



Second Circuit Finds Coverage in Cyber Fraud Case Medidata Solutions Inc. v. Federal Insurance Co.

On Friday, July 6, 2018, the United States Court of Appeals for the Second Circuit held that a fraudulent email that caused a company to transfer \$4.8 Million to the fraudster was a “direct loss” and was, therefore, covered by the company’s computer fraud insurance.

By defining “direct cause” as “proximate cause,” the Second Circuit Court of Appeals has settled a major ambiguity in computer fraud insurance policies in favor of policyholders. “Direct cause” is one of the most hotly debated issues in crime insurance and courts disagree on its interpretation. Earlier this year, the 9th Circuit found against coverage in a similar situation in Taylor & Lieberman v. Federal Insurance Company, 2017 WL 929211 (9th Cir.). These conflicting decisions could give rise to an appeal to United States Supreme Court.

The Loss

In 2014, an employee of Medidata Solutions Inc., (a cloud-based technology company) received an email purporting to be from the company’s president. As a result of the email, the company eventually wired \$4.8 million to an outside bank account. That email turned out to be spoofed, and the bank account belonged to a fraudster.

The district court explained in the underlying case:

“[S]poofing” is “the practice of disguising a commercial e-mail to make the e-mail appear to come from an address from which it actually did not originate. Spoofing involves placing in the ‘From’ or ‘Reply-to’ lines, or in other portions of e-mail messages, an e-mail address other than the actual sender’s address, without the consent or authorization of the user of the e-mail address whose address is spoofed.”

Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471, 477 n.2 (S.D.N.Y. 2017) (quoting Karvaly v. eBay, Inc., 245 F.R.D. 71, 91 n.34 (E.D.N.Y. 2007)).

The Claim

When the fraudster attempted the same scam a second time, Medidata discovered the fraud and tendered the loss under its Federal Executive Protection policy. The Policy contained a “Crime Coverage Section” addressing loss caused by various criminal acts, including Forgery Coverage Insuring, Computer Fraud Coverage, and Funds Transfer Fraud Coverage.

Federal denied coverage for two reasons: first, Federal claimed that no actual hacking or data breach took place “because the emails did not require access to Medidata’s computer system, a manipulation of those computers, or input of fraudulent information.” Medidata Sols., Inc., 268 F. Supp. 3d at 475. Second, Federal claimed Medidata did not sustain a “direct loss” because the spoofed emails directed Medidata’s employees to transfer the funds, and, therefore the fraudster’s computer-action was not the direct cause of the loss, rather Medidata’s actions (through its employees) was an intervening cause.

The Ruling

The District Court rejected Federal's arguments and the Second Circuit agreed.

First, the Second Circuit explained that there was a sufficient breach of a computer system because (1) the email system constituted a "computer system" within the meaning of the policy, and (2) the spoofing code was a fraudulent entry of data into that system for the purpose of making the fraudster's emails appear to come from a high-ranking member of Medidata's organization. Second, the court held that this was a "direct loss." The Court of Appeals agreed with several New York courts that has previously equated "direct loss" with "proximate cause." Using the "proximate cause" standard for "direct loss," the court explained why the loss was covered:

It is clear to us that the spoofing attack was the proximate cause of Medidata's losses. The chain of events was initiated by the spoofed emails, and unfolded rapidly following their receipt. While it is true that the Medidata employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred. The employees were acting, they believed, at the behest of a high-ranking member of Medidata. And New York law does not have so strict a rule about intervening actors as Federal Insurance argues.

By defining "direct cause" as "proximate cause," the Second Circuit Court of Appeals has significantly bolstered the effect of cybercrime coverage.

Cyber risks exist in every business. Even the smallest companies are entrusted with their customers' and employees' sensitive information. General liability, cyber risk, and crime insurance all cover certain pieces of those losses, but the intersection of these policies can often create coverage gaps. An insurance coverage attorney with cyber risk experience can review all of your company's insurance to make sure that your policies work with each other to maximize coverage, and identify uncovered losses that can be managed outside the insurance framework.

If you have any questions about cyber risks for your business, we're here to help. You can send us an email at coverage@sdvlaw.com or give us a call at (203) 287-2100 and your email will be directed to an experienced cyber risk attorney.