268 F.Supp.3d 471
United States District Court, S.D. New York.

MEDIDATA SOLUTIONS, INC., Plaintiff,
v.
FEDERAL INSURANCE CO., Defendant

15–CV–907 (ALC)
|
Signed 07/21/2017

Synopsis

Background: Insured corporation, which wired millions of dollars to unknown actor as a result of e-mail "spoofing" scheme, brought action against insurer, challenging insurer's denial of insured's claim under policy covering losses caused by certain criminal and fraudulent acts. Parties filed cross-motions for summary judgment.

Holdings: The District Court, Andrew L. Carter, Jr., J., held that:

[1] insured's losses were covered under computer fraud clause;

[2] insured's losses were covered under funds transfer fraud clause; and

[3] insured's losses were not covered by forgery clause.

Insured's motion granted; insurer's motion denied.

West Headnotes (8)

[1] Insurance
Application of rules of contract construction

Under New York law, insurance policies are interpreted according to general rules of contract interpretation.

Cases that cite this headnote

[2] Contracts
Intention of Parties

Under New York law, the fundamental, neutral precept of contract interpretation is that agreements are construed in accord with the parties' intent.

Cases that cite this headnote

[3] Contracts
Language of Instrument

Under New York law, a written agreement that is complete, clear and unambiguous on its face must be enforced according to the plain meaning of its terms.

Cases that cite this headnote

[4] Contracts
Ambiguity in general

Under New York law, when a contract is unambiguous, its interpretation is a question of law.

Cases that cite this headnote

[5] Insurance
Reasonable expectations

Insurance
Plain, ordinary or popular sense of language

In determining whether an insurance contract is ambiguous, a court applying New York law should focus on the reasonable expectations of the average insured upon reading the policy and employing common speech.

Cases that cite this headnote

[6] Insurance
Theft or Burglary

Under New York law, insured corporation's losses stemming from e-mail "spoofing" scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation's president, were covered under computer fraud clause in crime protection policy; scheme amounted to deceitful and

dishonest access of insured's computer system, as the fraud was achieved by entry into insured's e-mail system with spoofed e-mails that used computer code to mask the thief's true identity, and while insured's employees took other steps before approving the wire transfer, the transfer was still the direct result of the spoofed e-mails.

1 Cases that cite this headnote

[7] **Insurance**
Theft or Burglary

Under New York law, insured corporation's losses stemming from e-mail "spoofing" scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation's president, were covered under funds transfer fraud clause in crime protection policy; given that the wire transfer depended on obtaining the consent of several high level employees by trick, the fact that insured's accounts payable employee willingly sent the transfer did not transform it into a valid transaction.

Cases that cite this headnote

[8] **Insurance**
Theft or Burglary

Under New York law, insured corporation's losses stemming from e-mail "spoofing" scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation's president, were not covered under forgery clause in crime protection policy; even if the spoofed e-mails constituted a forgery, the policy only covered forgeries or alterations of a financial instrument.

Cases that cite this headnote

Attorneys and Law Firms

***472** Adam Seth Ziffer, Robin L. Cohen, Alexander Michael Sugzda, McKool Smith, New York, NY, for Plaintiff

Christopher M. Kahler, Sara Gronkiewicz–Doran, Scott Schmookler, Gordon & Rees LLP, Chicago, IL, Jeffrey Yehuda Aria Spiegel, Joseph Salvo, Gordon & Rees, LLP, New York, NY, for Defendant

MEMORANDUM AND ORDER GRANTING SUMMARY JUDGMENT

ANDREW L. CARTER, JR., District Judge:

Medidata Solutions, Inc. ("Medidata") commenced this action against Federal Insurance Company ("Federal") after Federal denied Medidata's claim for insurance coverage. The parties filed cross-motions for summary judgment and the Court ordered additional expert discovery. For the following reasons, Medidata's motion for summary judgment is GRANTED.

