United States Court of Appeals for the Fifth Circuit

United States Court of Appeals
Fifth Circuit
FILED
February 4, 2021
Lyle W. Cayce
Clerk

No. 20-60215

MISSISSIPPI SILICON HOLDINGS, L.L.C.,

Plaintiff—Appellant,

versus

AXIS INSURANCE COMPANY,

Defendant—Appellee.

Appeal from the United States District Court
for the Northern District of Mississippi
USDC No. 1:18-CV-231

Before WIENER, COSTA, and WILLETT, *Circuit Judges*.

PER CURIAM *

In this insurance dispute, Plaintiff-Appellant Mississippi Silicon Holdings, LLC appeals the district court's grant of summary judgment in favor of Defendant-Appellee Axis Insurance Company. Because we agree that Mississippi Silicon Holdings, LLC is not entitled to coverage under the

* Pursuant to 5TH CIRCUIT RULE 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5TH CIRCUIT RULE 47.5.4.

Computer Transfer Fraud provision of an insurance policy it purchased from Axis Insurance Company, we affirm.

I. BACKGROUND

Mississippi Silicon Holdings, LLC ("MSH"), a silicon metal manufacturer, was the victim of a cybercrime. In October 2017, MSH's Chief Financial Officer, John Lalley, received an email from a regular vendor, Energoprom, advising that future payments should be routed to a new bank account. A letter relaying the same instructions, written on Energoprom's letterhead and signed by an Energoprom executive, was attached to the email. The email body also contained previous emails between Lalley and Energoprom personnel concerning invoices and shipment details. Lalley thereafter authorized two wire transfers from MSH to Energoprom's new bank account, totaling approximately $1.025 million. These payments were made in accordance with MSH's three-step verification process for large transfers. First, Lalley initiated a transfer via the online banking system; second, another MSH employee confirmed the transfer on the bank's website; and third, MSH's Chief Operating Officer orally authorized the transfer on a phone call with a bank representative.

But something was amiss. In December 2017, Energoprom called MSH to discuss outstanding payments—payments MSH believed it had already made. At this point, MSH realized it had been the victim of cyber fraud and hired a forensic investigator to investigate the scheme.

After discovering the fraud, MSH submitted a sworn proof of loss to Axis Insurance Company ("Axis"), claiming $1,025,881.13 under a commercial crime insurance policy that covered, among other specifics, Computer Transfer Fraud, Social Engineering Fraud, and Funds Transfer Fraud. Axis granted the claim pursuant to the Social Engineering Fraud provision and sent MSH a check for $100,000.00 (the policy limit for that provision) but denied that either the Computer Transfer Fraud or Funds Transfer Fraud provisions were applicable. Both the Computer Transfer Fraud and Funds Transfer Fraud provisions had coverage limits of

$1,000,000. Axis explained that the Computer Transfer Fraud provision did not apply because (1) the funds were transferred with MSH employees' knowledge and (2) the fraud was accordingly not confined to the computer system, as the policy required.

MSH sued Axis in Mississippi state court, seeking declaratory judgment and damages for breach of contract based on the allegedly erroneous denial of Computer Transfer Fraud and Funds Transfer Fraud coverage.[1] Axis removed the case to federal court on the basis of diversity jurisdiction.

After discovery had occurred, both parties moved for summary judgment asking the district court to construe the Computer Transfer Fraud provision in their favor. The district court granted summary judgment for Axis, finding that, although the provision unambiguously "requires that the fraudulent act *directly* cause the loss," the instant loss was caused not by the fraudulent computer use, but by the affirmative acts of MSH employees in initiating and authorizing the transfer. The court also concluded that the provision's requirement that the transfer occur "without the Insured Entity's knowledge or consent" was not satisfied, again because the transfers were initiated with MSH's approval.[2] MSH timely appealed.

II. STANDARD OF REVIEW

We review summary judgment rulings de novo, construing all evidence and inferences in favor of the non-moving party.[3] Summary judgment is proper if "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law."[4] Questions of contract interpretation are also reviewed de novo, "including any questions about

---

[1] Although MSH maintains it is also entitled to payment under the Funds Transfer Fraud provision, this appeal concerns only the Computer Transfer Fraud provision.

[2] The district court denied coverage under the Funds Transfer Fraud provision for largely the same reason.

