August 27, 2018

Imposter's Emails Constitute Covered Computer Fraud Says Sixth Circuit

Related Attorneys: Jason Taylor

A week, to the day, after the Second Circuit affirmed coverage for a $4.8M email scam under a Federal Insurance Company "computer fraud" provision, the Sixth Circuit Court of Appeals found coverage under a Travelers "Wrap+" business insurance policy for another (albeit quite different) business email scam. In *Am. Tooling Ctr., Inc., v. Travelers Cas. & Sur. Co. of Am*., 2018 U.S. App. LEXIS 19208 (6th Cir. July 13, 2018), the Sixth Circuit held that the insured's transfer of approximately $834,000 to fraudsters in response to misleading emails purportedly sent the insured's vendor was covered under a "Computer Fraud" provision of Travelers' "Wrap+" policy.

The insured, ATC, is a tool and die manufacturer, which outsources some of its work to other die manufacturing companies overseas. One of those vendors is Shanghai YiFeng Automotive Die Manufacture Co., Ltd. ("YiFeng"). In early 2015, ATC's Vice President/Treasurer sent an email to his contact at YiFeng, requesting copies of all outstanding invoices. In response, ATC's executive had received an email purportedly from YiFeng, but which was actually sent by a third party that intercepted the executive's earlier emails. (The third party made the email appear to be from YiFeng by using the "yifeng-rnould" domain, which is easily confused for the correct domain: "yifeng-mould.com"). The third party, pretending to be YiFeng, instructed ATC to send payment for several legitimate outstanding invoices to a new bank account. Without verifying the new banking instructions, ATC wire transferred approximately $800,000 to a bank account that was not controlled by YiFeng. By the time the fraud was detected, the funds had been transferred and the wire transfers could not be reversed.

ATC sought recovery for its loss from Travelers, arguing that it fell within the "Computer Fraud" provision of Traveler's "Wrap" policy. The policy provided coverage for the insured's direct loss of…money, securities and other property directly caused by "computer fraud." In turn, "computer fraud" was defined as "the use of any computer to fraudulently cause a transfer" of money, securities, or other property from inside the premises to a person or place outside the premises. Travelers denied coverage arguing that the insured's loss was not a "direct loss" that was "directly caused by the use of a computer," as required by the policy.

At the District Court level, the Eastern District of Michigan agreed with Travelers finding that its policy did not afford coverage for ATC's loss. According to the District Court "direct" means "immediate." In the District Court's view, the fraudulent emails did not "directly" or immediately cause the transfer of funds from the insured's bank account. "Rather, intervening events between ATC's receipt of the fraudulent emails and the transfer of funds…preclude a finding of 'direct' loss 'directly caused' by the use of any computer."

The Sixth Circuit reversed. In so doing, the court first considered whether the insured suffered a "direct loss," as was required by Travelers' "Wrap" policy. Looking to an unpublished Michigan Appellate Court decision, the Sixth Circuit interpreted the term "direct loss" had to be the "immediate" or "proximate" cause. Based upon this construction, the court held that ATC suffered a direct loss at the time it transferred the money to the imposter (as opposed to later in time when ATC was required to make payment to the vendor). The court offered a simple analogy: A owes B $5. As A is handing the $5 to B, C runs by and snatches the $5. In this scenario, A has suffered a "direct" or "immediate" loss even if A owed that money to B and was preparing to hand him the $5.

Next, the court considered whether the impersonator's conduct constituted "computer fraud" as defined in the Travelers Policy. In finding the definition satisfied, the Sixth Circuit distinguished the Ninth Circuit's reasoning in an unpublished opinion, *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, 656 F. App'x 332 (9th Cir 2016). In *Pestmaster*, the Ninth Circuit interpreted the phrase "fraudulently cause a transfer" in the definition of "Computer Fraud" to require an unauthorized transfer of funds. In that case, the insured willingly gave the fraudster electronic access to its bank account to make payments on behalf of the insured. The fraudster did not make the payments and instead kept the money. According to the Ninth Circuit, the use of the computer was legitimate and authorized and the fraudulent conduct itself occurred without the use of computer.

In *American Tooling*, however, the Sixth Circuit reasoned that the impersonator sent ATC fraudulent email using a computer, and the emails fraudulently caused ATC to transfer the funds. Notably, the court cited to the breadth of the Travelers policy's "computer fraud" definition, finding that the policy "does not require, as Travelers argues, that the fraud cause any computer to do anything." According to the court, under the policy "computer fraud" included "the use of any computer to fraudulently cause a transfer…" Had Travelers wished to limit the definition of "computer fraud" to criminal behavior such as "hacking" or unauthorized access to the insured's computer system, it could have done so.

Finally, the Sixth Circuit determined that the "direct loss" was "directly caused by computer fraud." The court determined that the scheme only involved "two steps" -- the fraudulent emails and subsequent transfer, and therefore, satisfied the policy's requirement that the "direct loss" be "directly caused" by the computer fraud. The court reasoned that the first action included the imposter's fraudulent emails and that the second action included the multiple internal actions along with the transfer of money to the imposter.

In reaching its conclusion, the court looked to a recent unpublished opinion by the Eleventh Circuit, *Interactive Communs. Int'l Inc. v. Great Am. Ins. Co.*, 2018 U.S. App. LEXIS 12410 (11th Cir. May 10, 2018). In *Interactive*, hackers manipulated a glitch in a company's reward system and used multiple redemptions of gift cards to the tune of $11.4 million in losses for the insured. The Eleventh Circuit held that the manipulation of a computer system constituted "Computer Fraud," but that the loss did not directly result from that computer fraud, as there were at least two intervening steps between the "computer fraud" and loss itself. There the insured maintained control over the funds even after it was fraudulent induced to transfer "double redemptions" to an innocent third-party account.

In contrast, the *American Tooling* court found a lack of intervening "steps" to break the causal chain: the imposter sent the email and the company went through internal procedures which lead to the transfer of money. Thus, in the eyes of the Sixth Circuit, the transfer of money was directly caused by the computer fraud.

Although the results of the Second Circuit's ruling in *Medidata* and the Sixth Circuit's holding in *American Tooling* are similar, the cases present interesting differences. At the outset, the "fraud" in *Medidata* involved the spoofing of emails with a "computer code" that altered the appearance of the emails to recipients. In contrast, the scheme in *American Tooling* did not involve spoofing of emails or computer code, but a much simpler "cut and paste" of new letters in an email address. The key difference in the two cases may be the scope and breadth of the policies' respective computer fraud coverages. In *Medidata*, the relevant policy language afforded coverage for "the fraudulent (a) entry of Data into…a Computer System; [and] (b) change to Data elements or program logic of a Computer System." In contrast, the policy in *American Tooling* defined "computer fraud" as "the use of any computer to fraudulently cause a transfer" of money, securities, or other property.

It appears from the Sixth Circuit's holding that the breadth of the Travelers "Wrap" policy's definition of "computer fraud" provision is one of the keys to its decision. Had the Travelers policy contained similar, narrower language such as that utilized in other policies, the court's holding may have been different. The American Tooling decision is yet another reminder that not all computer crime or computer fraud coverages are alike and require particular scrutiny in cases of "social engineering fraud" or business email schemes.

Following the Sixth Circuit's ruling Travelers filed a petition for rehearing or rehearing *en banc* with the Sixth Circuit. While the Sixth Circuit has not yet ruled on Travelers petition for rehearing, on August 23, 2018, the Second Circuit rejected Federal's petition for panel rehearing, or in the alternative, for rehearing *en banc*, of the Second Circuit's ruling in *Medidata*.