IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 15-20499

United States Court of Appeals
Fifth Circuit
FILED
October 18, 2016
Lyle W. Cayce
Clerk

APACHE CORPORATION,

Plaintiff – Appellee Cross-Appellant

v.

GREAT AMERICAN INSURANCE COMPANY,

Defendant – Appellant Cross-Appellee

Appeals from the United States District Court
for the Southern District of Texas
USDC No. 4:14-CV-237

Before JOLLY, BARKSDALE, and SOUTHWICK, Circuit Judges.

PER CURIAM*

Texas law controls this diversity action, which arises out of Apache Corporation's being defrauded by criminals, in part by their use of an email; as a result of the fraud, and a flawed follow-up investigation by Apache, it made authorized payments of legitimate invoices from its vendor to the criminals' bank account, instead of to its vendor's. Great American Insurance Company (GAIC), Apache's insurer, denied its claim for coverage of its loss under GAIC's "Computer Fraud" provision of Apache's crime-protection insurance policy. At

* Pursuant to 5th Cir. R. 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5th Cir. R. 47.5.4.

issue is whether the district court correctly awarded summary judgment to Apache, on the basis that its loss was covered under that provision; and, if so, whether the court properly denied statutory penalties, subject to Texas Insurance Code § 542.060. VACATED and RENDERED.

I.

GAIC is headquartered in Ohio; Apache is an oil-production company, with its principal place of business in Houston, Texas, but operating internationally. In March 2013, during the coverage period for Apache's policy with GAIC, an Apache employee in Scotland received a telephone call from a person identifying herself as a representative of Petrofac, a vendor for Apache. The caller instructed Apache to change the bank-account information for its payments to Petrofac. The Apache employee replied that the change-request could not be processed without a formal request on Petrofac letterhead.

A week later, Apache's accounts-payable department received an email from a "petrofacltd.com" address. But, Petrofac's authentic email domain name is "petrofac.com"; the criminals created "petrofacltd.com" to send the fraudulent email. The email advised: Petrofac's "accounts details have now been changed"; and "[t]he new account takes . . . immediate effect and all future payments must now be made into this account". As noted in the email, an attachment to it was a signed letter on Petrofac letterhead, providing both old-bank-account information and the new-bank-account number, with instructions to "use the new account with immediate effect". In addition, the email stated: the "attached letter . . . has also been posted to you".

In response, an Apache employee called the telephone number provided on the letterhead to verify the request and concluded the call confirmed the authenticity of the change-request; next, a different Apache employee

approved and implemented the change. A week later, Apache was transferring funds for payment of Petrofac's invoices to the new bank account.

Within one month, however, Apache received notification Petrofac had not received the £4.3 million (approximately $7 million) Apache had transferred to the new (fraudulent) account. After an investigation determined the criminals were likely based in Latvia, Apache recouped a substantial portion of the funds. It contends, however, it suffered a loss, before the $1 million policy deductible, of approximately £1.5 million (approximately $2.4 million).

Apache submitted a claim to GAIC, asserting coverage under the "Computer Fraud" provision, which states:

> We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:
>
> a. to a person (other than a messenger) outside those premises; or
>
> b. to a place outside those premises.

In its denial letter, GAIC advised Apache's "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds".

Apache initiated this action in Texas state court in January 2014 against GAIC for denying its claim under the computer-fraud provision. After GAIC removed the action to district court, both parties moved for summary judgment.

The court denied GAIC's motion and granted Apache's, ruling, *inter alia*, "the intervening steps of the [post-email] confirmation phone call and

supervisory approval do not rise to the level of negating the email as being a 'substantial factor'". *Apache Corp. v. Great Am. Ins. Co.*, Civil Action No. 4:14-CV-237, 2015 WL 7709584, at *3 (S.D. Tex. 7 Aug. 2015). Moreover, the court reasoned that, if the policy only covered losses due to computer hacking, such an interpretation would render the policy "pointless". *Id.*

Apache moved for entry of final judgment, and sought, *inter alia*, statutory penalties under Texas Insurance Code § 542.060. But, in entering judgment, the court denied the penalties.

