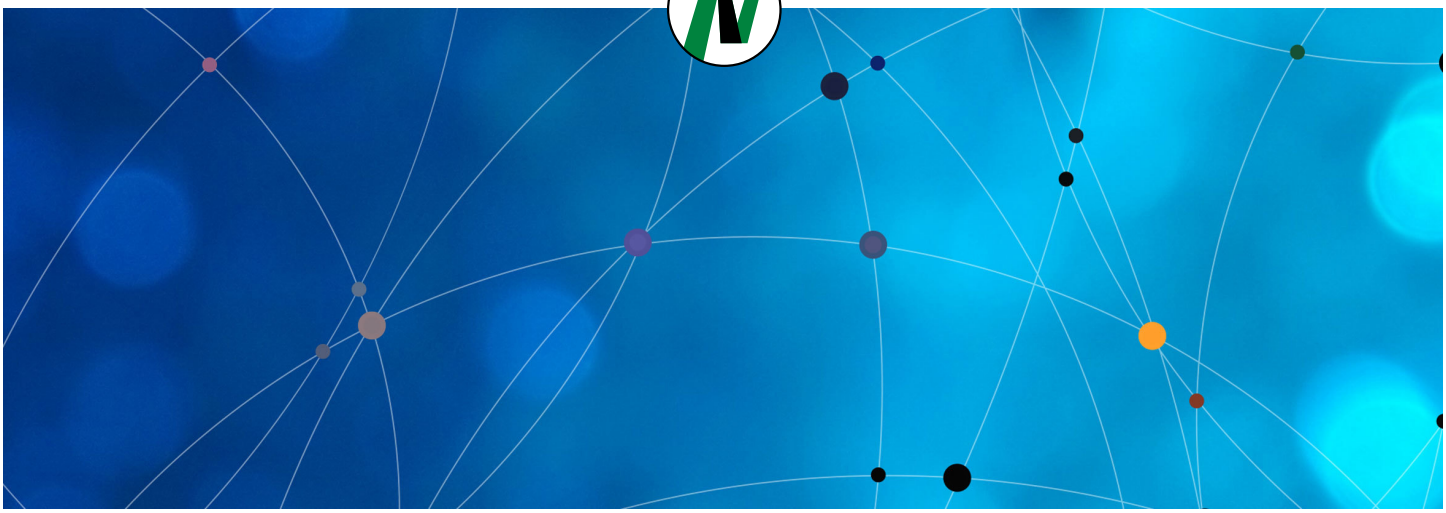

Two Court Rulings Show Coverage Difficulties for "Fake President" Fraud

08.02.2017 | By James H. Vorhis

A few weeks back, Nossaman's Insurance Recovery Report posted a blog about the difficulty obtaining insurance coverage for fake president fraud, which is also known as business e-mail compromise, or social engineering fraud. Two courts have recently reached opposite holdings on this exact topic, which highlight the difficulty policyholders face when they have been victimized by Fake President Fraud.

The policyholder-favorable of those rulings came out of a New York District Court, where the judge found in favor of coverage for this type of fraud under a crime policy issued by Federal Insurance Company. *Medidata Solutions, Inc. v. Federal Ins. Co.*, Case No. 15-CV-907 (S.D.N.Y. July 21, 2017). Docket No. 32. The case was typical of fake president fraud. In 2014, a fraudster imitating the president of Medidata Solutions, Inc. directed an employee in the accounts payable department to wire money overseas for a company acquisition. The e-mail included the president's e-mail address and picture, and copied a fake attorney. The employee performed some degree of due diligence, corresponding with the fake attorney by e-mail and phone before wiring the money. However, that employee ultimately wired $4.8 million dollars to a fraudulent account. Fortunately, the company discovered the fraud before a request to wire another $4.8 million was completed. Medidata sought coverage under its Federal Insurance Company crime policy, but Federal denied the claim. Medidata filed suit in February 2015.

The scope of coverage under the policy turned on a computer fraud provision in the crime policy that covered losses that occurred as a result of the fraudulent entry or changing of data in the policyholder's computer system. The question then arose: was this a fraudulent entry? Some courts had previously determined that fake president fraud does not result in a fraudulent entry or act because the company employee voluntarily makes those changes (although at the direction of a fraudulent actor). Here, though, Judge Andrew Carter Jr. disagreed, holding that the entry was indeed fraudulent because the fraudster used a computer code to alter a series of email messages to make them appear as if they originated from the company's president. In that regard, Judge Carter followed the decision in *Universal American Corp. v.*

National Union Fire Ins. Co. of Pittsburgh, Pa., which found such entries to be fraudulent because they violated the integrity of the computer system. To Judge Carter, it seemed implausible that one would ever find coverage under the narrow view other courts have taken because it would require the fraudster to break into the computer system and wire the money.

But then yesterday, a Michigan District Court reached the exact opposite ruling in *American Tooling Center Inc. v. Travelers Casualty and Surety Co.*, Case No. 5:16-cv-12108, 2017 U.S. Dist. LEXIS 120473 (E.D. Mich. Aug. 1, 2017). There, the fraudster sent e-mails posing as a vendor of the Michigan-based company, asking to forward payments due under a contract between the parties. The company sent the money, only to discover the money was lost forever. American Tooling Center sought coverage under its Travelers' crime policy because it constituted computer fraud, but Travelers denied the claim, arguing that there was not a direct loss that was directly caused by the use of a computer.

The relevant policy definition defined computer fraud as the use of any computer to fraudulently cause a direct loss by money transfer. American Tooling and Travelers obviously disagreed about those terms, but the Judge found in favor of Travelers because the term direct loss was synonymous with the term immediate, and there were steps in between the fraudulent e-mails and the wiring of money. In short, the Michigan court would require the exact thing – a fraudster hacking into the computer and sending the money directly – that the New York court found implausible.

What are the major takeaways from these rulings? First, it is always critical to carefully review the language in insurance policies. The *American Tooling Center* court distinguished the ruling in *Medidata* by contrasting the policy language because the *Medidata* policy did not include the term direct loss in its definition of fraud. To many people, that would be a minor distinction. But to the Michigan court it meant the difference between there being coverage or not. We believe that the *Medidata* court had the proper holding, that the Michigan court should have followed suit, and that Judge Carter's belief that a computer fraud coverage requirement that a fraudster perform a transfer for there to be coverage is too draconian. And because rulings on this subject have come down all over the place, policyholders that frequently conduct transfers via computer should consider contacting insurance professionals, be it an attorney to interpret the policy, or a broker to determine whether there might be a policy endorsement available specifically aimed at this type of event.