Guest Blog: Policyholder Victories Underscore Value of Crime Insurance for Cyber Fraud

If you suffer a theft at the hands of a cybercriminal, promptly check your insurance protection — particularly your crime insurance. Two major federal court cases decided this summer reaffirm the protection many policyholders already have available to them for cyber scams. With cybercrime rampant, policyholders should remember that there may be a number of insurance products they purchase (or can purchase) that provide cyber loss protection.

The Second Circuit's Unanimous Ruling in Medidata

Two weeks ago, in a case where United Policyholders had weighed in as a friend of the court, the U.S. Court of Appeals for the Second Circuit (applying New York law), ruled that the policyholder was entitled to crime insurance coverage for an all too familiar type of computer scam. In Medidata Solutions, Inc. v. Federal Insurance Company, Medidata sought crime insurance coverage for losses that resulted when an employee, responding to a fraudster's email purporting to be from the company's president, wired nearly $5 million to the fraudster's account. The insurance company denied coverage on grounds that the theft was not a "direct loss" and that coverage was available only for a "hacking" incident, notwithstanding that the term "hacking" does not appear in the computer fraud insuring agreement of the crime policy.

The Second Circuit followed the U.S. District Court for the Southern District of New York in rejecting both arguments. Noting that the policy provision in question "covered losses stemming from any 'entry of data into' or 'change to Data elements or program logic of' a computer system," the three-judge panel found, "While Medidata concedes that no hacking occurred, the fraudsters nonetheless crafted a computer-based attack that manipulated Medidata's email system, which the parties do not dispute constitutes a 'computer system' within the meaning of the policy."

The Second Circuit's analysis of the direct loss defense is also helpful to all crime insurance policyholders

looking to secure the insurance protection they paid for. While the crime insurance company had argued that Medidata had not suffered a direct loss, both the district and the appeals courts reasoned to the contrary. The Second Circuit found that just because “Medidata employees themselves had to take action to effectuate the transfer” of funds to the cybercriminal after the fraudulent emails were received, those intervening acts did not make the loss indirect. With regard to the direct loss defense, the Second Circuit wrote, “Medidata is correct that New York courts generally equate the phrase ‘direct loss’ to proximate cause,” and, “It is clear to us that the spoofing attack was the proximate cause of Medidata’s losses.”

The Medidata decision thus solidifies New York law equating direct losses to proximately caused losses under crime insurance policies, which is consistent with federal and state court precedents from 2000 and 2013, respectively. The Medidata decision is also consistent with a prior Eighth Circuit decision that found crime coverage for a computer theft, wherein the appellate court rejected the argument that coverage was excluded because an employee of the policyholder may have also contributed to the loss by not adhering to computer security procedures.

The Sixth Circuit’s Unanimous Ruling in ATC

And just several days ago, the United States Court of Appeals for the Sixth Circuit, applying Michigan law, found that an industrial policyholder (ATC) was entitled to crime insurance for a cyber scam in which a criminal tricked the policyholder into wiring money after receiving fraudulent emails. In Am. Tooling Center, Inc. v. Travelers Cas. & Surety Co., the Sixth Circuit held that computer fraud insurance coverage protected the policyholder where “the impersonator sent ATC fraudulent emails using a computer and these emails fraudulently caused ATC to transfer the money to the impersonator.” The Sixth Circuit refused to limit the coverage fraud insuring agreement to cases of computer “hacking” alone.

The Sixth Circuit also rejected the crime insurance company’s direct loss defense, holding that under either a proximate cause analysis or a “direct means immediate” approach, the loss to ATC was a “direct” one. The Sixth Circuit concluded: “ATC received the fraudulent email at step one. ACT employees then conducted a series of internal actions, all induced by the fraudulent email, which led to the transfer of the money to the impersonator at step two. This was the ‘point of no return’ making the theft from the computer fraud a ‘direct loss’ to ATC.” As such, the Sixth Circuit reversed the District Court’s prior ruling in favor of the insurance company.

Conclusion

With the amount of trickery going into thefts and embezzlements these days, crime insurance companies too often use the many steps involved in a fraudulent scheme to argue that losses are indirect and otherwise uncovered. The recent decisions of the Second Circuit and Sixth Circuit on the "direct loss" argument and the scope of computer fraud coverage are important victories for policyholders generally, making clear that where the predominant step in the chain is some type of covered fraudulent misconduct involving a computer, a court is not going to entertain a direct loss defense to excuse the insurance company from paying. As such, policyholders should be familiar with their crime coverage and promptly notify all potentially implicated lines of insurance coverage when a cybercriminal is afoot.

To read UP's amicus brief, click here.

Guest blogger **Joshua Gold** is Chair of Anderson Kill's Cyber Insurance Recovery Practice and was amicus counsel for United Policyholders in the Medidata Solutions, Inc. v. Federal Insurance Company case before the Second Circuit.