II.

GAIC challenges the summary judgment awarded Apache; on the other hand, Apache challenges the denial of statutory penalties. Because we vacate the judgment and render it for GAIC, we do not reach the penalties issue.

A summary judgment is reviewed *de novo*. *E.g.*, *Southern Ins. Co. v. Affiliated FM Ins. Co.*, 830 F.3d 337, 343 (5th Cir. 2016). Summary judgment is proper if the movant shows no genuine dispute as to any material fact and entitlement to judgment as a matter of law. Fed. R. Civ. P. 56(a). "The court must view the facts developed below in the light most favorable to the non-moving party." *La. Generating, L.L.C. v. Ill. Union Ins. Co.*, No. 15-30914, --- F.3d ----, 2016 WL 4150902, at *2 (5th Cir. 4 Aug. 2016). A genuine dispute of material fact exists "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party". *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). Interpretation of an insurance policy presents a question of law; therefore it is also reviewed *de novo*. *E.g.*, *Naquin v. Elevating Boats, L.L.C.*, 817 F.3d 235, 238 (5th Cir. 2016).

The summary-judgment record is very limited—there were no depositions or discovery responses. For its motion, GAIC attached: Apache's

proof of loss and supporting documents, such as the email at issue and the letterhead attachment to it; the crime-protection policy; and Apache's declination letter. Apache relied on GAIC's exhibits, in addition to two very brief, self-serving declarations executed by two Apache employees.

As noted, Texas law controls this diversity action. GAIC claims, *inter alia*, the loss was not a covered occurrence because: the email did not "cause a transfer"; and coverage under this provision is "unambiguously limited" to losses from "hacking and other incidents of unauthorized computer use". GAIC notes that, under Texas law, insurance provisions are interpreted according to the same rules applicable to contracts generally; but, it also asserts the "Supreme Court of Texas has 'repeatedly stressed the importance of uniformity when identical insurance provisions will necessarily be interpreted in various jurisdictions'", citing *McGinnes Indus. Maint. Corp. v. Phoenix Ins. Co.*, 477 S.W.3d 786, 794 (Tex. 2015). According to GAIC, the weight of authorities interpreting similar computer-fraud language, considered with Texas' policy goal of cross-jurisdictional uniformity, persuades against coverage for Apache's claim.

Apache counters that the plain meaning of the computer-fraud language covers its loss, and maintains any ambiguity in the terms should be resolved in favor of the insured's reasonable interpretation, even if the insurer's interpretation is more reasonable, relying on *RSUI Indem. Co. v. Lynd Co.*, 466 S.W.3d 113, 118 (Tex. 2015). Because the language of the provision says nothing about "hacking", Apache asserts it only needs to show that "any computer was used to fraudulently cause the transfer of funds".

As noted, under Texas law, courts interpret insurance policies using the same rules of construction applicable to contracts generally. *Tesoro Ref. & Mktg. Co., L.L.C. v. Nat'l Union Fire Ins. Co. of Pitt., Pa.*, No. 15-50405, --- F.3d ----, 2016 WL 4166173, at *2 (5th Cir. 29 July 2016); *Am. Mfrs. Mut. Ins. Co. v.*

Schaefer, 124 S.W.3d 154, 157 (Tex. 2003). The policy must be construed such that no provision is rendered meaningless. *Tesoro*, 2016 WL 4166173, at *2 (citing *Schaefer*, 124 S.W.3d at 157).

Mere disagreement about the meaning of a contract does not render it ambiguous. *Id.* "A contract is ambiguous only when the application of pertinent rules of interpretation to the face of the instrument leaves it genuinely uncertain which one of two or more meanings is the proper meaning." *Id.* (quoting *RSUI Indem.*, 466 S.W.3d at 119). The ambiguity, *vel non*, of an insurance provision is a question of law; if ambiguity is found, the court must adopt the interpretation favoring the insured. *Id.* (citing *RSUI Indem.*, 466 S.W.3d at 118; *Schaefer*, 124 S.W.3d at 157).