BACKGROUND

A. Medidata

Medidata provides cloud-based services to scientists conducting research in clinical trials. Medidata's Memorandum of Law in Support of Motion for Summary Judgment ("Pl's Mem.") at 3, ECF No. 37. Medidata used Google's Gmail platform for company emails. Affidavit of Glenn Watt in Support of Medidata's Motion for Summary Judgment, ("Watt Aff.") ¶ 2, ECF No. 39. Medidata email addresses consisted of an employee's first initial and last name followed by the domain name "mdsol.com" instead of "gmail.com". *Id.* ¶ 3. Email messages sent to Medidata employees were routed through Google computer servers. *Id.* ¶ 4. Google systems processed and stored the email messages. *Id.* ¶ 4. During processing, Google compared an incoming email address with Medidata employee profiles in order to find a match. *Id.* ¶ 9. If a match was found, Gmail displayed the sender's full name, email address, and picture in the "From" field of the message. *Id.* ¶¶ 8, 10, 11. After processing, the emails were displayed in the Medidata employee's email account. *Id.* ¶ 7. Medidata employees used computers owned by the company to ***473** access the email messages that were process and displayed by Google. *Id.*

B. Fraud on Medidata

In the summer of 2014, Medidata notified its finance department of the company's short-term business plans

which included a possible acquisition. Plaintiff's Rule 56.1 Statement ("Pl.'s 56.1") ¶ 36, ECF No. 36. Medidata instructed finance personnel "to be prepared to assist with significant transactions on an urgent basis." *Id.* ¶ 37. In 2014, Alicia Evans ("Evans") worked in accounts payable at Medidata. *Id.* ¶ 38. Evans was responsible for processing all of Medidata's travel and entertainment expenses. Joint Exhibit Stipulation ("Joint Ex. Stip.") Ex. 20, 41:16–21, ECF No. 41. On September 16, 2014, Evans received an email purportedly sent from Medidata's president. *Id.* Ex. 2. The email message contained the president's name, email address, and picture in the "From" field. *Id.* The message to Evans stated that Medidata was close to finalizing an acquisition, and that an attorney named Michael Meyer ("Meyer") would contact Evans. *Id.* The email advised Evans that the acquisition was strictly confidential and instructed Evans to devote her full attention to Meyer's demands. *Id.* Evans replied: "I will certainly assist in any way I can and will make this a priority." *Id.* Ex. 4.

On that same day, Evans received a phone call from a man who held himself out to be Meyer. *Id.* Ex. 20, 31:10–15. Meyer demanded that Evans process a wire transfer for him. *Id.* Meyer told Evans a physical check would not suffice because of time constraints. *Id.* Ex. 20, 36:5–8. Evans explained to Meyer that she needed an email from Medidata's president requesting the wire transfer. *Id.* Ex. 20, 34:17–20. Evans also explained she needed approval from Medidata Vice President Ho Chin ("Chin"), and Director of Revenue Josh Schwartz ("Schwartz"). *Id.*

Chin, Evans, and Schwartz then received a group email purportedly sent from Medidata's president stating: "I'm currently undergoing a financial operation in which I need you to process and approve a payment on my behalf. I already spoke with Alicia, she will file the wire and I would need you two to sign off." *Id.* Ex. 6. The email contained the president of Medidata's email address in the "From" field and a picture next to his name. *Id.* In response, Evans logged on to Chase Bank's online system to initiate a wire transfer. *Id.* Ex. 20, 13:20–14:16. Evans entered the banking information provided by Meyer and submitted the wire transfer for approval. *Id.* Ex. 20, 15:11–23, 16:17–17:05. Schwartz and Chin logged on to Chase's online banking system and approved the wire transfer. *Id.* Ex. 21, 13:20–14:16; Ex. 19, 59:16–18, 60:02–04. $4,770,226.00 was wired to a bank account that was provided by Meyer. *Id.* Ex. 8.

