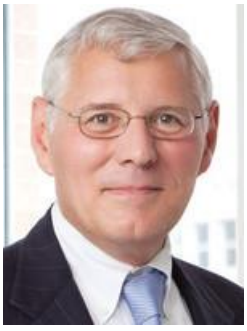
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Developing Trends In Cyberinsurance Litigation: Part 2

*Law360, New York (February 13, 2017, 3:49 PM EST) --*

**The Role of Traditional Insurance Coverage Decisions in Future Cybercoverage Litigation**


Thomas Rohback


Patricia Carreiro

While most cases thus far have arisen under traditional policies, many of these traditional policies now have cyberexclusions to avoid future attempts by insureds to seek coverage for data breaches from these traditional policies (and to require the separate purchase of cybercoverage). Although many of the cases that will arise may present novel issues, insurance companies will likely analyze the policy issues under familiar frameworks from their experience with more traditional forms of cover; e.g.: whether policies cover losses resulting from employee error or negligence, such as employees being tricked into taking actions that compromise the company's security or cost the company money; what types of hacks and breaches are within the policy's scope; what causal connection exists between an event and a loss; when a company's system is sufficiently restored; and the reasonable expectation of coverage and illusory coverage doctrines.

*Coverage for Employee Error / Negligence.*

Employee error is the leading cause of most corporate data breaches. The State of Cybersecurity Report, ACC Foundation (Dec. 9, 2015). Unfortunately for many insureds, multiple courts have held that traditional policies such as crime policies, financial institution bonds and the like do not cover transfers made when authorized users are tricked into issuing payments. For example, in Pestmaster Servs. Inc. v. Travelers Cas. & Sur. Co. of Am., No. 14-56294 (9th Cir. Jul. 29, 2016), the Ninth Circuit Court of Appeals specifically held that a crime policy defining computer fraud as "'[t]he use of any computer to fraudulently cause a transfer,'" only covered unauthorized fund transfers and specifically excluded transfers made by those authorized to make such transfers, but who were fraudulently induced to authorize the transfer. Similarly, in Universal Am. Corp. v. National Union Fire Insurance Co. of Pittsburgh, PA, 972 N.Y.S.2d 241 (N.Y. App. Div. 2013), the court found that a health insurer's financial institution bond rider for "computer systems fraud" would not cover the fraudulent Medicaid charges for untendered services processed through the insurer's claims system under the policy's coverage for the "fraudulent entry ... of Electronic Data or Computer program." The court found, like the court in Pestmaster, that "fraudulent entry" "refers to unauthorized access into plaintiff's computer system, and not to fraudulent content submitted by authorized users."

Some courts, however, have found coverage under fraud policies, even when the transfers are made by authorized personnel. For example, in Principle Solutions Group LLC v. Ironshore Indem. Inc., No. 1:15-CV-4130-RWS (N.D. Ga. Aug. 30, 2016), the court found coverage under a company's commercial crime policy's computer and funds transfer fraud provision for losses sustained when an employee transferred funds in response to a fraudulent email sent by someone posing as the company's managing director. The court, however, did not expressly consider the importance, or lack thereof, of the transfer resulting from an authorized employee being tricked into transferring funds. Instead, the court focused on the parties' dispute over whether the loss was a "direct" result of a fraudulent email (a prerequisite for coverage under the policy).

Like these fraud policies, some cyberpolicies include language regarding "unauthorized" access to their systems. The policy in the P.F. Chang's policy discussed previously is one such example ("actual or potential unauthorized access to such Person's Record"). Employers should be wary of potential gaps in their coverage based on courts' interpreting "unauthorized" access to their systems to exclude breaches caused by employee error.

*The Causal Connection Needed for Coverage*

The closeness of the causal connection needed between a loss and an event is a frequent point of contention where policy language and state causation law are determinative. For example in Bellingham v. BancInsure Inc., 823 F.3d 456 (8th Cir. 2016), the Eighth Circuit addressed whether a "computer system fraud" was the "proximate cause" of a loss where a bank employee, contrary to bank policy, left her token and that of another employee in the bank's computer when going home for the evening. Overnight, a hacker using a Trojan virus used her and another employee's passwords and passphrases to make transfers. While the bank said that the fraudulent transfer was caused by the hacker's crime, the insurer blamed the loss on the employee's violation of company policies, the theft of the employees' passwords and the bank's failure to update its antivirus software. The Eighth Circuit, like the district court before it, found a motion for summary judgment favoring coverage appropriate, largely based on Minnesota's concurrent-causation law. Minnesota's concurrent-causation law states that "when policyholder's loss results from combination of covered and excluded risks, loss is covered unless excluded risk is the 'overriding cause' of the loss." The court held that employee negligence does not convert direct loss into indirect loss, and that an "illegal wire transfer is not [a] 'foreseeable and natural consequence" of an employee failing to follow proper computer security, even if that negligence "'played an essential role.'" Insurers attempting to avoid similar holdings will need clear contractual language to contract around concurrent-causation laws.