As also noted, the Texas Supreme Court has stressed its policy preference for "uniformity when identical insurance provisions will necessarily be interpreted in various jurisdictions". *McGinnes*, 477 S.W.3d at 794 (responding to fifth circuit certified question). And, even when uniformity is made impossible by jurisdictional splits, Texas courts "strive for uniformity as much as possible". *Id.* (internal quotation marks omitted) (quoting *Trinity Universal Ins. Co. v. Cowan*, 945 S.W.2d 819, 824 (Tex. 1997)).

For our *Erie*-guess, the parties agree that only the computer-fraud provision is at issue. In contending Apache's loss is not covered under it because the loss did not, as required by the provision, "result[] directly from the use of any computer to fraudulently cause a transfer", GAIC maintains the transfer of funds to the fraudulent bank account resulted from other events: before the email, the telephone call directing Apache to change the account information; and, after the email, the telephone call by Apache to the criminals to confirm the change-request, followed by the Apache supervisor's review and approval of the emailed request, Petrofac's submission of invoices, the review

and approval of them by Apache employees, and Apache's authorized and intentional transfer of funds, even though to the fraudulent bank account. (As discussed, the email stated that the attached letter on Petrofac letterhead "has also been posted [mailed] to" Apache. There is no evidence in the summary-judgment record, however, that Apache received a hardcopy of the letter. Nor is there any evidence Apache relied on one, as opposed to the electronic version attached to the fraudulent email, in telephoning to confirm the information provided. In any event, although this mailed-letter point was presented by GAIC at oral argument here, it is waived because it was not raised in district court or in GAIC's opening brief on appeal, with the alleged mailing of the letter only noted belatedly in its reply brief.)

In response to GAIC's position, Apache claims the loss is covered, based on the "commonly understood meaning" of the computer-fraud-provision's terms. It asserts GAIC attempts to add terms it wishes had been included in the provision.

The parties do not cite any Texas authority interpreting "the use of any computer to fraudulently cause a transfer" in the context of the computer-fraud provision, nor have we found any. Instead, GAIC relies primarily on unpublished opinions as persuasive authority; none are by Texas courts and almost all are outside our circuit. Apache attempts to distinguish them. Bearing in mind the limited weight accorded such non-binding authority, as well as Texas' policy preference for cross-jurisdictional uniformity, a detailed—albeit numbing—analysis of the cited authorities is required. *See McGinnes*, 477 S.W.3d at 794.

GAIC cites the ninth circuit's decision in *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, affirming coverage-denial under a similarly worded computer-fraud provision. (*Pestmaster II*), No. 14-56294, --- Fed. App'x

----, 2016 WL 4056068, at *1 (9th Cir. 29 July 2016), *aff'g Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.* (*Pestmaster I*), No. CV 13-5039-JFW, 2014 WL 3844627 (C.D. Cal. 17 July 2014) (unpublished). That policy defined "computer fraud" as "[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property". *Pestmaster I*, 2014 WL 3844627, at *4.

The underlying fraud was committed by a payroll contractor against the insured. *Id.* at *1. The contractor had been hired, *inter alia*, to withhold and submit payments for the insured's payroll taxes. *Id.* To that end, the contractor prepared invoices for the insured, and was authorized to initiate transfers of funds from the insured to the contractor's bank account, in order to pay invoices approved by the insured. *Id.* (The district court considered the contractor's initiating the transfer of funds as the relevant "use of a computer". *Id.* at *7–8.) Instead of paying the approved invoices, the contractor fraudulently used the insured's funds to pay her own expenses, ultimately leaving the insured indebted to the Internal Revenue Service for payroll taxes. *Id.* at *2, 7–8.