On September 18, 2014, Meyer contacted Evans requesting a second wire transfer. *Id.* Ex. 20, 42:02–10. Evans initiated the second wire transfer and Schwartz approved it. *Id.* Ex. 21, 40:24–41:20. However, Chin thought the email address in the "Reply To" field seemed suspicious. *Id.* Ex. 19, 46:08–24. Chin spoke with Evans about his suspicions and Evans composed a new email to Medidata's president inquiring about the wire transfers. *Id.* Ex. 20, 50:04–20. Medidata's president told Evans and Chin that he had not requested the wire transfers. *Id.* Medidata employees then realized that the company had been defrauded. *Id.* Ex. 19, 63:09–64:18. Medidata contacted the FBI and hired outside counsel to conduct an investigation. *Id.* The investigations revealed that an unknown actor altered the emails that were sent to Chin, Evans, and Schwartz to appear ***474** as if they were sent from Medidata's president. *Id.*

C. Medidata Insurance Policy

Medidata held a $5,000,000 insurance policy with Federal called "Federal Executive Protection". *Id.* Ex. 1. The Policy contained a "Crime Coverage Section" addressing loss caused by various criminal acts, including Forgery Coverage Insuring, Computer Fraud Coverage, and Funds Transfer Fraud Coverage. *Id.*

1. Computer Fraud Coverage

The Policy's, "Computer Fraud Coverage", protected the "direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party." *Id.* The Policy defined "Organization" as "any organization designated in Item 4 of the Declarations for this coverage section." *Id.* Item 4, in turn, lists "Medidat[a] Solutions, Inc., and its subsidiaries" as a covered Organization. *Id.* The Policy defined "Third Party" as "a natural person other than: (a) an Employee; or (b) a natural person acting in collusion with an Employee." *Id.*

The Policy defined "Computer Fraud" as: "[T]he unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." *Id.* A "Computer Violation" included both "the fraudulent: (a) entry of Data into ... a Computer System; [and] (b) change to Data elements or program

logic of a Computer System, which is kept in machine readable format ... directed against an Organization." *Id.* The Policy defined "Data" broadly to include any "representation of information." *Id.* The Policy defined "Computer System" as "a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are: (a) owned and operated by an Organization; (b) leased and operated by an Organization; or (c) utilized by an Organization." *Id.*

2. Funds Transfer Fraud Coverage

The Policy's Funds Transfer Fraud Coverage protected "direct loss of Money or Securities sustained by an Organization resulting from Funds Transfer Fraud committed by a Third Party." *Id.* The Policy defined "Funds Transfer Fraud" as: "fraudulent electronic ... instructions ... 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." *Id.*

3. Forgery Coverage

The Policy's Forgery Coverage protected "direct loss sustained by an Organization resulting from Forgery or alteration of a Financial Instrument committed by a Third Party". *Id.* "Forgery" is defined as "the signing of the name of another natural person ... with the intent to deceive ... Mechanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures." *Id.*

4. Claim For Coverage

On September 25, 2014, Medidata submitted a claim to Federal requesting coverage of the fraud under three clauses. *Id.* Ex. 11. Federal assigned regional claims technician Michael Maillet ("Maillet") to investigate the fraud on Medidata. *Id.* Ex. 12.

On December 24, 2014, Federal denied Medidata's claim for coverage. *Id.* Federal denied coverage under the computer fraud clause, because there had been no "fraudulent entry of Data into Medidata's computer system." *Id.* at 4. As support, Federal ***475** explained that [t]he subject emails containing false information were sent to an inbox which was open to receive emails from any member of the public" thus the entry of the fictitious emails "was authorized." *Id.* In addition, Federal concluded that there had been no "change to data elements" because the emails did not cause any fraudulent change to data elements or program logic of Medidata's computer system. *Id.* Federal conceded that Gmail added the name and picture of Medidata's president because of the email, however, Federal stated that the fake email did not cause this to happen. *Id.* According to Federal, Medidata's computer system, "populated the email in the normal manner." *Id.* at 5.

