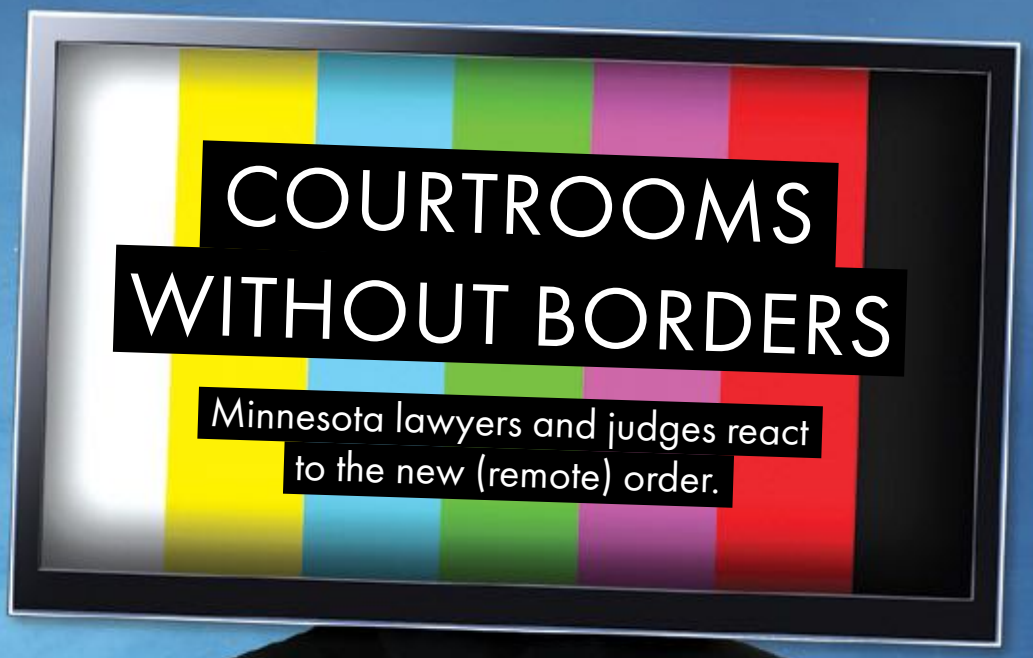
MINNESOTA STATE BAR ASSOCIATION

OCTOBER 2022

BENCH+BAR of Minnesota



COURTROOMS WITHOUT BORDERS

Minnesota lawyers and judges react to the new (remote) order.

Plus: Remote pro bono and Greater Minnesota

SOCIAL ENGINEERING OR COMPUTER FRAUD?

In cyber insurance, the difference matters

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

Many organizations view cyber-insurance policies as a final line of defense against the risks associated with cybercrime. Given the potential for damages, and the prevalence of cyberattacks, cyber-insurance policies are increasingly common. Even so, these policies can be confusing and difficult to dissect, sometimes resulting in unwanted surprises when it comes to filing a claim. Take for example *SJ Computers, LLC v. Travelers Casualty and Surety Company* (21-CV-2482 (PJS/JFD) (D. Minn. 8/12/2022)).

Essentially, SJ Computers fell victim to a social engineering scam in which a bad actor accessed its systems and sent fraudulent invoices appearing to originate from a known vendor. The CEO wired about $600,000 to the bad actor, and only realized what had happened once the transaction had cleared. Seeing that the emails were fraudulent, SJ Computers looked to its policy with Travelers Casualty and Surety Company of America.

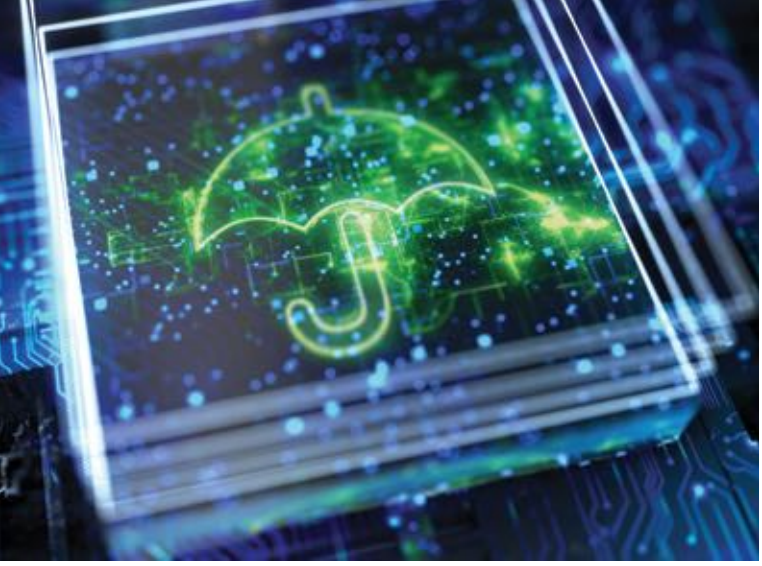
This policy contained two separate agreements, one pertaining to computer fraud and the other to social engineering fraud. According to the order, *computer fraud* was defined as "intentional, unauthorized, and fraudulent entry or change of data or computer instructions directly into a computer system." *Social-engineering fraud* was defined as "the intentional misleading of an employee or authorized person by a natural person impersonating [a vendor, or that vendor's attorney, client, or that client's attorney, employee, or authorized person] through the use of a communication." When SJ Computers made its claim under the social-engineering fraud agreement, it quickly learned that coverage was capped at $100,000. Litigation ensued when Travelers would only provide coverage under this agreement, and not the computer-fraud agreement with its $1 million coverage limit.