The insured filed an action after being denied coverage under the crime-protection policy for the tax debt; but, the district court rejected coverage under the computer-fraud provision because the "claimed losses did not 'flow immediately' and 'directly' from [the contractor's] use of a computer". *Id.* at *8. "[T]here was no loss when funds were initially transferred to [the contractor] because the transfers were authorized by [the insured]". *Id.*

In affirming, the ninth circuit interpreted "the phrase 'fraudulently cause a transfer' to require an unauthorized transfer of funds". *Pestmaster II*, 2016 WL 4056068, at *1. "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", essentially covering losses from all forms of fraud rather than a specified risk category. *Id.*

GAIC also cites *Brightpoint, Inc. v. Zurich Am. Ins. Co.*, in which a district court ruled similar policy language did not cover a loss claimed by an insured distributor of prepaid mobile-telephone cards. No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377, at *7 (S.D. Ind. 10 March 2006) (unpublished). After the distributor received a facsimile-transmission of purchase orders, post-dated checks, and bank guarantees from a purported customer, the distributor delivered the inventory in exchange for the original documents. *Id.* at *2. The transaction was a fraud, with the distributor's never receiving payment. *Id.* at *3.

The court assumed, without deciding, that the facsimile-transmission constituted "use of a computer". In concluding the loss was not covered, it stated:

> We do not view the faxed [documents] to have "fraudulently cause[d] a transfer" of the phone cards, as required under the policy definition of "Computer Fraud." . . . [T]he facsimile simply alerted the [insured] to the fact that [the insured's customer], or perhaps in this case some other person mimicking his methods, wished to place an order. Only after [the insured] received the physical documents would [it] release the phone cards and, based on established practices of [the insured], the cards would not have been turned over simply on the basis of the facsimile.

Id. at *7.

Additionally, GAIC points to a summary-judgment ruling in its favor by the Northern District of Texas. *See GAIC v. AFS/IBEX Fin. Servs., Inc.*, No. 3:07-CV-924-O, 2008 WL 2795205, at *2 (N.D. Tex. 21 July 2008)

(unpublished). There, an employee of the insured insurance-premium-finance company used a computer to submit more than 100 false loan applications to induce the insured to issue checks that the employee deposited for personal use. *Id.* The insured's claim with GAIC sought coverage under, *inter alia*, the computer-fraud provision of a crime-protection insurance policy; the claim was denied. *Id.*

As in this instance, the computer-fraud provision covered a loss "resulting directly from the use of any computer to fraudulently cause a transfer of . . . property". *Id.* at *14. The court interpreted this language as being "designed to cover losses *directly* stemming from fraud perpetrated by use of a computer". *Id.* (emphasis in original). Notably, the insured did not present "any evidence or arguments in opposition" to GAIC's claiming the provision did not apply, but the court nonetheless determined the loss was not covered. *Id.*

As GAIC notes, similar policy language was at issue in *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, but the court denied the insurer's motion to dismiss and allowed the insured's claim to go forward. No. 11-6187, 2012 WL 1067694, at *4 (D. N.J. 29 March 2012) (unpublished). The facts considered in *Vonage*, however, differ from those here, because the insured was unquestionably "hacked"—hackers gained access to the insured's servers to fraudulently route international telephone calls. *Id.* at *1.

The only decision discussed by the parties which ruled the policy language covered computer-use limited to email communications was later vacated by the Superior Court of Connecticut. *See Owens, Schine, & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, 50 Conn. L. Rptr. 665, 2010 WL 4226958, at *8 (Conn. Super. Ct. 20 Sept. 2010) (unpublished), *vacated*, 2012 WL 12246940 (Conn. Super. Ct. 18 Apr. 2012) (unpublished). The policy at

issue defined "computer fraud" as "[t]he use of any computer to fraudulently cause a transfer". *Id*. at *4.

