CARLTON FIELDS

Phishing for Coverage: When Is Fraud a 'Computer Fraud'?

October 09, 2015

In late June, the New York Court of Appeals affirmed a trial court ruling that there was no coverage for a health insurance company policyholder, under a "computer systems fraud" rider issued by its insurer, for an underlying $18 million liability it incurred as a result of paying fraudulent claims submitted by providers for services never performed, under certain of its Medicare Advantage plans. In August, a Texas federal court found coverage under a "computer fraud" provision in a crime protection policy, for a policyholder that made wire transfers totaling $2.4 million to a party that fraudulently purported to be its vendor, and which had, using artifice, caused the policyholder to change its payment wiring instructions. The insurer has appealed to the Fifth Circuit Court of Appeals. Now, as the calendar has turned to October, aka "Cybersecurity Awareness Month," cyber insurance industry watchers are looking to the Southern District of New York, where summary judgment briefing is complete in a coverage case brought by a medical technology company against its insurer under the "computer fraud" provision of an executive protection portfolio policy, for $4.8 million in losses it sustained as a result of wiring funds to the wrong recipient based on fraudulent emails. So when is a fraud a covered "computer fraud"? A look at the above cases reveals the ways courts are struggling with this issue. In Universal American Corp. v. National Union Fire Ins. Co. of Pittsburgh, P.A., 37 N.E.3d 78, 25 N.Y.3d 675 (June 25, 2015), the New York Court of Appeals addressed a coverage dispute between Universal American Corp., a health insurance company, and its insurer, National Union Fire Insurance Company of Pittsburgh. Universal issues Medicare Advantage plans. According to Universal, it has a computerized billing system that allows health care providers to submit claims directly. The majority of claims submitted are processed, approved and paid automatically, without manual review. Universal contended that it sustained $18 million in losses for fraudulent claims it paid that were submitted by providers for services that were never rendered. Universal tendered a claim to National Union, which issued a financial institution bond to Universal that insured against losses resulting from dishonest and fraudulent acts. The bond contained a "computer systems fraud" rider that provided coverage for "loss resulting directly from a fraudulent ... entry ... or change of Electronic Data or Computer Program. ..." National Union declined coverage on the basis that the bond did not cover losses from Medicare fraud. Universal thereafter filed a declaratory judgment action. On cross-motions for summary judgment, the New York state trial court denied Universal's motion and granted National Union's motion, holding that coverage under

the rider did not extend to the claims because the "entry" or "change" to the computer system was not "fraudulent," because the providers who made the entries/changes were authorized users on the system. The court held that the term "fraudulent" unambiguously modified the terms "entry" and "change" in the provision, and that the coverage was therefore not intended to address fraudulent claims submitted by authorized users, but rather was intended to cover *unauthorized* entry by, for example, a hacker or virus. Universal appealed, and the case was closely watched, as United policyholders filed an amicus brief in favor of reversal. However, the New York Court of Appeals affirmed, agreeing with the trial court's analysis of the placement of the term "fraudulent" as modifying the "entry" or "change" only, and the fact that the word was not used to modify "electronic data" or "computer program" was telling. In other words, the policy covered *fraudulent entry or change* of electronic data, not the authorized *entry of fraudulent electronic data*. Word choice and placement are critical in coverage disputes, and to the extent National Union intended the coverage to be limited to situations involving "hackers" or the like, and not to this type of Medicare fraud, it succeeded with this particular policy wording. However, a federal court in Texas grappled with a similar issue, and came out in favor of the policyholder. Apache Corp., an oil and gas exploration company in Texas, received a call from an individual purporting to be one of its vendors, Petrofac Facilities Management Ltd. The caller requested that Apache change the payment/wiring instructions on its account. Apache asked that the request be made in writing on Petrofac letterhead. The written request was thereafter emailed from an email address that appeared to be an email from Petrofac. Upon receiving the letter attached to the email, which was on letterhead, Apache called the representative listed on the letterhead to confirm authenticity. The person who was called at the number on the letterhead confirmed the change request. Thereafter, Apache wired approximately $2.4 million in funds before recognizing that the account was fraudulent. Apache looked to its insurer, Great American Insurance Company, for coverage under the "computer fraud" provision of its crime protection policy. Great American's policy covered loss "resulting directly from the use of any computer to fraudulently cause a transfer of ... property from inside the premises ... to a person ... outside those premises." Great American declined coverage, asserting that here, the "use" of a computer was merely incidental to the fraudulent scheme, insofar as only the initial email entailed the use of a computer. All the other steps — phone calls, letters, etc. — did not involve use of a computer, and therefore the loss did not arise "directly" from the use. Apache filed suit seeking coverage. In *Apache Corp. v. Great American Ins. Co.*, No. 4:14-cv-00237 (S.D. Tex. Aug. 7, 2015), the court agreed with Apache, finding the loss was covered. It looked to Fifth Circuit precedent interpreting the term "caused directly" in the context of a fraud provision in a crime policy, noting that the Fifth Circuit had previously found that the term "cause directly" is synonymous in meaning to the tort concept of "cause in fact," which is established by a showing that an act or omission was a "substantial factor" in bringing about harm, and that without it, the harm would not have occurred. The court noted: To adopt Defendant's reading would be to limit the scope of the policy to the point of almost non-existence. That is, if anytime some employee interaction took place between the fraud and the loss, or any fraud was perpetrated any way other than a direct "hacking," the insurance company could be relieved of paying under the Policy. *Id.* at 6. It is difficult to reconcile this holding

