New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Insurance law

WWW.NYLJ.COM

VOLUME 264—NO. 67

MONDAY, OCTOBER 5, 2020

Crime Insurance Failing to Keep Up With Cyber Criminal Innovation

BY JOSHUA GOLD

While a pandemic continues to rage, it is understandable to lose focus on the continued scourge of computer-enabled theft. In fact, cyber criminals are counting on it. Hackers routinely rely upon a state of distraction and the craft of diversion to hack, scam and steal.

As such, it is useful for in-house lawyers, their counselors, and risk managers to keep in mind that insurance coverage regularly purchased by organizations to protect against crime losses can protect against computer fraud incidents.

The Hacks Keep Coming

In the age of COVID-19, foreign cyber criminals have hacked pharmaceutical companies looking for a coronavirus cure, law enforcement databases have been hacked, criminals have sought to interfere in elections, and (to prove no one is immune), a cyber security firm was hacked as a means of revenge. Most recently, a cyber scam involving Twitter and several of its high-profile users was revealed in which cyber criminals used hacked accounts to perpetrate fraud through a bogus cryptocurrency donor "match."

© SHUTTERSTOCK

Most commercial organizations purchase crime insurance. Although the terms of the crime insurance can vary, almost all modern commercial crime policies contain in the body of the form an express promise of insurance coverage for losses directly resulting from "computer fraud." Even with the prevalence of computer crime, your trusty crime insurance policy reduces cause to worry, right? Unfortunately, no. Many crime insurance companies fight Computer Fraud insurance claims regularly. See *Sanderina, LLC v. Great Am. Ins. Co.*, No.: 2:18-cv-00772-JAD-DJA (D. Nev. Sep. 11, 2019) for a discussion of crime insurance cases finding coverage and those finding no insurance coverage for the policyholders' Computer Fraud losses; see also *American Tooling Ctr., Inc. v. Travelers Cas. and Sur. Co. of Am.*, 895 F. 3d 455 (6th Cir. 2018); and *Apache Corp. v. Great Am. Ins. Co*., 662 F. App'x 252 (5th Cir. 2016).

Among the various arguments insurance companies have deployed to attempt to deny "Computer Fraud" coverage under crime policies, three have been focal points in multiple court contests.

Brute Force Hacking

First, insurance coverage has been denied where computers were used to commit fraud and steal but where the computer system security itself was not compromised. See *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 25 N.Y.3d 675 (NY 2015) (ruling that computer fraud coverage under crime policy is intended to apply "to losses incurred from unauthorized access to [policyholder]'s computer system" but refusing to find crime coverage where fraudulent billing information was submitted by authorized users of computer

JOSHUA GOLD *is a shareholder in the New York office of Anderson Kill P.C. and chair of the firm's insurance recovery group.*

system). Hacking, however, is not a prerequisite to coverage.

In *American Tooling*, the U.S. Court of Appeals for the Sixth Circuit found computer fraud coverage and held that "Travelers' attempt to limit the definition of "computer fraud" to hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer is not well-founded."

In a 2018 case, *Medidata Sols., Inc. v. Fed. Ins. Co.*, 729 F. App'x 117, 118 (2d Cir. 2018), the U.S. Court of Appeals for the Second Circuit, applying New York law, rejected a crime insurance company's arguments concerning the scope of the Computer Fraud coverage that it had sold to the policyholder. Specifically, in that case, the cyber criminal had impersonated a senior executive of the company by sending fraudulent emails and telephone communications to dupe employees to wire transfer money to the cyber criminal. The crime insurance company argued that because emails were used to defraud the policyholder, there was no actual "hacking" of the computer system—according to the insurance company, a prerequisite for coverage. In ruling against the insurance company, the court held that fraudulently encoded emails meant to cloak the identity of the true emailer, and entered through the computer system of policyholder, triggered computer fraud coverage. See also *The Childrens Place, Inc. v. Great American Insurance Company* (D.N.J., Apr 25, 2019) (rejecting insurance company motion to dismiss Computer Fraud insurance claim and finding the Medidata decision "persuasive"); and *Sanderina* (in rejecting coverage for policyholder, noting that cases "from other circuits interpreting similar policies but finding coverage are distinguishable because the facts present emails that were infected with malicious code or intercepted by hackers.").

Sophisticated Schemes

Some insurance companies will contest insurance coverage where the cyber criminal perpetrates a sophisticated computer fraud against the policyholder. In *Interactive Communications International, Inc. v. Great American Insurance Co.*, (11th Cir. May 10, 2018), for example, the insurance company argued that the loss was not a "direct" loss. The Eleventh Circuit, applying Georgia law, held that the insured's loss did not directly result from computer fraud. The court held that the multi-step cyber scam prevented the loss from being deemed a covered direct loss. In *Retail Ventures, Inc. v. National Union Fire Ins. Co. of Pittsburgh, Pa.*, 691 F.3d 821 (6th Cir. 2012), however, the Sixth Circuit ruled that the policyholder's loss "directly resulted" from a hack. There, the loss included amounts due to fraudulent card transaction assessments and penalties, establishment of call centers for affected customers, and legal fees to address a regulatory consent decree arising from hacked credit card account information. (The author represented Retail Ventures in this case.) See also *American Tooling Ctr.* (applying analysis of decision in *Interactive Communications* and finding computer fraud coverage for policyholder).

Policyholders should resist insurance company attempts to apply unduly narrow interpretations of direct loss coverage.

Actions Bar Coverage Argument

Some insurance companies will argue that the policyholder's loss results not from cyber crime committed against the policyholder, but instead from the actions or omissions of the policyholder's employees. For example, in *State Bank of Bellingham v. Bancinsure, Inc.*, 823 F.3d 456 (8th Cir. 2016), the insurance company argued that a bank's employees' "negligent actions" "played an essential role" in the loss and those actions rendered intrusion into Bellingham's computer system by a "malicious and larcenous virus" a virtual certainty. The court found that the "overriding cause" of the loss the Bank "suffered remains the criminal activity of a third party." See also the *Medidata* decision above, finding that when fraud is the proximate cause of loss, the loss can be deemed "direct" and is not barred by actions of employees.

Policyholders should resist insurance company attempts to apply unduly narrow interpretations of direct loss coverage. Such arguments are unrealistic given the way in which most cyber crime is perpetrated. We are a long way down the road from tellers dipping their hands into the till or the company petty cash box being raided. Most crime worth insuring against today is complex and sophisticated. If certain insurance companies choose to restrict coverage to unreasonable levels, they should be avoided at all costs.