The insured, a law firm, was defrauded by criminals who sent emails to the firm, representing themselves as Chinese businessmen in need of legal services. *Id*. at *1. All communications between the firm and the criminals were carried out by email. *Id*. at *7. A retainer agreement was signed, scanned, and emailed to the firm by the criminals. *Id*. at *1. They claimed they needed the firm's services to collect a debt owed by an American company. *Id*. After a fraudulent check was received by the firm from the supposed debtor, the firm deposited the check in its trust account. *Id*. The firm then successfully wired funds from that account to one in South Korea; but, after the firm's bank discovered the fraud, it refused to honor the fraudulent check provided by the criminals to the firm, resulting in its financial loss. *Id*. at *2.

In denying the insurer's summary-judgment motion, the court ruled "[t]he emails were the proximate cause and 'efficient cause' of [the insured's] loss because the [emails] set the chain of events in motion that led to the entire loss". *Id*. at *8. As discussed, the decision, however, was vacated by the very court that rendered it.

Again, this vacated trial-court ruling is the only presented decision interpreting the computer-fraud policy language to cover a loss when the computer use at issue was limited to email correspondence. Therefore, with the exception of the district court's ruling at issue, there is cross-jurisdictional uniformity in declining to extend coverage when the fraudulent transfer was the result of other events and not directly by the computer use.

Here, the "computer use" was an email with instructions to change a vendor's payment information and make "all future payments" to it; the email, with the letter on Petrofac letterhead as an attachment, followed the initial

telephone call from the criminals and was sent in response to Apache's directive to send the request on the vendor's letterhead. Once the email was received, an Apache employee called the telephone number provided on the fraudulent letterhead in the attachment to the email, instead of, for example, calling an independently-provided telephone contact for the vendor, such as the pre-existing contact information Apache would have used in past communications. Doubtless, had the confirmation call been properly directed, or had Apache performed a more thorough investigation, it would never have changed the vendor-payment account information. Moreover, Apache changed the account information, and the transfers of money to the fraudulent account were initiated by Apache to pay legitimate invoices.

The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would, as stated in *Pestmaster II*, convert the computer-fraud provision to one for general fraud. *See* 2016 WL 4056068, at *1. We take judicial notice that, when the policy was issued in 2012, electronic communications were, as they are now, ubiquitous, and even the line between "computer" and "telephone" was already blurred. In short, few—if any—fraudulent schemes would not involve some form of computer-facilitated communication.

This is reflected in the evidence at hand. Arguably, Apache invited the computer-use at issue, through which it now seeks shelter under its policy, even though the computer-use was but one step in Apache's multi-step, but flawed, process that ended in its making required and authorized, very large invoice-payments, but to a fraudulent bank account.

The email was sent only after Apache's advising, in reply to the criminals' change-request telephone call, that the request had to be made on Petrofac letterhead. The criminals complied: by attaching to the email (sent using a slightly different domain name) a letter on altered letterhead; and, as stated in the email, by allegedly mailing that letter to Apache. Accordingly, the computer-use was in response to Apache's refusing, during the telephone call, to, for example, transcribe the change-request, which it could have then investigated with its records.

No doubt, the better, safer procedure was to require the change-request to be made on letterhead, especially for future payment of Petrofac's very large invoices. But the request must still be investigated properly to verify it is legitimate. In any event, based on the evidence in the summary-judgment record, Apache followed-up on the request in the email and its attachment. In other words, the authorized transfer was made to the fraudulent account only because, after receiving the email, Apache failed to investigate accurately the new, but fraudulent, information provided to it.

Moreover, viewing the multi-step process in its simplest form, the transfers were made not because of fraudulent information, but because Apache elected to pay legitimate invoices. Regrettably, it sent the payments to the wrong bank account. Restated, the invoices, not the email, were the reason for the funds transfers.

In sum, and applying Texas law in making this *Erie* guess, both the plain meaning of the policy language, as well as the uniform interpretations across jurisdictions, dictate Apache's loss was not a covered occurrence under the computer-fraud provision. *See McGinnes*, 477 S.W.3d at 794.

III.

For the foregoing reasons, the judgment is VACATED and judgment is RENDERED for Great American Insurance Company.