

Email Impersonation-Wire Transfer Loss Is Not Covered By Computer Fraud Provision, Says Minnesota Court (Insurance Law Alert)

10.03.22



(Article from *Insurance Law Alert*, September 2022)

For more information, please visit the [Insurance Law Alert Resource Center](#).

A Minnesota district court granted an insurer's motion to dismiss, finding that losses stemming from a fraudulent email and subsequent wire transfer were subject to coverage under a social engineering fraud provision, and not a computer fraud provision. *SJ Computers, LLC v. Travelers Cas. & Sur. Co. of Am.*, 2022 WL 3348330 (D. Minn. Aug. 12, 2022).

A fraudster tricked SJ Computers into wiring nearly \$600,000 into his bank account. The bad actor emailed fraudulent invoices to the company's purchasing manager, purporting to be one of the company's vendors and providing new wire transfer instructions. He then hacked into the purchasing manager's email account and, impersonating him, forwarded the invoices to the CEO for payment. The CEO made several unsuccessful attempts to verify the changes with the actual vendor, but ultimately proceeded with the wire transfer without obtaining verification.

When the fraud was discovered, SJ Computers sought coverage under a social engineering provision, which defined social engineering fraud as "the intentional misleading of an Employee or Authorized Person by a natural person impersonating: (1) a Vendor . . . through the use of a Communication." Subsequently, SJ Computers revised its claim to seek coverage under a computer fraud provision, which included a significantly higher liability limit and covered a "direct loss . . . directly caused by Computer Fraud," with Computer Fraud defined as "an intentional, unauthorized, and fraudulent entry or change of data or computer instructions directly into a Computer System." The policy provided that the two provisions were mutually exclusive and that any loss caused by social engineering fraud was excluded under the computer fraud provision and vice versa. Travelers accepted coverage for the loss under the social engineering fraud provision, but denied coverage under the computer fraud provision. SJ Computers sued, and the court dismissed its complaint.

The court agreed with Travelers that the loss at issue was not caused by computer fraud, defined to expressly exclude any "entry or change [of data or computer instructions] made by an Employee . . . in reliance upon any fraudulent . . . instruction." The court stated: "That is precisely what happened here." SJ Computers argued that the fraudulent conduct was actually two separate acts (the hacking into the email system and subsequent wire transfers) and that only the latter act was excluded from the computer fraud provision, whereas the former was not because the bad actor was not an employee. The court rejected this argument, finding it illogical to fragment the fraud into separate acts. Further, the court held that even if the hacking component could be considered in isolation, computer fraud coverage would still be unavailable

because the hacking did not “directly cause” a “direct loss,” as required by that provision. Rather, the loss was directly caused by a series of subsequent actions, including the ultimate wire transfer of funds.

Finally, the court ruled that even if the loss could be construed to fall within the computer fraud provision, coverage would be barred by an exclusion that applied to losses resulting from fraudulent instructions used by an employee to enter data or send instructions. That exclusion applied to all coverages except the social engineering fraud provision, thus further supporting the conclusion that the type of fraud experienced by SJ Computers was social engineering fraud rather than computer fraud.

Authors and Contacts	Bryce Friedman		Joshua Polster	
	Partner		Partner	
	bfriedman@stblaw.com		joshua.polster@stblaw.com	
	+1-212-455-2235		+1-212-455-2266	