Federal denied coverage under the funds transfer fraud clause because the wire transfer had been authorized by Medidata employees and thus was made with the knowledge and consent of Medidata. *Id.*

Finally, Federal rejected Medidata's claim for Forgery Coverage because the emails did not contain an actual signature and did not meet the Policy's definition of a Financial Instrument. *Id.* Federal also based its denial of both the Forgery Coverage and the Computer Fraud Coverage claims on the belief that the emails did not directly cause Medidata's loss, because no loss would have taken place if Medidata employees had not acted on the instructions contained in those emails. *Id.*

On January 13, 2015, Medidata sent a letter responding to the denial and setting forth the basis for coverage under the Policy. *Id.* Ex. 14. Federal replied on January 30, 2015, reasserting its denial of coverage for the claim. *Id.* Ex. 15.

DISCUSSION

Summary judgment is appropriate where "the pleadings, depositions, answers to interrogatories and admissions on file, together with affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986); *see also* Fed. R. Civ. P.

56(c). "There is no issue of material fact where the facts are irrelevant to the disposition of the matter." *Chartis Seguros Mexico, S.A. de C.V. v. HLI Rail & Rigging, LLC,* 967 F.Supp.2d 756, 761 (S.D.N.Y. 2013). "Speculation, conclusory allegations and mere denials are not enough to raise genuine issues of fact." *Id.* (citing *National Union Fire Ins. Co. of Pittsburgh, Pa. v. Walton Ins. Ltd.*, 696 F.Supp. 897, 900 (S.D.N.Y. 1988)).

The burden lies with the moving party to demonstrate the absence of any genuine issue of material fact and all inferences and ambiguities are to be resolved in favor of the nonmoving party. *See Celotex Corp.*, 477 U.S. at 323, 106 S.Ct. 2548 (1986); *see also Hotel Emps. & Rest. Emps. Union, Local 100 v. City of New York Dep't of Parks & Recreation,* 311 F.3d 534, 543 (2d Cir. 2002). If "no rational jury could find in favor, of the nonmoving party because the evidence to support its case is so slight, there is no genuine issue of material fact and a grant of summary judgment is proper." *Gallo v. Prudential Residential Servs., Ltd. P'ship*, 22 F.3d 1219, 1224 (2d Cir. 1994). An identical standard applies where the parties file cross-motions for summary judgment: "each party's motion must be examined on its own merits, and in each case all reasonable inferences must be drawn against the party whose motion is under consideration." *Morales v. Quintel Entm't, Inc.*, 249 F.3d 115, 121 (2d Cir. 2001) (citation omitted).

[1] **[2]** **[3]** **[4]** **[5]** Under New York law, insurance policies are interpreted according to general rules of contract interpretation. ***476** *Olin Corp. v. Am. Home Assur. Co.*, 704 F.3d 89, 98 (2d Cir. 2012). "The fundamental, neutral precept of contract interpretation is that agreements are construed in accord with the parties' intent. ... [A] written agreement that is complete, clear and unambiguous on its face must be enforced according to the plain meaning of its terms." *Bank of New York v. First Millennium, Inc.*, 598 F.Supp.2d 550, 556 (S.D.N.Y. 2009) *aff'd*, 607 F.3d 905 (2d Cir. 2010) (citing *Greenfield v. Philles Records, Inc.*, 98 N.Y.2d 562, 569, 750 N.Y.S.2d 565, 780 N.E.2d 166 (2002)). When a contract is unambiguous, its interpretation is a question of law. *See 82–11 Queens Blvd. Realty, Corp. v. Sunoco, Inc. (R & M),* 951 F.Supp.2d 376, 381 (E.D.N.Y. 2013). In determining whether an insurance contract is ambiguous, a Court should focus "on the reasonable expectations of the average insured upon reading the policy and employing common speech." *Universal Am. Corp. v. Nat'l Union Fire Ins. Co.,* 25 N.Y.3d 675, 680, 16 N.Y.S.3d 21, 37 N.E.3d 78 (2015).

