17-2492-cv

IN THE
United States Court of Appeals
FOR THE SECOND CIRCUIT

MEDIDATA SOLUTIONS, INC.,

Plaintiff-Appellee,

vs.

FEDERAL INSURANCE COMPANY,

Defendant-Appellant.

ON APPEAL FROM A JUDGMENT, ENTERED JULY 21, 2017, OF THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK (CIVIL ACTION NO. 15-CV-907-ALC)

BRIEF OF AMICUS CURIAE SUPPORTING REVERSAL

CHIESA SHAHINIAN & GIANTOMASI PC
One Boland Drive
West Orange, New Jersey 07052
Ph. (973) 530-2054 / Fax: (973) 530-2254
email: akent@csglaw.com
Attorneys for Amicus Curiae
The Surety & Fidelity Association of America

On the Brief:
Andrew S. Kent

DISCLOSURE STATEMENT

The Surety & Fidelity Association of America (SFAA) is a District of Columbia Nonprofit Corporation. SFAA has no stockholders and it is not part of a subsidiary, conglomerate, affiliate or parent corporation. No publicly held corporation holds more than a 10% interest in SFAA.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

STATEMENT OF INTEREST

The Surety & Fidelity Association of America (SFAA) is a national trade association of companies licensed to write fidelity and surety insurance. The 414 members of SFAA write the vast majority of fidelity insurance policies issued in the United States and in New York State.[1]

In conjunction with representatives of policy-holder groups, SFAA drafts fidelity insurance policy forms[2] and files these forms with the insurance departments of all states that require the filing of fidelity forms. SFAA also collects statistics on premiums and losses under surety and fidelity bonds and files these statistics with state insurance departments. These statistics are used by SFAA member companies in determining premiums and by the state insurance departments in reviewing filed rates. SFAA is licensed by the New York Department of Financial Services as a Rating Organization.

SFAA, its members active in writing crime policies to insure commercial businesses, and the businesses insured by such policies have a mutual interest in

---

1 No counsel for a party to this appeal authored this Brief, in whole or in part. No person – other than The Surety & Fidelity Association of America and its members – contributed money to fund the preparation or submission of this Brief.

2 *See BancInsure v. Highland Bank*, 779 F.3d 565 (8th Cir. 2015) ("BancInsure's Financial Institution Bond, often referred to as a bankers blanket bond, is a version of a standard form bond initially drafted by the Surety Association of America in 1916 and modified from time to time with input from the American Bankers Association."); *First State Bank of Monticello v. Ohio Cas. Ins. Co.*, 555 F.3d 564, 568 (7th Cir. 2009) (discussing the drafting of fidelity insurance policies).

seeing that the risks of loss transferred by the insurance policies are predictable and consistent with the premiums charged. It is important to both insurers and insureds that the courts enforce these policies as written.

SFAA agrees with the arguments of defendant-appellant Federal Insurance Company (hereinafter "Federal") and will try not to repeat them. SFAA submits this amicus curiae brief primarily to address the consequences if this Court were to agree with the interpretation of the "Funds Transfer Fraud" and "Computer Fraud" insuring clauses, and related provisions of the "Executive Protection Portfolio Policy" ("the Policy") urged by the insured, plaintiff-respondent Medidata Solutions, Inc. (hereinafter "Medidata").

Pursuant to Rule 29(a)(2) of the Federal Rules of Appellate Procedure, all of the parties to this action have consented to SFAA's filing of an amicus curiae brief.

SUMMARY OF ARGUMENT

On September 16, 2014, Medidata sustained a loss when it wire transferred $4,770,226 from its account at Chase Bank to an account at a bank in China that proved to be the account of a fraudster and not of the party that Medidata thought it was paying. The District Court granted summary judgment to Medidata, holding that this loss was covered by the "Funds Transfer Fraud"[3] and "Computer Fraud"

---

3 Some of the defined terms in the subject policy appear in boldface print in the original document. To avoid confusion, this brief uses only normal typeface.

insuring clauses of the Policy.[4] Medidata's argument rests on the fact that the perpetrator of the fraud (hereinafter "the Criminal") sent the three Medidata employees involved in the wire transfer several spoofed e-mails purporting to be from Medidata's president (in addition to the Criminal placing at least one telephone call to Medidata, while holding himself out as Medidata's attorney).

The $4,770,226 transfer does not fit the Policy's definition of a Funds Transfer Fraud, and the spoofed e-mails were not a Computer Fraud. The District Court, therefore, erred in granting summary judgment to Medidata. By expanding the definitions of "Funds Transfer Fraud" and "Computer Fraud" to cover this loss – an approach rejected by the courts that most recently have determined cases involving similar facts, including the Fifth Circuit and the Ninth Circuit – the District Court's reasoning, if accepted by this Court, would have serious adverse consequences for the availability and cost of insurance coverage needed by businesses for actual funds transfer and computer frauds.