with the New York Court of Appeal's holding in *Universal*. While the two courts interpreted terms within similar "computer fraud" provisions, the two decisions ultimately reflect differing views as to whether a "computer fraud" provision is designed solely to cover hacking-type incidents, or if it is more expansive than that, and may also include coverage for phishing scams and the like. The Fifth Circuit Court of Appeals will get its chance to weigh in, as Great American filed a notice of appeal. But the next court to decide the issue will likely be the U.S. District Court for the Southern District of New York. Medidata Solutions Inc. is a medical technology company. In a suit it filed in New York federal court earlier this year, Medidata alleges it was the victim of an international wire transfer fraud, by which certain mid-level employees were deceived by emails from the perpetrators of the fraud who made it appear that the emails came from a Medidata executive that was requesting the transfer of funds. As a result, some $4.8 million in funds were wired to a fraudulent account. Medidata sued its insurer, Federal Insurance Co., alleging that Federal wrongfully declined Medidata's claim for coverage for the loss. Federal, in its memorandum seeking summary judgment, notes that the alleged impostor did not "hack" Medidata's computers, implant a virus, breach firewalls or otherwise manipulate Medidata's computer systems. It also notes that the fraud was initiated by a telephone call, which was followed up by the confirming email at issue. The insuring clause at issue is contained in a Federal executive protection portfolio policy, and covers "direct loss … resulting from Computer Fraud committed by a Third Party." "Computer fraud" is defined as the "unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." Finally, "computer violation" is defined as "fraudulent ... (1) entry of Data into or deletion of Data from a Computer System, (2) change to Data elements or program logic of a Computer System ... or (3) introduction of instructions, programmatic or otherwise, which propagate themselves through a Computer System." Not surprisingly, the parties' briefing, which was completed in August and September, focuses on the New York Court of Appeals ruling in *Universal* in June, although Medidata cited the more recent *Apache* decision in a supplemental filing. While the court's original order setting a briefing schedule denied the parties' request for oral argument, the denial was without prejudice. Thus, the court could issue a written ruling based solely on the parties' written submissions at any time, given that briefing is complete, or it could call for oral argument. In any event, the court will have to grapple with the tension between rulings in this nascent niche of cyber insurance coverage for "computer fraud" and the intention behind the coupling of the terms "computer" and "fraud." The takeaway from these cases for insurers is that they must very carefully delineate the scope of the coverage they intend, and how they market and portray the coverage, particularly given the unpredictability of this relatively new area of coverage dispute. The takeaway for policyholders is to make sure they understand the contours and limits of the coverage they are purchasing. The other takeaway for policyholders is, of course, the familiar refrain corporate America hears from its IT professionals everyday: Don't fall for phishing scams! Republished with permission by *Law360* (subscription required). Originally published by *PropertyCasualtyFocus*.

Authored By

John C. Pitblado

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology