Scammed by an Email? Phishing for Coverage.

Criminals will probably never stop robbing banks, because—in the words of Willie Sutton—that's where the money is. But modern technology has spawned modern criminals, and today email and other forms of electronic communication are increasingly being used to part people from their money.

Email scams have a name of their own—phishing attacks. Phishing is a cyber attack that uses email that appears to be from a legitimate person or entity in order to trick the email recipient into responding in a way that benefits the scammer who sent it. One common phishing scam involves tricking the recipient into wiring funds to the fraudster's account by masquerading as a client or vendor.

The Sixth Circuit recently weighed in on the insurance coverage available for such an scam. In *American Tooling Center, Inc. v. Travelers Casualty & Surety Company*, 895 F.3d 455 (6th Cir. 2018), the insured received a series of emails from a fraudster pretending to be the insured's Chinese vendor. The fraudster apparently learned the vendor's email and obtained an email address that closely mimicked the vendor's. The scammer then contacted the insured, who never noticed the one letter difference in the email addresses between real-vendor and fake-vendor. The scammer then had several innocent exchanges with the insured before asking the insured to send the amount due on several invoices to a new bank account "due to some new bank rules in the province." The insured innocently wired over $800,000 to the account provided. When the real vendor contacted the insured a short time later seeking payment, the insured discovered the scam.

The issue in the lawsuit was whether the insured had coverage for the lost money under the Travelers crime policy, which provided coverage for various types of criminal activities such as forgery, alteration, employee theft, and computer fraud, defined as:

> Computer Fraud
>
> The company will pay the **Insured** for the **Insured's** direct loss of, or direct loss from damage to, **Money**, **Securities** and **Other Property** directly caused by **Computer Fraud**.

The policy defined **Computer Fraud** as "the use of any computer to fraudulently cause a transfer" of money from a financial institution to a person outside the insured's premises.

The insured argued that the facts satisfied the requirements of the **Computer Fraud** coverage. Travelers disagreed, arguing that (1) the loss was indirect, not direct, since various steps interceded between the fraudulent email and the wire transfer, and (2) the definition of **Computer Fraud** required a computer to have actually *caused* the fraudulent transfer; it was insufficient to simply use a computer and then later have a fraudulent transfer.

The district court found for Travelers. On appeal, the Sixth Circuit reversed and found coverage. The court held that the loss was direct because the insured immediately lost its money when it transferred the funds to the impersonator—there was no intervening event that broke the causation chain. The court further held that the impersonator's use of a computer to send the fraudulent emails satisfied the "fraudulently cause" language of the policy.

The court in *Medidata Solutions, Inc. v. Federal Insurance Co.*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017) reached a similar conclusion in another email spoofing case. The facts of the scam were different, but the result was the same. The insured was induced to wire money to an account set up by a scammer pretending to be the company's president. The court found

coverage under the relatively standard language of the Computer Fraud coverage part of the Commercial Crime Policy.

But not all insureds have faired as well. In *Tayler & Lieberman v. Federal Insurance Co.*, 681 Fed. Appx. 627 (9th Cir. 2017), an accounting firm was duped into sending wire transfers of a client's funds to a scammer in response to a fraudulent email. The court ruled for the insurer, although the result may have been predicted on a different fact pattern—it was a client's money and not the insured's money that was lost—and a different fraud scheme.

The insurer also prevailed in *Schmidt v. Travelers Indemnity Co.*, 101 F.Supp.3d 768 (S.D. Ohio 2015), but based primarily on a "voluntary parting" exclusion not contained in the policies in *American Tooling* and *Medidata*.

So, what's the lesson? First, be very careful with wire transfers. Have internal checks to verify that the money is being wired to the correct account. A telephone call to the recipient confirming any new wiring instructions is advisable. And second, have a Commercial Crime Policy that includes Computer Fraud coverage. Based on the case law, the Computer Fraud coverage gives an insured the best chance of recovering for a loss based on email phishing.