A. Computer Fraud Coverage

[6] Medidata argues that the Policy's Computer Fraud clause covers the company's loss in 2014, because a thief fraudulently entered and changed data in Medidata's computer system. Pl.'s Mem. at 14–20. Specifically, Medidata asserts that the address in the "From" field of the spoofed emails constituted data which was entered by the thief posing as Medidata's president. *Id.* at 14. Also, a thief entered a computer code which caused Gmail to "change" the hacker's email address to the Medidata president's email address. *Id.* at 19–20.

Federal argues that Medidata's loss in 2014 is not covered by the Computer Fraud clause, because the emails did not require access to Medidata's computer system, a manipulation of those computers, or input of fraudulent information. Federal's Memorandum of Law in Support of Summary Judgment ("Def's Mem.") at 9–12, ECF No. 34. The Court has reviewed the Policy and concludes that, as a matter of law, the unambiguous language of the Computer Fraud clause provides coverage for the theft from Medidata.

Under Medidata's policy, a computer violation occurs upon the "the fraudulent: (a) entry of Data into or deletion of Data from a Computer System" or "(b) change to Data elements or program logic of a Computer System, which is kept in machine readable format." The New York Court of Appeals shed light on these phrases in *Universal,* which involved a health insurance company that was defrauded by healthcare providers who entered claims for reimbursement of services that were never rendered. 25 N.Y.3d at 681–82, 16 N.Y.S.3d 21, 37 N.E.3d 78. [1] Universal sought insurance coverage for the losses incurred by the fraudulent claims. *Id.* at 679, 16 N.Y.S.3d 21, 37 N.E.3d 78. Universal's computer fraud clause covered "loss resulting directly from a fraudulent entry of Electronic Data or Computer Program into, or change of Electronic Data or Computer Program within" the insured's computer system." ***477** *Id.* In denying coverage, the Court of Appeals held that the unambiguous language of Universal's policy "applie[d] to losses incurred from unauthorized access to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users."

Id. at 680–81, 16 N.Y.S.3d 21, 37 N.E.3d 78. The court reasoned that the drafter's "intentional placement of 'fraudulent' before 'entry' and 'change' manifest[ed] the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access." *Id.* at 681, 16 N.Y.S.3d 21, 37 N.E.3d 78.

Here, the fraud on Medidata falls within the kind of "deceitful and dishonest access" imagined by the New York Court of Appeals. *Id.* It is undisputed that the theft occurred by way of email spoofing. [2] Joint Factual Stipulation Following Discovery ("Joint Fact Stip.") ¶ 7, ECF 72. To that end, the thief constructed messages in Internet Message Format ("IMF") which the parties compare to a physical letter containing a return address. *Id.* ¶ 2. The IMF message was transmitted to Gmail in an electronic envelope called a Simple Mail Transfer Protocol ("SMTP"). *Id.* ¶ 1. Much like a physical envelope, the SMTP Envelope contained a recipient and a return address. *Id.* To mask the true origin of the spoofed emails, the thief embedded a computer code. *Id.* ¶ 10. The computer code caused the SMTP Envelope and the IMF Letter to display different email addresses in the "From" field. *Id.* The spoofed emails showed the thief's true email address in the SMTP "From" field, and Medidata's president's email address in the IMF "From" field. *Id.* ¶¶ 20–21. When Gmail received the spoof emails, the system compared the address in the IMF "From" field with a list of contacts and populated Medidata's president's name and picture. *Id.* ¶ 15. The recipients of the Gmail messages only saw the information in the IMF "From" field. *Id.* ¶ 11.

