Cyberinsurance Update 2019: Misdirection Abounds

This year saw courts consider the scope of cyberinsurance coverage for claims involving the hacking of emails and the manipulation of search terms in online advertising.

November 27, 2019

Source: New Jersey Law Journal

The use of fraudulent email communications to defraud companies is becoming all too common, and courts have reached differing conclusions on whether such losses fall within the scope of policies providing coverage for cybercrimes. Recently, the District of New Jersey became the latest court to weigh in on this question.

In addition, the Western District of Washington recently questioned whether cyberliability coverage extends to claims arising out of a policyholder's use of online advertising that infringes on a competitor's trademark in order to misdirect potential customers.

Coverage for Computer Fraud and Fraudulently Induced Transfers

In April 2019, Judge Esther Salas, in the District of New Jersey, addressed an insurer's motion to dismiss an action seeking insurance coverage under a crime policy for two payments totaling $967,714.29 that were intercepted by a cybercriminal. *The Children's Place v. Great Am. Ins. Co.,* No. 2:18-cv-11963 (D.N.J. Apr. 25, 2019). In that case, The Children's Place, an international retailer of children's apparel based in New Jersey, sought coverage from its insurer, Great American Insurance Company, for payments that it inadvertently made to a cybercriminal posing as one of its suppliers. The Children's Place alleged that the cybercriminal obtained the payments by using email domain names that were virtually identical to that of the supplier to intercept emails and "insert[] itself into the [email] conversation making it appear that the previously legitimate conversation was being continued." The Children's Place also alleged that the cybercriminal obtained its vendor setup form and the supplier's letterhead and used them to provide The Children's Place with payment instructions that surreptitiously directed payments to the cybercriminal's own bank account.

The Great American crime policy provided coverage for "Computer Fraud," defined to include "the use of any computer … to gain direct access to your computer system … and thereby fraudulently cause the transfer of money, securities or other property." The policy also included an endorsement providing coverage for "Fraudulently Induced Transfer," which was defined to include a payment "made in good faith reliance upon … instruction … from a person purporting to be an Employee, your customer, a Vendor or an Owner establishing or changing the method, destination or account for payments." The policy included a condition precedent stating that a "Fraudulently Induced Transfer" would be covered only if, prior to issuing the payment, the policyholder "verified the authenticity and accuracy of the instruction received … by calling, at a

predetermined telephone number, the Employee, customer, Vendor or Owner who purportedly transmitted the instruction."

Great American took the position that the payments were not covered losses under the policy's definition of "Computer Fraud" because there was no allegation that the cybercriminal gained direct access to a computer system belonging to The Children's Place. Judge Salas rejected that argument, finding that the allegations that the cybercriminal intercepted emails and inserted himself into an email conversation, along with an allegation that this allowed him to "effectively gain[] access to [The Children's Place's] email system," were sufficient to create a factual issue as to whether the loss arose from an infiltration of a computer system. The court cited to case law from the Second Circuit, *Medidata Solutions v. Federal Insurance Company,* 268 F. Supp. 3d 471 (S.D.N.Y. 2017), *aff'd,* 729 App'x 117 (2d Cir. 2018), for the proposition that the transmission of an email that disguises its true sender could qualify as gaining access to an email system. The court also rejected the insurer's argument that fraudulent emails could not be said to be the direct cause of a loss that involved the voluntary transfer of funds, holding that the allegations of the complaint were sufficient to permit a jury to decide the issue of causation. Accordingly, the court denied Great American's motion to dismiss the complaint in so far as it sought coverage for "Computer Fraud."

Turning to the endorsement providing coverage for "Fraudulently Induced Transfer," the court addressed the argument by The Children's Place that a condition precedent requiring a policyholder to "verif[y] the authenticity and accuracy of … instruction[s]" before making a payment would render coverage illusory. The Children's Place argued that, if instructions were verified, no loss would ever occur. The court agreed that interpreting the condition precedent to require actual verification would render the coverage illusory. However, rather than hold the condition precedent void, as The Children's Place urged, the court held that the provision had to be interpreted to mean that the policyholder had to "attempt to verify" payment instructions. As it appeared that The Children's Place had failed to make such effort, the claim for coverage was dismissed to the extent it sought coverage under the "Fraudulently Induced Transfer" endorsement. The case remains pending with discovery ongoing.

The court's decision in *The Children's Place* shows that parties must carefully examine the terms of cyberinsurance policies and consider the particular facts of each claim for coverage under those policies. It also suggests that provisions requiring policyholders to take precautionary measures cannot impose conditions that render coverage illusory, while teaching that policyholders ignore such conditions at their own peril.

Coverage for "AdWord" Infringement

In a decision issued in September 2019 in *Mid-Century Insurance Company v. Hunt's Plumbing & Mechanical*, No. 19-cv-0285 (W.D. Wash. Sept. 17, 2019), a federal district court raised the possibility that an insurance policy providing "Cyber Liability and Data Breach Response Coverage" covers liability arising from what could be called "AdWord" hijacking or "AdWord" infringement. Such claims arise when a company purchases rights from an online advertising service, such as Google's "AdWords," to use another company's trademark or tradename to direct traffic to its own website. The New Jersey Law Journal has reported on similar claims

involving a law firm's trademark infringement suit against another firm accused of using Google's AdWords service to misdirect potential clients to that other firm's website. Charles Toutant, "Suit Accuses Law Firm of Hijacking Competitor's Prospective Clients Via Sponsored Searches," New Jersey Law Journal (June 26, 2018).

In *Mid-Century*, Hunt's Plumbing, a plumbing company located in Tacoma, Washington, sought coverage from its insurer for a local competitor's claims alleging that it manipulated Google AdWords to misdirect the competitor's customers to its own website. According to the competitor's complaint, individuals who used Google to search for the name of the competitor's business, "Beacon Plumbing," would see a text advertisement displaying the phrase "Beacon Plumbing Save On Energy Bills. Call Now." Those who clicked on the text advertisement were directed to the website for Hunt's Plumbing. Beacon's lawsuit against Hunt's Plumbing asserted claims for trademark infringement, tortious interference, and violation of a state consumer protection act.

Hunt's Plumbing sought coverage for Beacon's claims under its business owner's policy with Mid-Century Insurance Company, which in turn filed a declaratory judgment action seeking a declaration that there was no coverage for the AdWord-manipulation suit. Mid-Century sought summary judgment on the issue of coverage. The court granted Mid-Century summary judgment with respect to the policy's traditional lines of coverage, including coverage for personal and advertising injury. However, the court found that neither party sufficiently addressed whether coverage existed under the cyberliability portion of the policy, finding that the cyberliability "coverage form specifically lists '[i]nfringement of … trademark … [or] metatags' and '[i]mproper deep-linking' as covered acts." (Modifications and omissions in original.)

The court in *Mid-Century* directed the parties to file briefs addressing whether the claims against Hunt's Plumbing are covered under the cyberliability portion of its policy. Shortly thereafter, the parties reached a settlement, leaving open the question of whether there is cybercoverage for AdWord-manipulation claims. The extent of such coverage will need to be addressed in the future.

Cyberrisk is a threat to entities big and small. As more businesses obtain cyber-specific coverage, courts will be called on to determine the extent to which such coverage applies to deceitful conduct used to defraud policyholders and to a policyholder's own deceptive conduct.