Minnesota Federal Court Rejects Insured's Attempt to Cast Social Engineering Fraud As Computer Fraud Under Crime Policy

By: Celestine Montague and Paul A. Briganti
Insurance Coverage and Bad Faith Alert
8.16.22

On August 12, 2022, the U.S. District Court for the District of Minnesota dismissed a policyholder's complaint seeking a declaration that $600,000 in social engineering fraud loss fell within a crime policy's computer fraud coverage. *SJ Computers, LLC v. Travelers Cas. & Sur. Co. of Am.*, No. 21-CV-2482, 2022 U.S. Dist. LEXIS 144158 (D. Minn. Aug. 12, 2022). The court determined that, instead, the loss fell solely within the policy's coverage for social engineering fraud, which had limits of $100,000. In so holding, the court rejected what it characterized as frivolous arguments by the policyholder "to avoid this obvious conclusion" and "to prolong a lawsuit that it is destined to lose."

The policyholder, SJ Computers, LLC (SJ Computers), was a provider of refurbished computer parts. In March 2021, SJ Computers' purchasing manager received emails purporting to originate from one of its vendors, ERI Direct. The emails attached invoices and instructed SJ Computers to pay them by wire transfer to a bank account number that differed from the account number ERI Direct had used in the past. The "bad actor" then hacked the purchasing manager's email account and forwarded the invoices from that account to SJ Computers' CEO. Despite being unable to contact ERI Direct, the CEO initiated a wire transfer for around $600,000 to the new bank account number. A few days later, after the bad actor had withdrawn the funds, SJ Computers discovered the fraud.

SJ Computers submitted a claim under its commercial crime policy, which contained coverage parts for direct loss directly caused by "social engineering fraud" and "computer fraud." The policy defined these terms, in relevant part, as follows:

> "Social engineering fraud" means "the intentional misleading of an Employee or Authorized Person by a natural person impersonating . . . a Vendor . . . through the use of a Communication."
>
> "Computer fraud" means "an intentional, unauthorized, and fraudulent entry or change of data or computer instructions directly into a Computer System," but does not include: (1) an "entry or change made by an Employee [or] Authorized Person . . . made in reliance upon any fraudulent . . . instruction"; or (2) "social engineering fraud."

SJ Computers initially positioned the claim under the social engineering fraud coverage part, but sought to reposition under the computer fraud coverage after realizing it was subject to a much higher limit of liability ($1 million) than the limit applicable to the social engineering fraud coverage ($100,000). The insurer accepted social engineering fraud coverage and paid the applicable limit, but disclaimed computer fraud coverage.

SJ Computers sued the insurer in the Minnesota federal district court, seeking a declaration that the claim fell entirely within the computer fraud coverage, such that it was entitled to recover an additional $500,000 in limits under the policy. In granting the insurer's motion to dismiss the complaint, the court concluded that SJ Computers' claim fell outside the definition of "computer fraud" because its CEO, "in reliance upon [a] fraudulent instruction" from the bad actor, had used a computer system to change the wire payment instructions and initiate the transfer to what he thought was the vendor's bank account. The court found, instead, that the claim fell solely within the social engineering coverage because the fraud involved:

1. "the intentional misleading of an Employee" (SJ Computers' CEO)
2. "by a natural person" (the bad actor)
3. "impersonating a Vendor" (ERI Direct) or "an Employee" (the purchasing manager of SJ Computers)
4. through the use of a Communication (the fake invoices and emails).

The court rejected SJ Computers' attempts to "avoid the plain language of the Policy" and to fragment the fraud into distinct parts, certain of which, SJ Computers argued, constituted "computer fraud." According to the court, the hacking of the purchasing manager's email account, even if appropriately viewed in isolation and deemed an act of computer fraud, could not be said to have "directly cause [d]" a "direct loss" to SJ Computers, as required by the computer fraud insuring agreement. The court acknowledged a few cases from other jurisdictions that examined whether the connection between the loss and the use of a computer was "direct" so as to satisfy the requirements for computer fraud coverage. The court, however, found those cases distinguishable because they did not involve a policy providing coverage for both computer fraud and social engineering fraud, "much less" a policy that "makes clear" computer fraud and social engineering fraud are "mutually exclusive categories."

After observing that the meaning of "direct" had to be interpreted in the context of the entire policy, the court stated:

> If the fraudulent scheme that victimized SJ Computers is going to be fragmented into pieces and each piece viewed in isolation, then what 'directly caused' loss to SJ Computers was not the piece involving the bad actor's use of the purchasing manager's account to send the fake invoices, but rather the piece involving the CEO's use of his computer to act on the fake invoices. That piece — the piece that did 'directly cause[]' a 'direct loss' to SJ Computers — was social-engineering fraud, not computer fraud, as even SJ Computers concedes.

The court further held that, even assuming SJ Computers had been victimized by "computer fraud," coverage would be precluded by an exclusion for loss "resulting from forged, altered, or fraudulent . . . instructions used as source documentation to enter Electronic Data or send instructions[.]"[1] According to the court, the exclusion's "unambiguous language" precluded coverage because SJ Computers' loss resulted from "fraudulent instructions" that its CEO had "used as source documentation" to "send instructions" to SJ Computers' bank to wire money to the bad actor's account.

In finding that the circumstances involved social engineering fraud, the court observed that "the drafters of the Policy anticipated precisely the type of fraud that victimized SJ Computers, defined that fraud as social-engineering fraud, and, for good measure, excluded that fraud from the definition of computer fraud." The court denied SJ Computers' arguments, "ranging from creative to desperate," that sought to characterize the circumstances as involving computer fraud. In the court's view, the policy "clearly anticipate [d] — and clearly addresse[d] — precisely the situation that gave rise to SJ Computers' loss," and the policy "ben[t] over backwards to make clear" that the situation presented — intentional misleading of SJ Computers' CEO by a bad actor impersonating a vendor through emails — involved social engineering fraud rather than computer fraud.

If you have any questions or would like further information, contact Celestine Montague (montaguec@whiteandwilliams.com; 215.864.6813) or Paul Briganti (brigantip@whiteandwilliams.com; 215.864.6238).

[1] The exclusion expressly did not apply to claims for social engineering fraud.