Published on *The National Law Review* https://natlawreview.com

Courts' Approach To Cyber Insurance Continues to Evolve

Article By:

McDermott Will & Emery

As more companies purchase cyber insurance to protect against the risks of computer hacking and data breaches, the body of law interpreting these policies is evolving rapidly. Risk managers and counsel should monitor these developments as they determine the best available policy forms to meet their companies' needs. This report compiles many of the most noteworthy court decisions in this area.

IN DEPTH

Cyber risks are becoming increasingly prevalent and increasingly a source of potential liability, expense and lost income. As companies look to their insurance programs to mitigate these risks, they should consider the body of law resolving disputes over insurance coverage for data breaches and other types of costly cyber incidents. Judicial treatment of policy provisions continues to evolve, and while existing precedent decided on other lines of coverage may provide some guidance, courts have yet to interpret many key cyber insurance policy provisions. In this fast-moving environment, companies should work with their brokers and counsel to determine the best available policy forms to meet their cyber risk management needs.

To date, the majority of court decisions addressing cyber losses primarily involve three separate lines of coverage: comprehensive general liability (CGL), crime/fidelity and cyber insurance. These decisions provide a starting point for determining whether a particular cyber-related claim is covered by insurance.

CGL Policies

The first large disputes over insurance coverage for cyber incidents involved CGL policies, which generally include personal and advertising injury liability insurance for injuries caused by the publication of material that violates an individual's right to privacy. Most courts have rejected coverage for cyber incidents under CGL policies, either finding no "publication" of private material, or finding insufficient the "publication" by a third party instead of the insured. Further, in 2014, the Insurance Services Office, Inc. issued endorsements for use with CGL policies to clarify that traditional CGL policies exclude coverage for many types of cyber incidents. Together, these developments limit the chance of a successful cyber claim under a CGL policy, and suggest the frequency of litigated disputes going forward will decline.

The cases below represent the most noteworthy decisions involving coverage for data breaches under CGL insurance policies.

Was There a "Publication"?

In *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, the Connecticut Supreme Court held that Federal Insurance Company was not required to cover losses related to an incident wherein computer tapes containing private information fell out of the back of a van, were retrieved from the road by an unknown person, and were never recovered. 317 Conn. 46, 115 A.3d 458 (2015). The court found no "publication" sufficient to trigger the policy coverage because there was no evidence that anyone ever accessed the confidential information on the tapes. *Id.* at 50-51.

In *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C.*, on the other hand, the Fourth Circuit affirmed the lower court's decision that the insurer had a duty to defend the policyholder against a cybersecurity-related class action. 644 F. App'x 245 (4th Cir. 2016) (unpublished). Plaintiffs in the underlying litigation alleged that the policyholder, Portal, had failed to secure its server, making their medical records available to unauthorized users online. The lower court held that making confidential medical records publicly accessible via an internet search constitutes "publication" of those materials, and the insurer therefore had a duty to defend. *Id.* at 247. The Fourth Circuit affirmed. *Id.* at 248.

Publication by a Third Party

Even where there has been "publication" of private information, courts have held that CGL policies only cover publication *by the policyholder*, rather than a third party, such as a hacker. In March 2014, the New York Supreme Court determined whether CGL coverage existed for the PlayStation Network data breach. *Zurich Am. Ins. v. Sony Corp. of Am.*, No. 651982/2011, 2014 WL 8382554, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014). The court held that although there had been "publication" of confidential information, coverage did not exist because the publication was carried out by a third party, rather than Sony, the insured. Sony appealed, but the case settled in 2015 before the appellate court ruled on the case. *See also St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.*, No. 617CV540ORL41GJK, 2018 WL 4732718, at *5 (M.D. Fla. Sept. 28, 2018) (holding third-party data breach not covered under a CGL policy, and currently on appeal to the Eleventh Circuit); *Innovak Int'l, Inc. v. Hanover Ins. Co.*, 280 F. Supp. 3d 1340 (M.D. Fla. 2017) (finding no allegations that private material was published, and that even if the information was published, it was not a publication "by Innovak" but rather by hackers (citing *Sony Corp.*, 2014 WL 8382554)).

Crime/Fidelity Policies

Crime insurance (sometimes called a fidelity bond) protects the insured against a broad range of losses due to fraud, embezzlement and theft by others. Courts have reached varying results when determining coverage for cyber-related losses under computer fraud provisions in crime/fidelity policies. Though courts historically have taken a narrow view of what constitutes covered "computer fraud," a pair of 2018 appellate court decisions holding that computer fraud coverage applied to "social engineering" schemes (an attack that relies on human interaction to manipulate users into making security mistakes) could have a large impact on claims under this line of coverage.

Cases Finding No "Direct Loss"

In *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, the Ninth Circuit affirmed the district

court's ruling that Pestmaster's losses were not covered under its crime policy. 656 F. App'x 332, 333 (9th Cir. 2016) (unpublished). The losses stemmed from the failure of Pestmaster's payroll company to pay Pestmaster's payroll taxes; Pestmaster would transfer funds to its payroll vendor, who would then retain the funds, rather than use them to pay the applicable taxes. The court interpreted the phrase "fraudulently cause a transfer" in Pestmaster's crime policy to require an *unauthorized* transfer of funds. 656 F. App'x at 333. The court noted that "reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a 'General Fraud' Policy." *Id.*

Later in 2016, the Fifth Circuit found the *Pestmaster* court's reasoning persuasive. In *Apache Corp. v. Great Am. Ins. Co.*, the court held that a loss resulting in part from spoofed e-mails directing Apache's payment of invoices to a fraudulent bank account was not covered by the "computer fraud" provision in its crime protection insurance policy. 662 F. App'x 252 (5th Cir. 2016) (unpublished).