This past August, U.S. District Court for Minnesota Chief Judge Patrick Schiltz granted Travelers' motion to dismiss, acknowledging the definitions of computer fraud and social engineering fraud contained within its policy with SJ Computers. Although SJ Computers attempted to argue that their policy did in fact cover their losses, the court ultimately favored Travelers:

> "Travelers offers several reasons why SJ Computers' loss is not covered under the computer-fraud agreement: First, the conduct in which the bad actor engaged was not computer fraud as that term is defined by the Policy. Second, even if the bad actor engaged in computer fraud, SJ Computers' loss was not 'directly caused by' that computer fraud. Third, Exclusion H of the Policy explicitly precludes computer-fraud coverage for SJ Computers' loss. And finally, the conduct in which the bad actor engaged meets the definition of social-engineering fraud, and social-engineering fraud is explicitly excluded from coverage under the computer-fraud agreement... [T]he Court agrees with Travelers on every point."

The court also distinguished this case from others that contend with the same issues of computer and/or social-engineering fraud, writing that "those cases are distinguishable in a crucial respect: None of them analyze an insurance policy that covers *both* computer fraud *and* social-engineering fraud—much less an insurance policy that makes clear that computer fraud and social-engineering fraud are mutually exclusive categories." Furthermore, "The Policy clearly anticipates—and clearly addresses—precisely the situation that gave rise to SJ Computers' loss, and the Policy bends over backwards to make clear that this situation involves social-engineering fraud, not computer fraud." The order concludes, "Because the fraud that caused SJ Computers' loss plainly meets the definition of social-engineering fraud, that fraud cannot also meet the definition of computer fraud. The Policy could not be clearer on this point: "*Computer Fraud* does not include *Social Engineering Fraud*" (emphasis in original).

The court's order is clear: Given the definitions included in the Travelers policy, SJ Computers could only make a claim under the social-engineering agreement. This is precisely the course of action which SJ Computers took when it made its claim to begin with, based on the circumstances of the case. SJ Computers only attempted to pursue a different course of action when it learned that



CYBER-INSURANCE POLICIES ARE VALUABLE COMPONENTS OF AN ORGANIZATION'S CYBERSECURITY PLAN, BUT IT IS CRITICAL TO UNDERSTAND THEIR LIMITATIONS AND THE SPECIFICS OF YOUR POLICY.

the social-engineering agreement provided far less coverage than the computer-fraud agreement.

Our current cyberthreat landscape makes cyber-insurance policies a necessity for many organizations. It should be noted that as cybercrime proliferates, policy language is becoming increasingly specific. "Due to rising cyber-related claims... insurers started to clarify cyber policy language further in 2019 for 'silent cyber' coverage, where the policy does not explicitly include or exclude cyber risk within a policy. Firms have addressed silent cyber issues by adopting language that specifically excludes or affirms coverage, or by adopting coverage sublimits, which reduces the benefits of the policies."* Insurers are prioritizing making cyber policies as clear as possible, including definitions that prevent ambiguously broad claims.

From a cybersecurity perspective, this case is a decisive example of both the limitations of cyber insurance and the importance of reviewing your policy. Social engineering attacks continue to abound, and organizations should look to proactive measures to safeguard themselves against the risks. Learning to spot fraudulent emails and taking the time to verify wire transfer requests are ways in which education and training can prevent phishing attacks. Cyber-insurance policies are valuable components of an organization's cybersecurity plan, but it is critical to understand their limitations and the specifics of your policy. Asking the right questions now can prevent problems down the road, and acknowledging the fact that a cyber-insurance policy is not a "fail safe" for bad security practices can help inform an organization's security goals. ▲

** www.fitchratings.com/research/insurance/russian-cyberattacks-may-test-insurer-war-exclusion-policy-language-01-03-2022*