Federal's reading of *Universal* is overbroad. In this case, Federal focuses on the thief's construction of the spoofed emails and computer code before sending them to Gmail, arguing that, as a result, there was no entry or change of data to Medidata's computer system. Def's Mem. at 9–12. Under this logic, *Universal* would require that a thief hack into a company's computer system and execute a bank transfer on their own in order to trigger insurance coverage. However, this reading of *Universal* incorrectly limits the coverage of the policy in this case. It is true that the Court of Appeals in *Universal* peppered its opinion with references to hacking as the example for a covered violation. *See e.g., id.* at 681, 16 N.Y.S.3d 21, 37 N.E.3d 78 ("[T]he the rider covers losses from a dishonest entry or change of electronic data or computer program, constituting what the parties agree would be "hacking" of the computer system."). But a hacking is one of many methods a thief can use, and "is an everyday term for unauthorized access to a computer system." *Dial Corp. v. News Corp.*, No. 13-CV-6802, 2016 WL 690868, at *3 (S.D.N.Y. Feb. 17, 2016) (citation omitted). Thus, *Universal* is more appropriately read as finding coverage for fraud where the perpetrator violates the ***478** integrity of a computer system through unauthorized access and denying coverage for fraud caused by the submission of fraudulent data by authorized users. *Id.* (noting "[o]ther language in the rider confirms that the rider seeks to address unauthorized access"). Indeed, an examination of the trial court's analysis in *Universal* further emphasizes this point. The N.Y. Supreme Court held Universal's policy "indicates that coverage is for an unauthorized entry into the system, i.e. by an unauthorized user, such as a hacker, or for unauthorized data, e.g. *a computer virus.*" The trial court was also concerned with unauthorized users and corrupting data instead of authorized users submitting untruthful content. [3] *Id.* ("Nothing in this clause indicates that coverage was intended where an authorized user utilized the system as intended, i.e. to submit claims, but not where the claims themselves were fraudulent.").

Federal's reliance on *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, is also misplaced. The court in *Pestmaster*, held that a corporation's computer fraud insurance policy did not cover a theft by the company's payroll administrator, because the administrator was authorized to withdraw funds from the corporation's bank account, notwithstanding the fact that he later misappropriated the payroll funds. No. 13-CV-5039 (JFW), 2014 WL 3844627, at *6 (C.D. Cal. July 17, 2014). Relying on *Universal,* the Court explained that "Computer Fraud occurs when someone hacks or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds." *Id.* (internal quotation marks omitted). In contrast, the fraud on Medidata was achieved by entry into Medidata's email system with spoofed emails armed with a computer code that masked the thief's true identity. The thief's computer code also changed data from the true email address to Medidata's president's address to achieve the email spoof.

In challenging causation, Federal contends that "there is no direct nexus" between the spoofed emails and the

fraudulent wire transfer. Defs Mem. at 13–15. According to Federal, the spoofed emails "did not create, authorize, or release a wire transfer" because Medidata employees received telephone calls from the thief and took other steps in approving the fraudulent transfer. *Id.* at 16. As support, Federal cites to the Fifth Circuit's decision in *Apache Corp. v. Great American Ins. Co.* denying coverage of a similarly worded computer fraud provision. 662 Fed.Appx. 252 (5th Cir. 2016). The underlying fraud in *Apache* was achieved through a muddy chain of events. The insured was duped into sending payments to thieves that were intended for the insured's vendor. *Id.* at 253. The thieves engaged in a concerted effort to achieve the fraud which included phone calls, spoofed emails, and falsified documents. *Id.* Applying Texas law, the Fifth Circuit held that the insured's computer fraud provision did not cover the theft because "the fraudulent transfer was the result of other events and not directly by the computer use." *Id.* The Court explained that the insured "invited the computer-use at issue ... 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, ***479** very large invoice payments, but to a fraudulent bank account." *Id.* at 258–59. In contrast, Medidata employees did not invite the spoofed emails at issue. The chain of events began with an accounts payable employee receiving a spoofed email from a person posing as Medidata's president. To the extent that the facts of this case fit within *Apache,* the Court finds its causation analysis unpersuasive. The Court finds that Medidata employees only initiated the transfer as a direct cause of the thief sending spoof emails posing as Medidata's president.