[3] *Evanston Ins. Co. v. Mid-Continent Cas. Co.*, 909 F.3d 143, 146 (5th Cir. 2018).

[4] Fed. R. Civ. P. 56(a).

whether the contract is ambiguous."[5] If a contract is ambiguous, the district court's interpretation is reviewed for clear error.[6]

III. LAW & DISCUSSION

State law governs questions of contract interpretation[7]; in this diversity action, Mississippi law applies.[8] "Under Mississippi law, an insurance policy is a contract subject to the general rules of contract interpretation."[9] The primary concern is giving effect to the intent of the contracting parties.[10] The inquiry begins with the four corners of the contract, focusing on the plain meaning of the contract's language.[11] Consideration of parol and extrinsic evidence is only permissible if the contract's language is ambiguous.[12] A provision is ambiguous if it is susceptible to two or more reasonable interpretations, not merely if the parties disagree about its meaning.[13] If ambiguities exist, they must be resolved in favor of the insured.[14] Additionally, the court must consider the policy as a whole and take care to give "operative effect to every provision in order to reach a reasonable overall result."[15]

This dispute boils down to a disagreement over the interpretation of the policy's Computer Transfer Fraud provision. That provision reads:

> The insurer will pay for loss of . . . Covered Property resulting directly from Computer Transfer Fraud that causes the

---

[5] *Pioneer Expl., L.L.C. v. Steadfast Ins. Co.*, 767 F.3d 503, 511–12 (5th Cir. 2014).

[6] *Alford v. Kuhlman Elec. Corp.*, 716 F.3d 909, 912 (5th Cir. 2013).

[7] *ACS Const. Co. of Miss. v. CGU*, 332 F.3d 885, 888 (5th Cir. 2003).

[8] *McBeth v. Carpenter*, 565 F.3d 171, 176 (5th Cir. 2009) ("A federal court sitting in diversity applies state substantive law.").

[9] *ACS*, 332 F.3d at 888 (citing *Clark v. State Farm Mut. Auto. Ins. Co.*, 725 So.2d 779, 781 (Miss. 1998)).

[10] *Id.*

[11] *Alford*, 716 F.3d at 913.

[12] *Id.*

[13] *Wiley v. State Farm Fire & Cas. Co.*, 585 F.3d 206, 212 (5th Cir. 2009).

[14] *J & W Foods Corp. v. State Farm Mut. Auto. Ins. Co.*, 723 So.2d 550, 552 (Miss. 1998).

[15] *Id.*

> transfer, payment, or delivery of Covered Property from the Premises or Transfer Account to a person, place, or account beyond the Insured Entity's control, *without the Insured Entity's knowledge or consent*.

The district court and the parties on appeal focus on whether the loss "result[ed] directly from" the fraud scheme, but we first consider whether that provision was intended to cover the fraud scheme that occurred in this case. The policy defines "Computer Transfer Fraud" as "the fraudulent entry of Information into or the fraudulent alteration of any Information within a Computer System." "Information" is further defined as "electronic data and computer programs." "Electronic Data," in turn, means "facts or information converted to a form which is usable in a Computer System and stored on electronic processing media for use by a Computer Program." "Computer Program" is defined as "a set of related electronic instructions that direct and enable a Computer System to receive, process, store, retrieve, send, create, or otherwise act upon Electronic Data." Finally, "Computer System" is defined as "computer hardware, software and all components thereof linked together through a network of devices accessible through the internet . . . that are operated by . . . the Insured Entity and used to collect, transmit, process, maintain, store and retrieve Electronic Data."

MSH contends that the receipt of the fraudulent email falls within the Computer Transfer Fraud provision. Axis argues that the instant scheme does not constitute Computer Transfer Fraud because the scheme only involved emails that "did not have any functionality that permitted them to do anything other than sit in [MSH's] email system," and suggests that some kind of "hacking" is required.

Both this court and others have ruled that the mere receipt of an email does not constitute computer fraud in the context of similar insurance

provisions.[16] Although the instant scheme involved the creation of a "fraudulent channel" in MSH's email system through which the scammers could monitor and, when necessary, alter emails sent between MSH and Energoprom, we agree that the manipulation of emails in this manner does not constitute Computer Transfer Fraud as defined by the insuring agreement. The fraudsters apparently gained access to the company's email system, but they did not manipulate those systems through the introduction of data or programs that could independently instruct the Computer System "to receive, process, store, retrieve, send, create, or otherwise act upon Electronic Data." At best, the breach allowed the fraudsters to monitor the computer system and to act based on the information they learned.