ARGUMENT

Under New York law, an unambiguous provision of an insurance contract must be enforced according to its plain and ordinary meaning. *See, e.g., The Burlington Ins. Co. v. NYC Transit Auth.,* 79 N.E.3d 477, 481 (N.Y. 2017);

---

4 Medidata also argued that its loss was covered by the "Forgery" insuring clause. The District Court rejected this argument, and SFAA understands that it is not before this Court.

Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 37 N.E.3d 78, 80 (2015). Applying this principle to the Policy and Medidata's loss, there was neither a covered Funds Transfer Fraud loss nor a covered Computer Fraud loss.

I. There Was No "Funds Transfer Fraud"

Insuring Clause 6 of the Policy covers the direct loss of "Money … resulting from Funds Transfer Fraud committed by a Third Party." (A-206) "Third Party", in turn, means "a natural person other than: (a) an Employee; or (b) a natural person acting in collusion with an Employee." (A-211)

The Policy defines "Funds Transfer Fraud" as follows:

> Funds Transfer Fraud means fraudulent electronic . . . instructions (other than Forgery), purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, without such Organization's knowledge or consent.

(A-209)

Medidata was an "Organization", and Chase Bank was a "financial institution", but the only transfer instruction issued "to" Chase was not issued by a "Third Party". There was no dispute that the wire transfer instructions were in fact issued to Chase by an employee of Medidata, with Medidata's knowledge and consent. Indeed, the whole point of the Criminal's telephone call and spoofed e-mails was to get Medidata's authorized employees to make the transfer. Ms. Evans in the Accounts Payable Department, Mr. Chin, Medidata's vice president, and Mr.

Schwartz, Medidata's Director of Revenue, all knew of the transfer and affirmatively approved it. Therefore, there was no Funds Transfer Fraud "committed by a Third Party." Medidata, acting through its authorized officers and employees, both knew of the transfer and consented to it.

In *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, 656 F. App'x 332 (9th Cir. 2016), the Ninth Circuit affirmed a judgment for the insurer under substantially similar facts. In rejecting the insured's "Funds Transfer Fraud" arguments, the Ninth Circuit stated:

> First, Pestmaster argues that the transfer of funds from its bank account to Priority 1's bank account is covered by the Funds Transfer Fraud provision. The district court found that this provision "does not cover authorized or valid electronic transactions . . . even though they are, or may be, associated with a fraudulent scheme." We agree that there is no coverage under this clause when the transfers were expressly authorized.

Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332, 333 (9th Cir. 2016).

In *Taylor & Lieberman v. Federal Insurance Co.*, 681 F. App'x 627 (9th Cir. 2017), which involved a "Funds Transfer Fraud" provision that, like the one in the instant case, required that the transfer instruction be made "without an Insured Organization's knowledge or consent", the Ninth Circuit held:

> This coverage is inapplicable because T&L requested and knew about the wire transfers. After receiving the fraudulent emails, T&L directed its client's bank to wire the funds. T&L then sent emails confirming the transfers to its client's email address. Although T&L

> did not know that the emailed instructions were fraudulent, it did know about the wire transfers.

Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627, 629 (9th Cir. 2017).

In the instant case, the District Court attempted to distinguish *Pestmaster* and *Taylor & Lieberman* when it concluded:

> The fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer depended upon several high level employees' knowledge and consent which was only obtained by trick. As the parties are well aware, larceny by trick is still larceny. Therefore, Medidata has demonstrated that the Funds Transfer Fraud clause covers the theft in 2014.

Medidata Solutions, Inc. v. Fed. Ins. Co., No. 15-CV-907 (ALC), 2017 WL 3268529, *7 (S.D.N.Y. July 21, 2017).

In attempting to distinguish prior decisions like *Pestmaster* and *Taylor & Lieberman,* the District Court misapprehended the Funds Transfer Fraud insuring clause. The clause does not provide coverage for all electronic funds transfers tainted by fraud, nor "larceny by trick." It covers funds transfer fraud "committed by a Third Party" in the (defined) form of a fraudulent electronic or written instruction "issued to a financial institution" made without the knowledge or consent of the insured; for example, if the Criminal (a "Third Party" under the Policy) had obtained the user credentials of the employees and logged into the Chase Bank system to make the transfers without Medidata's knowledge or

consent. Such outwitting of the computer system is a very different risk than misleading the insured's human employees – who have the ability to take reasonable steps to confirm the legitimacy of a wire transfer request or direction received by e-mail – and who then make an authorized transfer based upon such request or direction. Here, the only person who submitted a funds transfer instruction "to" a financial institution was an authorized employee of the insured itself, who did so with the Insured's knowledge and consent. Medidata's loss therefore did not fall within the Funds Transfer Fraud coverage.