The court in Retail Ventures Inc. v. Nat'l Union Fire. Insurance Co. of Pittsburgh, Pa., 691 F.3d 821 (6th Cir. 2012) applied Ohio's proximate cause standard to find coverage for losses associated with DSW's data breach. Hackers, using the local wireless network at a DSW store, accessed Retail Venture's computer system, including payment card information for 1.4 million customers across 108 stores. The hackers then used this information to make fraudulent charges. Retail Ventures sought coverage under its crime policy's computer fraud rider, which covered losses "resulting directly from ... theft of any Insured property by Computer Fraud." To determine whether the loss resulted "directly" from computer fraud, the lower court, applying Ohio law, applied a proximate cause standard and refused to require computer fraud to be the "'sole' and 'immediate' cause of the insured's loss."

Such policies should be contrasted from broader policies that provide coverage for either "direct *or indirect*" causation, such as the endorsement in Metro Brokers Inc. v. Transp. Insurance Co., 603 Fed. App'x. 833 (11th Cir. 2015) (emphasis added). In Metro Brokers, thieves, using a keystroke virus,

authorized transactions from a real estate brokerage firm's bank account. The endorsement had an exclusion for losses "caused directly or indirectly by malicious code or computer viruses," which the insurer used to argue against coverage. The insured, however, insisted that the loss was caused by the thief authorizing the transfers, not the computer virus. The Eleventh Circuit ruled against coverage, in part, because of the policy exclusion's broad language exempting even losses caused indirectly by malicious code. The court reasoned that this language meant that even if the thief authorizing the transfer was the direct cause of the loss, the thief's use of malicious code to authorize the transfers was still an indirect cause of the loss, thereby falling within the scope of the exclusion.

Courts' analyses of breach causation also focus on the degree of a cyberconnection. For example, how much computer usage was necessary to trigger computer fraud insurance coverage was addressed in Apache Corp. v. Great Am. Insurance Co., No. 15-20499, (5th Cir. Oct. 18, 2016). In that case, the court declined insurance coverage for losses sustained when an employee was tricked into changing a vendor's payment information to the fraudster's account. The court's decision looked at the closeness of the link between the fraudulent transfer and the use of a computer in the fraud, finding that the use of a computer to send a single email in a longer chain of events that caused the transfer was insufficient to bring the scheme within the policy's coverage. This result is likely, at least in part, due to the close connection Texas and the Fifth Circuit traditionally require between the insured event and the loss.

**The Next Litigation Battleground**

Insurers and insurance brokers competing for cyberinsurance sales often make representations regarding the quality of coverage. These representations and insureds' beliefs about future coverage, however, are fodder for later litigation. For example, in New Hotel Monteleone LLC v. Certain Underwriters at Lloyd's of London, No. 2:16-CV000061-ILRL-JCW (E.D.La. 2016), New Hotel Monteleone suffered a data breach and hired an insurance agent, Eustis Insurance Co., to procure a cyberpolicy to cover its potential exposure. When that coverage didn't turn out to be what New Hotel expected, it sued Eustis, which filed a third-party complaint against the insurance broker, R-T Specialty, which Eustis had hired to procure an appropriate policy for New Hotel.

Another area of anticipated litigation relates to claims of illusory coverage. In First Bank of Delaware Inc. v. Fidelity and Deposit Co. of Maryland, No. N11C-08-221 (Del Super. Ct. Oct. 30, 2013), First Bank subcontracted with DAS to process credit card payments. DAS was hacked, causing millions of dollars in unauthorized withdrawals, for which First Bank was liable. First Bank sought coverage under its directors and officers policy's "electronic risk liability" coverage, which covered "any unauthorized use of, or unauthorized access to electronic data or software with a computer system." The court found that this attack clearly fell within the policy's fraud exclusion for losses based on fraudulent activity. Nonetheless, the court refused to respect the exclusion, reasoning that every unauthorized use or access to the insured's electronic data or software would almost necessarily involve fraud and thus such an exclusion would render the electronic risk coverage illusory.

A similar argument for illusory coverage may be brewing in Columbia Casualty Co. v. Cottage Health System, No. 2:16-cv-3759, currently in the Central District of California. Cottage Health, a hospital network operator had a data breach in 2013 that exposed patients' medical information. Predictably, they were sued, settled, and sought coverage under their "NetProtect360" policy, which included a breach response and crisis management expense coverage endorsement. Columbia Casualty is seeking a declaratory judgment that it was not obligated to cover the loss because Cottage's insurance application made "material misrepresentations and/or omissions of fact" regarding its cybersecurity practices that voided the policy "ab initio" and because the policy contained a specific exclusion for losses resulting

"directly or indirectly" from Cottage's failure to follow "minimum required practices," including "continuously implement[ing] the procedures and risk controls identified in the Insured's application." It is not unusual to see this sort of limiting language in cyberpolicies, and this case may be one of the first of many which focus on the insured's protection of its system and its data as a factor in determining the availability of coverage. Because most breaches utilize known vulnerabilities, the courts' views of the enforceability or illusory nature of such policies will have a significant impact on cyberinsurance coverage.

—By Thomas Rohback and Patricia Carreiro, Axinn Veltrop and Harkrider LLP

*Thomas Rohback is a partner with Axinn Veltrop and Harkrider LLP in the firm's Connecticut and New York offices. Patricia Carreiro is an associate at the firm's Connecticut office.*