Additionally, contract terms cannot be read in isolation. Even if we were to assume that the instant scheme constituted Computer Transfer Fraud, other language in the provision clearly suggests that this was not the type of scheme Axis agreed to insure MSH against. The provision only covers losses resulting from Computer Transfer Fraud that "causes the transfer . . . of Covered Property from [the Insured's account] to a[n] . . . account beyond the Insured Entity's control, *without the Insured Entity's knowledge or consent*." MSH argues on appeal that the district court erred in concluding

---

[16] *See Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252, 258 (5th Cir. 2016) ("To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would . . . convert the computer-fraud provision to one for general fraud."); *see also Taylor & Lieberman v. Fed. Ins. Co.*, 681 F. App'x 627, 629 (9th Cir. 2017) ("First, there is no support for [an insured's] contention that sending an email, without more, constitutes an unauthorized entry into the recipient's computer system."); *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 656 F. App'x 332, 333 (9th Cir. 2016) ("Because computers are used in almost every business transaction, 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."); *Kraft Chem. Co., Inc. v. Fed. Ins. Co.*, 2016 WL 4938493, at *6 (Ill. Cir. Ct. Jan. 05, 2016) ("The gravamen of Plaintiff's allegations giving rise to the purported fraud emanate from the transmission of an email containing a fraudulent address from the sender. As a matter of law, this without more cannot constitute computer fraud pursuant to the Policy.").

that "the *transfers* must be without Mississippi Silicon's knowledge or consent – not that the *fraud* must be."[17]

The policy means what it says: Coverage under the Computer Transfer Fraud provision is available only when a computer-based fraud scheme causes a transfer of funds without the Insured's knowledge or consent. Here, three MSH employees affirmatively authorized the transfer; it therefore cannot be said that the fraud caused a transfer without the company's knowledge. Had Axis intended, as MSH suggests, to only protect against employee collusion, it could have limited the provision to transfers that occur "without the Insured Entity's knowledge of or consent to the Computer Transfer Fraud." Rather than include such language, however, the agreement plainly limits coverage to instances in which the *transfer* is made without knowledge or consent.[18]

---

[17] In support of this argument, MSH cites *Medidata Solutions, Inc. v. Federal Insurance Co.*, in which the court held that Medidata's knowledge of a transfer was insufficient to preclude coverage under a provision that compensated the insured for losses resulting from "fraudulent . . . instructions" purporting to be from Medidata directing a bank to transfer funds "without [Medidata's] knowledge or consent" because "the validity of the wire transfer depended upon [Medidata's] knowledge and consent which was only obtained by trick." 268 F. Supp. 3d 471, 480 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018). However, the relevant portion of *Medidata* involved a *funds* transfer fraud provision, not a *computer* transfer fraud provision, and the use of the word "fraudulent" as a modification of "instruction" suggests that the Medidata's knowledge of the fraudulent nature of the instruction, rather than just the instruction itself, is relevant to coverage. Further, although *Medidata* arguably supports MSH's position, it is not binding, and applying its analysis would require us to overlook the plain language that the instant policy employs.

Moreover, other courts have held the exact opposite. For example, in *Taylor*, the Ninth Circuit denied coverage under a policy that covered fraudulent instructions issued to a financial institution to transfer funds from the insured's account "without an Insured Organization's knowledge or consent" because "although [the Insured] did not know that the emailed instructions were fraudulent, it did know about the wire transfers." 681 F. App'' at 629; *see also Sanderina, LLC v. Great Am. Ins. Co.*, 2019 WL 4307854, at *4 (D. Nev. Sept. 11, 2019).

[18] Consider, by way of contrast, the insurance provision in *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, 944 F.3d 886 (11th Cir. 2019). That provision covered

Moreover, the policy already limited coverage in the manner MSH suggests. The Policy also contained coverage (which MSH received) for Social Engineering Fraud, which is defined as follows:

> The Insurer will pay for loss of Money or Securities resulting directly from the transfer, payment, or delivery of Money or Securities from the Premises or a Transfer Account to a person, place, or account beyond the Insured Entity's control by:
>
> > a. an Employee acting in good faith reliance upon a telephone, written, or electronic instruction that purported to be a Transfer Instruction but, in fact, was not issued by a Client, Employee or Vendor[.]