II. There Was No "Computer Fraud"

The Policy defines Computer Fraud as "the unlawful taking or the fraudulently induced transfer of Money, Securities, or Property resulting from a Computer Violation." (A-207) It then defines "Computer Violation" as follows:

> Computer Violation means the fraudulent:
>
> (a) entry of Data into or deletion of Data from a Computer System;
>
> (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format; or
>
> (c) introduction of instructions, programmatic or otherwise, which propagate themselves through a Computer System,
>
> directed against an Organization.

(A-207 – A-208)

In *Universal American Corp. v. National Union Fire Ins. Co. of Pittsburgh, Pa.*, 37 N.E.3d 78 (N.Y. 2015), the New York Court of Appeals considered similar language and held that it does not provide coverage for losses resulting from the authorized entry of fraudulent data into the insured's computer system. That is, the word "fraudulent" modifies "entry" (the act), not "data" (what is entered). The Court of Appeals stated:

> The rider's reference to "fraudulent" does not also qualify what is actually acted upon, namely the "electronic data" or "computer program" itself. The intentional word placement of "fraudulent" before "entry" and "change" manifests the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access.

Universal Am., 37 N.E.3d at 81.

In the instant case, it was the content of the e-mails that was fraudulent, not the access, *i.e.,* not the act that caused the transfer. The Joint Stipulation of Findings Following Expert Discovery establishes how the Criminal sent the e-mails, and confirms that there was no hacking of, fraudulent entry into, or use of Medidata's computer system outside of the sending/receipt of the e-mails. (A-661, Joint Stipulation, at ¶¶ 33-37.) Medidata's computer system did exactly what it was supposed to do – it forwarded the e-mails to the intended recipients' mailboxes. There was no change to the computer system, and no fraudulent access to the system – Medidata's computer system, like just about every system, allowed anyone to send it an e-mail.

Medidata relies upon the addition of its president's picture and information to the e-mails, but that is what the computer system was programmed to do. The Criminal did nothing to cause these additions. They were part of Medidata's e-mail system as it existed before and after the Criminal's e-mails. Moreover, there was no evidence from which to conclude that the Criminal knew that his "spoofed" e-mail even would cause that picture to appear. The Criminal simply sent e-mails falsely representing that they were sent by Medidata's president.

In *Apache Corp. v. Great American Insurance Co.*, 662 F. App'x 252 (5th Cir. 2016) – another case involving very similar facts – the Fifth Circuit reversed the lower court's award of summary judgment to the insured. A criminal called the insured and sent an e-mail purportedly from one of the insured's vendors asking that future payments to the vendor be sent to a specified bank account. The insured complied and suffered a substantial loss when the payments went into the account of the criminal and not the vendor. The District Court held that the loss was a covered "computer fraud", and the insurer appealed. The Fifth Circuit reversed, concluding "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." *Apache,* 662 F. App'x at 259.

Similarly, in *Taylor & Lieberman*, the Ninth Circuit held that sending e-mails with fraudulent payment instructions was not a basis for coverage under the computer fraud provision of that policy. *Taylor & Lieberman,* 681 F. App'x at 629. *Kraft Chemical Co. v. Federal Ins. Co.*, No. 13 M2 002568, 2016 WL 4938493 (Ill. Cir. Ct. Jan. 5, 2016), is a recent trial court decision similarly holding that fraudulent e-mails were not an unauthorized entry into or an unauthorized change to the insured's computer system for purposes of the "computer violation" provision of the subject policy.

The only involvement of Medidata's computer system in its loss was its transmission of e-mails as it was designed to do. The Criminal did not alter or re-program the computer system or any data stored in it. Given the ubiquity of e-mail in modern business, concluding that what occurred here constitutes covered "computer fraud" would render almost every theft a covered "computer fraud", which patently is not the intention of the "computer fraud" coverage in the Policy or any similar policy. The lower court erred when it concluded that Medidata's loss was covered "computer fraud".

III. If Accepted by This Court, Medidata's Argument Would Drastically Increase the Cost and Decrease the Availability of Insurance Against True Computer Fraud

As mentioned above, Medidata's argument in this case would convert the "computer fraud" insuring agreement into coverage for any loss involving an e-

mail. Medidata essentially argues that there were fraudulent statements in the e-mails, therefore there was "computer fraud". In modern commerce, however, e-mail communications are routine. The conclusion that any loss involving fraudulent or misleading e-mails is a covered "computer fraud" under the language of Federal's policy, or any other typical "computer fraud" coverage, is not reasonable.

