Cyber Insurance Update: Recent Developments in Coverage for Cyber Claims

November 29, 2018

Source: New Jersey Law Journal

Cyber security threats continue to grow in magnitude and number. While courts have yet to see a flood of coverage litigation over the terms of cyber insurance policies, the past year has presented coverage disputes in two areas involving traditional lines of insurance: (i) coverage for social engineering email scams under business and crime policies and (ii) coverage for data breaches under the standard commercial general liability policy provision for "personal and advertising" injuries.

Social Engineering Email Scams

Social engineering scams involve the manipulation of employees into taking actions that compromise corporate security or finances. These scams are becoming more prevalent with the increased reliance on electronic forms of communication. A common scam is the "Fake-President" scheme, which involves fraudsters impersonating corporate executives or other individuals in order to trick employees into transferring funds or disclosing sensitive information. The FBI recently announced that these and other forms of business email compromise have resulted in the theft or attempted theft of more than $12 billion since 2013. Courts are divided on whether such losses fall within the scope of computer fraud coverage under business and crime policies.

On July 6, 2018, the U.S. Court of Appeals for the Second Circuit issued a summary order in Medidata Solutions, Inc. v. Federal Insurance Co., 729 Fed. App'x 117 (2d Cir. July 6, 2018), holding that a social engineering email scam that tricked employees into transferring $4.8 million from company accounts resulted in a covered loss under the computer fraud provision of a crime policy.

The insured's employees received several emails that were made to appear as though they were from the insured's president. In fact, fraudsters used computer code to make the president's picture and his email address appear in the "From" field. The emails instructed employees to wire funds to an external account to facilitate a business acquisition. An individual who was identified as an attorney involved in the deal was copied on the emails. Subsequently, the employees received telephone calls from the purported attorney, who stressed the urgent need for the wire transfer.

The employees learned of the scam only after wiring $4.8 million dollars from company accounts. Medidata submitted the loss as a claim to its insurer, Federal Insurance Company, under its crime-fraud policy. Federal denied the claim, asserting that it was not a "direct loss" resulting from the hacking of Medidata's computer system as required under the policy.

The computer fraud provision at issue applied to the "direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party." The policy defined "Computer Fraud" as "the unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." A "Computer Violation" was defined to include both "the fraudulent: (a) entry of Data into … a Computer System; [and] (b) change to Data elements or program logic of a Computer System…." The term "Third Party" was defined as "a natural person other than: (a) an Employee; or (b) a natural person acting in collusion with an Employee."

The district court had entered summary judgment for Medidata. The Second Circuit affirmed, finding that the loss was covered under the terms of the policy. It reasoned that the loss involved both computer fraud and the fraudulent entry of data into a computer system because the spoofing attack used computer code to manipulate Medidata's email system to create the appearance of emails from Medidata's president. The court held that there was a "direct loss" caused by the spoofing emails even though the Medidata employees also received fraudulent instructions by phone and took voluntary action to effectuate the transfer of funds.

Just one week after the Second Circuit issued its decision in Medidata, the Sixth Circuit issued a decision in American Tooling Center, Inc. v. Travelers Casualty & Surety Co., 895 F.3d 455 (6th Cir. 2018). The Sixth Circuit held that an email impersonation scam qualified as computer fraud under the computer crime section of a business insurance policy issued by Travelers.

In American Tooling, a thief intercepted an email that the insured's employee had sent to one of the insured's vendors. The thief sent a response email to the insured, impersonating the vendor. The thief provided the employee with banking information and asked that the employee use that information to make payment on outstanding balances due to the vendor. The employee unwittingly transferred approximately $834,000 to the thief using this banking information.

Travelers denied the claim on the grounds that there was no "direct loss" as required for coverage and that the policy's definition of "Computer Fraud" requires more than the mere use of a computer and instead requires that a computer "fraudulently cause the transfer." The Sixth Circuit held otherwise, finding that the insured did suffer a direct loss because the thief's "emails fraudulently caused [the insured] to transfer the money to the [thief]."