In *Interactive Communications Int'l, Inc. v. Great Am. Ins. Co.*, the Eleventh Circuit denied coverage for the loss InComm incurred as a result of fraudsters' manipulation of a glitch in InComm's computerized telephone system that allowed them to redeem duplicative value from reloadable debit cards. 731 F. App'x 929 (11th Cir. 2018) (unpublished). The court held that the loss did not "result[] directly" from the computer fraud, as required for coverage. *Id.* at 935. Rather, "several steps typically intervened between the fraudulent manipulation of the [computerized interactive telephone] system to enable duplicate chit redemptions, on the front end, and InComm's ultimate loss, on the back." *Id.* at 934.

Cases Finding "Direct Loss"

Two of the most recent cases on this issue have found that the insured incurred covered "direct loss" due to computer fraud.

In *Medidata Sols. Inc. v. Fed. Ins. Co.*, the Second Circuit affirmed the district court's decision that the computer fraud provision in Medidata's insurance policy covered losses resulting from an email spoofing attack. 729 F. App'x 117, 118 (2d Cir. 2018) (unpublished). Email "spoofing" is the practice of disguising an e-mail to make it appear to come from an e-mail address other than the actual sender's address, without the consent of the user whose e-mail address was spoofed. The relevant policy provision covered losses stemming from any "entry of Data into" or "change to Data elements of program logic of" a computer system. *Id.* Rejecting the insurer's argument that the policy applied only to hacking-type intrusions, the court found that the spoofing code was a "fraudulent entry of data into the computer system" and made a "change to a data element." *Id.* Accordingly, the court held that Medidata's losses were covered by the terms of the computer fraud provision. *Id.* at 119.

One week after the Second Circuit's decision in *Medidata*, the Sixth Circuit similarly held that the computer fraud provision in a business insurance policy covered losses resulting from an email spoofing attack. *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455, 465 (6th Cir. 2018). An employee of the insured received emails purportedly from the company's Chinese vendor, directing payment on outstanding invoices to a new bank account that was not, in fact, controlled by the vendor. The court found, among other things, that the insured suffered a "direct" loss when it mistakenly transferred funds to an impersonator, and that the impersonator's spoofing scheme constituted "computer fraud."

Cyber Policies

There is not yet a significant body of case law interpreting cyber insurance policies. These policies typically include first and third party coverage for network security and data privacy events, and there are a wide variety of coverage options available. The following cases are some of the first in this newly developing body of law, and they afford an incomplete picture of how many common policy provisions will be interpreted by the courts.

In *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc.*, the US District Court for the District of Utah held that under technology errors and omissions liability coverage, the insurer, Travelers, had no duty to defend the insured, Federal Recovery Services (FRS), against allegations that FRS acted with knowledge, willfulness and malice. 103 F. Supp. 3d 1297 (D. Utah 2015). The facts are as follows:

- FRS provided data storage and processing to a fitness company called Global Fitness Holdings. at 1299.
- Global Fitness Holdings alleged that FRS refused to transfer its data pursuant to a contract "until Global Fitness satisfied several vague demands for significant compensation." at 1300.
- The relevant Technology Errors and Omissions Liability form covered loss caused by "any error, omission or negligent act." at 1302.
- The court held that Global Fitness did not allege errors, omissions or negligence, but rather "knowledge, willfulness, and malice," and therefore Travelers had no duty to defend FRS under the policy.

Commentators have noted that this case could have a limited impact because it involved a contract dispute between a policyholder and consumer rather than a third party hacking or unintended disclosure, and was decided on the longstanding principle that liability insurance does not cover intentional harm.

The US District Court for the District of Arizona analyzed a cyber-insurance policy in *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co*., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *8 (D. Ariz. May 31, 2016). The policy at issue covered "direct loss, legal liability, and consequential loss resulting from cyber security breaches." In 2014, P.F. Chang's was hacked and thousands of its customers' credit card data was posted online. *Id.* at *1-2. Federal Insurance Co. disclaimed coverage for fees and assessments that P.F. Chang's had agreed to reimburse its credit/debit card processor as a result of the breach, and P.F. Chang's brought suit. *Id.* at *2. The court found that two exclusions for loss assumed by contract, as well as a similar restriction in the definition of "Loss," barred coverage for P.F. Chang's contractually assumed liability. *Id.* at *7-8. In analyzing coverage, "the Court turned to cases analyzing commercial general liability insurance policies for guidance, because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same." *Id.* at *8.

One recently settled case involved coverage under a financial institution bond's computer and electronic crime rider (C&E Crime Rider), rather than a stand-alone cyber policy. On June 28, 2018, the National Bank of Blacksburg sued its insurer, Everest National Insurance Co., seeking coverage for two multimillion-dollar cyberattacks likely perpetrated by hackers in Russia using phishing

emails. *Nat. Bank of Blacksburg v. Everest Nat. Ins. Co.*, No. 7:18-cv-310 (W.D. Va). At issue in the case was whether the cyberattacks should be covered under the bank's C&E Crime Rider with its higher coverage limit, or the bank's debit card rider, which had a much lower limit. The bank argued that Everest improperly denied coverage under the policy's two exclusions for losses related to the use of credit or debit cards and ATMs. On January 23, 2019, the parties settled as a result of mediation proceedings.

National Law Review, Volumess IX, Number 140