It would not be difficult to write an insurance policy that protected against any loss caused by fraudulent statements in an e-mail. The premium for such a policy, however, would be utterly prohibitive. An insured is far better off exercising prudent business practices to prevent fraud losses that it can control through reasonable internal controls, and insuring against only those losses that it cannot reasonably or efficiently prevent. For example, all businesses run the risk of loss from employee dishonesty. Fidelity bonds, however, exclude the risk of loss caused by an employee after the employer knows he or she is dishonest.[5] It is far more efficient not to continue employment of known crooks than to insure against the inevitable losses they will cause.

---

5 For example, Exclusion 13 on page 10 of 17 of the Policy terminates coverage as to any employee if a responsible officer of the Insured knows of a dishonest act by that employee while employed by the Insured or of a dishonest act exceeding $25,000 committed prior to such employment.

Under Medidata's interpretation, the Computer Fraud provision of the Policy would convert virtually any fraud into a covered loss as long as a computer was used somewhere in the course of the transaction, even if the computer was used simply to send an e-mail or prepare a letter or other document. This not only is not what the "computer fraud" coverage provides, it would change "computer fraud" coverage into simple "fraud" coverage. To be covered, "computer fraud" must require some type of unauthorized manipulation of the insured's computer system, not merely sending an e-mail to an insured.

An example of covered "computer fraud" would be if a criminal accessed the insured's computer system, such as by obtaining an employee's user name and password or other identifying or verifying information, and used this unauthorized access to enter fraudulent data or instructions, thereby directly causing an automated transfer of property or funds belonging to the insured. The insured has neither opportunity nor discretion to stop the loss from occurring. By contrast, in the instant case, the fraud was limited to the content of the e-mails requesting that Medidata wire transfer money to a specific bank account to further an alleged corporate acquisition. Medidata had ample opportunity to verify the contents of the e-mails, and made the transfers of its own volition. The Criminal never accessed Medidata's computer system or caused Medidata's computer system to

effect a funds transfer. Throughout this event, Medidata's computer system functioned exactly as it was supposed to function.

As stated above, Medidata had multiple opportunities to discover the fraud before it made the payments. In fact, when the Criminal tried to repeat the fraud two days later, one of Medidata's employees noticed that the "reply to" e-mail address was not a Medidata address, and a phone call to Medidata's president exposed the fraud. It would seem prudent to have confirmed the transaction before wiring $4.7 million to China.[6] As the Fifth Circuit said in *Apache,* "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." *Apache,* 662 F. App'x at 259.

If Medidata's arguments were to prevail, the "computer fraud" coverage that businesses require will become extremely expensive, as the insurer will be called upon to pay avoidable losses involving e-mail. In effect, in the modern world, the insurer would be providing very broad coverage and would have to underwrite and charge accordingly. As the Ninth Circuit said in *Pestmaster*:

> 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

---

6 Indeed, one of the employees misunderstood a statement by Ms. Evans and as a result thought she had verbally confirmed the requested transfer with Medidata's president.

> this Crime Policy into a "General Fraud" Policy. While Travelers could have drafted this language more narrowly, we believe protection against all fraud is not what was intended by this provision, and not what Pestmaster could reasonably have expected this provision to cover.

Pestmaster, 656 F. App'x at 333.

Recent, well-publicized events have demonstrated the difficulty of maintaining cyber security. Prudent businesses need to insure against losses resulting from hackers entering fraudulent data or instructions in their computer systems. If "computer fraud" insurance is construed so overbroadly to cover losses resulting from e-mails that fool the insured's employees, who do not take commercially reasonable steps to confirm the substance of the e-mails, such insurance will become much harder to obtain and substantially more expensive.

CONCLUSION

SFAA respectfully urges this Court to reverse the District Court and enter judgment for Federal. Neither the "funds transfer fraud" nor the "computer fraud" insuring clauses of the Policy cover Medidata's loss.

Respectfully submitted,

CHIESA SHAHINIAN & GIANTOMASI PC
Attorneys For
Amicus Curiae
The Surety & Fidelity Association
of America

/s/
Andrew S. Kent, Esq.

Dated: November 28, 2017

CERTIFICATE OF COMPLIANCE

In Accordance With Fed. R. App. P. Rule 32(a)

I, Andrew S. Kent, Esq., hereby certify as follows:

(1) The foregoing Brief of Amicus Curiae, The Surety & Fidelity Association of America, is in compliance with type-volume limitation and typeface requirements and type style requirements.

(2) This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains **3,271** words, excluding the parts of the brief exempted by Fed. R. App. P. 32 (a)(7)(B)(iii), as calculated by the Microsoft Word 2010 word processing system used to prepare the brief.

(3) This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32 (a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 word processing program in font size 14 in Times New Roman type style.

Dated: November 28, 2017

/s/
Andrew S. Kent, Esq.

CHIESA SHAHINIAN & GIANTOMASI PC
One Boland Drive
West Orange, New Jersey 07052
Attorneys for Amicus Curiae
The Surety & Fidelity Association of America