Federal also cites to the Ninth Circuit's decision in *Taylor & Lieberman v. Federal Ins. Co.*, denying coverage of a computer fraud provision. ("*Taylor I* "), 681 Fed.Appx. 627, 628 (9th Cir. 2017). In *Taylor*, an accounting firm fell victim to an email spoofing scam after a thief invaded the email account of the accounting firm's client. *Id.* at 628. The thief, disguised as the client, sent emails requesting wire transfers to a specified bank account. *Id.* The district court keenly pointed out the "series of far more remote circumstances" than simply a theft directly from the accounting firm. *Taylor & Lieberman v. Fed. Ins. Co.*, No. 14-CV-3608 (RSWL) (SHX), 2015 WL 3824130, at *4 (C.D. Cal. June 18, 2015) ("*Taylor II* "). The district court emphasized that the thief stole money from the client not the accounting firm, and that the accounting firm was seeking reimbursement for the loss of its client's money. *Id.* at *4. Importantly, the court added, "if the funds had been held in an account owned or attributed to Plaintiff, such as an escrow account and a hacker had entered into Plaintiff's computer system ... then Plaintiff would be correct in asserting coverage from the Policy." *Id.* The Ninth Circuit agreed, noting that the mere sending of emails from the client to the accounting firm did not constitute unauthorized entry into the accounting firm's computer system. *Taylor I*, 681 Fed.Appx. at 629–30. But Medidata did not suffer a loss from spoofed emails sent from one of its clients. A thief sent spoofed emails armed with a computer code into the email system that Medidata used. Also, the fraud caused transfers out of Medidata's own bank account. Therefore, Medidata was "correct in asserting coverage from the Policy." *Taylor II*, 2015 WL 3824130, at *4.

Accordingly, Medidata has demonstrated that its losses were a direct cause of a computer violation.

B. Funds Transfer Fraud Coverage

[7] Medidata argues that it was improperly denied coverage under the Funds Transfer Fraud clause because the theft in 2014 "(1) caused a direct loss of money; (2) by fraudulent electronic instructions purportedly issued by Medidata; (3) issued to a financial institution; (4) to deliver money from Medidata's accounts; (5) without Medidata's knowledge or consent." Pl's Mem. at 20. Federal challenges the last of the requisite elements, arguing that the bank wire transfer in 2014 was voluntary and with Medidata's knowledge and consent. Def's Mem. at 21–24. Federal also argues that, because Medidata employees voluntarily transferred the money, it was actually issued by Medidata instead of "purportedly issued" as the Policy demands. *Id.* at 24–25. The Court finds that the unambiguous language of the Policy covers the theft from Medidata in 2014.

The Policy defines Funds Transfer Fraud as: "fraudulent electronic ... instructions ... 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." ***480** Joint Ex. Stip., Ex. 1. Under *Pestmaster*, which Federal relies, a funds transfer fraud agreement, "does not cover authorized or valid electronic transactions ...even though they are, or maybe, associated with a fraudulent scheme."