The decisions in Medidata and American Tooling depart from earlier decisions in which the Fifth and Ninth Circuits held that computer fraud policies do not cover losses where a company's employee transfers funds in response to deceptive emails. See Taylor & Lieberman v. Fed. Ins. Co., 681 Fed. App'x 627 (9th Cir. Mar. 9, 2017); Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co., 656 Fed. App'x 332 (9th Cir. July 29, 2016); Apache Corp. v. Great Am. Ins. Co., 662 Fed. App'x 252 (5th Cir. 2016). The Fifth and Ninth Circuits held that such losses do not result directly from the use of a computer to fraudulently transfer funds because the employee's act of transferring company funds constitutes an intervening cause.

The Eleventh Circuit is due to weigh in on this issue. In Principle Solutions Group v. Ironshore Indemnity, Inc., No. 1:15-cv-4130 (N.D. Ga. Aug. 30, 2016), a district court granted summary judgment to a policyholder, holding that there was coverage for an email spoofing scheme based on a finding that the language of the policy's computer fraud provision was ambiguous. The

appeal was argued on November 9, 2018, and, as of the writing of this article, a decision has not yet been issued.

Data Breaches Under CGL Coverage B

In addition to providing coverage for bodily injury and property damage, the standard CGL policy provides coverage for "personal and advertising injury." This coverage ("Coverage B") applies to several types of claims, including those that arise out of an insured's act of "publication" or "making known" material that violates a person's right to privacy. In St. Paul Fire & Marine Insurance Co. vs. Rosen Millennium, Inc., No. 6:17-cv-540 (M.D. Fla. Sept. 28, 2018), the U.S. District Court for the Middle District of Florida addressed the question of whether a data breach caused by a hacker's intrusion into a company's payment system falls within the scope of this coverage.

The insured, Rosen Millennium, Inc. ("RMI"), provided data security services to its parent company, Rosen Hotels & Resorts, Inc. ("RHR"). RHR discovered a potential credit card breach at one of its hotels when it found malware installed on its payment network. RHR disclosed this suspected data breach to potentially affected customers and sent a demand letter to RMI, alleging that it was entitled to over $1.4 million from RMI to compensate it for expenses arising from the data breach, including forensic investigation, crisis management, attorneys' fees, notification to credit card holders, and fees from credit card companies for the costs associated with card replacement and fraudulent charges.

RMI submitted a claim under Coverage B of its CGL policy with St. Paul. This section of the CGL policy provided coverage for injury "caused by a personal injury offense," which included "[m]aking known to any person or organization covered material that violates a person's right of privacy."

St. Paul argued that Coverage B only provides coverage for a publication resulting from an act of the insured, not from the acts of third parties, i.e., there was no coverage because the actions of the third-party hackers, not RMI, led to the loss. The district court agreed and granted St. Paul summary judgment. The court relied on similar trial court decisions in Innovak International, Inc. v. Hanover Insurance Co., 280 F. Supp. 3d 1340 (M.D. Fla. 2017) and Zurich American Insurance Co. v. Sony Corp., No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb 21, 2014). Also, the court distinguished other cases where coverage for data breaches was found on the basis of the inadvertent disclosure of sensitive information through careless acts of the insured as opposed to data breaches perpetrated by third-party hackers.

Rosen Millennium is on appeal before the Eleventh Circuit. It remains to be seen whether Rosen Millennium will have any influence on the landscape for data breach coverage given the unique facts of the case. St. Paul argued strenuously that there was no "claim" under the terms of the CGL policy, asserting that RMI's demand for indemnification was an attempt to manufacture coverage under a third-party liability policy for what was really a first-party loss to RHR, the parent company. Notably, RMI and RHR were represented in the coverage action by the same counsel. It will be interesting to see what the Eleventh Circuit does with this case.

As the number of cyberattacks increases, so too will the number of businesses obtaining comprehensive coverage under cyber-specific coverage. Until then, courts will be called upon frequently to determine whether coverage for cyber-related losses exists under traditional insurance policies.