The policy admittedly anticipates situations in which one fraud could fall under various fraud-related provisions.[19] The fact that MSH recovered under the Social Engineering Fraud provision in the instant case is not itself dispositive. However, as the district court noted, the Social Engineering Fraud provision specifically contemplates situations in which an employee relies in good faith on a fraudulent instruction. The Computer Transfer Fraud provision does not. Instead, the Computer Transfer Fraud provision specifically disclaims coverage for transfers made with the insured's

---

losses resulting from a "fraudulent instruction" that "direct[ed] a financial institution to debit [Principle's] transfer account and transfer, pay or deliver money or securities from that account." *Id.* at 889. A fraudulent instruction was defined as an "electronic or written instruction initially received by [Principle], which instruction purports to have been issued by an employee, but which in fact was fraudulently issued by someone else without [Principle's] or the employee's knowledge or consent." *Id.* at 890. The *Principle* policy clearly indicates that the insured's knowledge about the fraud itself would preclude coverage, but does not limit coverage to instances when the resulting *transfer* is unknown to the insured.

[19] Considering the fact that the policy states that "[i]f a single loss is covered under more than [one] Coverage, the limit of Insurance that applies to such loss will not exceed the highest Limit of Insurance for each loss that applies," the district court concluded that "the fact that the Social Engineering Fraud provision is applicable on these facts does not preclude MSH from obtaining additional coverage if a different provision with a higher policy limit is in fact applicable." We agree with this sound reasoning.

knowledge. Had Axis intended to provide coverage in instances of Computer Transfer Fraud when MSH knew of the transfer but, in good faith, believed it to be legitimate, that provision would have said so.

Our obligation to read the integrated provision as a whole bolsters our conclusion that coverage is not due. Although Computer Transfer Fraud is subject to a precise definition under the policy, the specific provision plainly does not extend to all instances of Computer Transfer Fraud—only to those that caused a funds transfer *without* MSH's knowledge. By imposing the knowledge requirement, the policy narrowed the scope of the provision, limiting the types of computer transfer fraud that would trigger coverage to instances in which a computer itself is tricked into fraudulently transferring funds from MSH's bank account to a third party without MSH's knowledge. Unfortunately for MSH, coverage simply does not extend to the fraud scheme at issue here.

Because we conclude that the MSH's knowledge of (and involvement in) the instant transfer precludes coverage in this case, we need not address whether its loss "result[ed] directly from" the fraud scheme.[20] Further, because we agree that the policy clearly and unambiguously precludes coverage, we conclude that the district court did not abuse its discretion in concluding that MSH's objections to the magistrate judge's discovery ruling were moot.[21]

---

[20] This is a complicated question we will, no doubt, need to answer one day. But because we can resolve this case on simpler grounds, today is not that day. *Compare Principle,* 944 F.3d at 892 (interpreting the phrase as implying a proximate causation standard in the context of a similar insurance policy) *with Interactive Commc'ns Int'l, Inc. v. Great Am. Ins. Co.,* 731 F. App'x 929, 931 (11th Cir. 2018) (unpublished) (applying a "direct means direct" approach because "one thing results 'directly' from another if it flows straightway, immediately, and without any intervention or interruption") *and with Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455, 460 (6th Cir. 2018) (declining to decide whether "direct" means immediate or proximate because coverage was available under either definition).

[21] On appeal, MSH also argues that the district court erred in denying as moot MSH's objections to a magistrate judge's discovery order that prevented MSH from

AFFIRMED.

compelling the production of documents related to subsequent modifications made to the language of the crime coverage provisions of the insurance policy. The magistrate judge denied the request, citing Federal Rule of Evidence 407, which bars evidence of subsequent remedial measures to prove culpable conduct, and noting that MSH had not shown why the requested information would be relevant. MSH objected to the ruling, but the district court denied those objections in its summary judgment ruling, explaining that because the policy unambiguously prevented MSH from recovering under the policy, any subsequent changes in the policy's language were irrelevant and the objections thus moot.