2014 WL 3844627, at *5. However, *Pestmaster* involved a corporation that made several valid electronic transfers to its payroll administrator who later misappropriated the funds. *Id.* at *6. The court justified the denial of coverage by pointing out, "there is no evidence that... any third party, gained unauthorized entry into Pestmaster's bank's electronic fund transfer system **or pretended to be an authorized representative** or otherwise altered the electronic instructions in order to wrongfully divert money from the rightful recipient." *Id.* (emphasis added). Also unpersuasive is Federal's reliance on *Cumberland Packing Corp. v. Chubb Ins. Corp.*, which interpreted a funds transfer fraud agreement. 29 Misc.3d 1208(A), 2010 WL 3991185, at *5 (Sup. Ct. 2010). The court in *Cumberland* denied coverage to a policyholder who had voluntarily transferred funds to Bernie Madoff for investment purposes. *Id.* The court reasoned that "Madoff was expressly authorized to act as plaintiffs' broker/agent" which did not involve unauthorized instructions to transfer money. *Id.* In this case, it is undisputed that a third party masked themselves as an authorized representative, and directed Medidata's accounts payable employee to initiate the electronic bank transfer. It is also undisputed that the accounts payable personnel would not have initiated the wire transfer, but for, the third parties' manipulation of the emails. 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.

C. Forgery Coverage

[8] The theft from Medidata in 2014 does not trigger coverage under the Forgery clause, because the Policy requires a "direct loss resulting from Forgery or alteration of a Financial Instrument committed by a Third Party." Joint Ex. Stip., Ex. 1. The parties vehemently dispute whether the spoofed emails containing Medidata's president's name constitute a forgery. *See* Pl's Mem. at 18; Def's Mem. at 17. However, the Court need not resolve the matter. Even if the emails contained a forgery, the absence of a financial instrument proves fatal to Medidata's claim for coverage. In a strained reading of the Policy, Medidata argues that a forgery itself triggers coverage even in the absence of a financial instrument. Medidata's Memorandum of law in Further Support of Summary Judgment ("Pl's Reply") at 20, ECF No. 52. However, "[t]he entire contract must be reviewed and particular words should be considered, not as if isolated from the context, but in the light of the obligation as a whole and the intention of the parties as manifested thereby. Form should not prevail over substance and a sensible meaning of words should be sought." *Riverside S. Planning Corp. v. CRP/Extell Riverside, L.P.*, 13 N.Y.3d 398, 404, 892 N.Y.S.2d 303, 920 N.E.2d 359 (2009) (citations, alterations, and internal quotation marks omitted). Medidata's interpretation of the Policy would render the word forgery vague and create ambiguity in the clause. To the contrary, a forgery or alteration are both means by which a person can corrupt a financial instrument resulting in a loss to ***481** the insured. If forgery is viewed in isolation, the Policy would certainly be converted to a general crime policy. Therefore, Medidata has not demonstrated that it suffered a loss that was covered by the Forgery clause.

CONCLUSION

For the foregoing reasons, Medidata's motion for summary judgment is **GRANTED** and Federal's motion for summary judgment is **DENIED.**

SO ORDERED.

All Citations

268 F.Supp.3d 471

Footnotes

1 The trial court noted "the perpetrators enrolled new members in the ... plan with the person's cooperation, in return for which the member received a kickback from the provider. In some cases, the provider used the member's personal information without that person's knowledge. In either event, the provider itself did not enroll in the plan. Instead, they were able to submit claims after obtaining a National Provider Identifier (NPI) from [the agency of the U.S. Department

of Health and Human Service tasked with overseeing this market]. In some cases, the NPI was obtained for a fictitious provider, in other cases it was fraudulently taken from a legitimate provider."

2 A court in this district defined "Spoofing" as "the practice of disguising a commercial e-mail to make the e-mail appear to come from an address from which it actually did not originate. Spoofing involves placing in the "From" or "Reply-to" lines, or in other portions of e-mail messages, an e-mail address other than the actual sender's address, without the consent or authorization of the user of the e-mail address whose address is spoofed." *Karvaly v. eBay, Inc.*, 245 F.R.D. 71, 91 n.34 (E.D.N.Y. 2007) (citation and internal quotation marks omitted).

3 The Appellate Division appeared to have a similar concern when it found that the language of the policy "was intended to apply to wrongful acts in manipulation of the computer system, i.e., by hackers, and did not provide coverage for fraudulent content consisting of claims by bona fide doctors and other health care providers authorized to use the system for reimbursement for health care services that were not provided."