IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI
ABERDEEN DIVISION

MISSISSIPPI SILICON HOLDINGS, LLC PLAINTIFF

V. CIVIL ACTION NO. 1:18-CV-231-SA-DAS

AXIS INSURANCE COMPANY DEFENDANT

ORDER AND MEMORANDUM OPINION

Mississippi Silicon Holdings, LLC ("MSH") initiated this civil action on November 7, 2018, by filing its Complaint [2] for declaratory judgment and breach of contract against AXIS Insurance Company in the Circuit Court of Tishomingo County, Mississippi. AXIS removed the action to this Court on the basis of diversity jurisdiction. *See* Notice of Removal [1]. Both parties filed Motions for Summary Judgment [93, 95], each of which has been fully briefed and is now ripe for review.

Factual and Procedural Background

MSH is a manufacturing company that makes silicon metal at its plant in Burnsville, Mississippi. As part of its manufacturing process, MSH utilizes graphitized carbon electrodes. Since it began production in 2015, MSH has purchased its electrodes from a Russian supplier, Energoprom.

Throughout October 2017, John Lalley, MSH's Vice President of Finance and Chief Financial Officer, engaged in various email communications with Olga Rozina, an Energoprom employee, regarding MSH's purchases and certain invoices which had come due. On October 23, 2017, Lalley received an email listing "Olga Rozina" in the "from" line. Attached to the email, which Lalley received at his typical work email address, was a document that contained information for a bank account at Bulgarian-American Credit Bank and requested that MSH wire its future payments to that account. The October 23 email advised that MSH should send its

payments to the new bank account, which was Energoprom's agent collector's account, "due to issues [Energoprom was] having with [its] account." After engaging in additional email correspondence, Lalley ultimately advised "Olga Rozina" that MSH would "make a partial payment of $250,000 this Friday or Monday . . . [and] [w]e will pay the balance on around November 17."

On October 27, 2017, Lalley electronically logged into MSH's transfer account with Trustmark Bank and initiated a wire transfer in the amount of $250,030.00 to the Bulgarian-American Credit Bank account identified on the attachment to the October 23 email. After Lalley initiated the transfer, Patricia McPheters, another MSH employee, logged into MSH's account on Trustmark Bank's website and confirmed the transfer. Following McPheters' authorization, a representative from Trustmark Bank made a phone call to Eddie Boardwine, MSH's Plant Manager. During the conversation, Boardwine verbally authorized the transfer. According to Lalley, MSH utilized this three-step verification process for all transfers in excess of $100,000.00. After the verification process was completed, $250,030.00 was transferred from MSH's account to the Bulgarian-American Credit Bank account listed on the attachment to the October 23 email.

At 2:42 a.m. on November 17, 2017, Lalley received an additional email from "Olga Rozina," through which she indicated that she was sending "shipping documents and invoice attached for Lot#7." She also requested that Lalley provide information regarding "the estimated date of payment for 2 invoices left due in October/November." In another email that Lalley also received at 2:42 a.m. on November 17, 2017, "Olga Rozina" advised that Lalley should ignore the banking information located on the invoice attached to the previous email, implying that Lalley should continue to send payments to the Bulgarian-American Credit Bank account. Later that day, Lalley initiated an additional transfer in the amount of $775,851.13 from MSH's

account at Trustmark Bank to the Bulgarian-American Credit Bank account listed on the attachment to the October 23 email. The same three-step verification process set forth above in relation to the October 27, 2017 transfer was completed in connection with this transaction, and the money was ultimately transferred. At 12:43 p.m. on November 17, 2017, Lalley responded to "Olga Rozina" confirming that the transfer had been initiated.

On December 11, 2017, Pereveznyuk Ludmila, an employee of Energoprom, called Lalley advising that Energoprom had not received any payment from MSH for its outstanding invoices and requesting an update as to when payment could be expected. After Lalley explained that MSH had made payments to the Bulgarian-American Credit Bank account in accordance with the instructions attached to the October 23 email he had received from "Olga Rozina," Ludmila denied that Olga Rozina or any Energoprom employee had sent such an email. By the end of his conversation with Ludmila, Lalley concluded that his emails with "Olga Rozina" since October 23 had not actually been with Olga Rozina and that MSH had been a victim of fraud.

At all relevant times, MSH had in place a Privatus Platinum Insurance Policy issued by AXIS.[1] Among other coverages, the Policy provided coverage for Social Engineering Fraud ($100,000.00 policy limit), Computer Transfer Fraud ($1,000,000.00 policy limit), and Funds Transfer Fraud ($1,000,000.00 policy limit).

The Social Engineering Fraud provision of the Policy provides 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

[1] Although not separately attached as an exhibit to either party's respective Motion for Summary Judgment, the Policy is attached to John Lalley's deposition transcript which was attached to AXIS' Motion for Summary Judgment. [Dkt. 93, Ex. B-51].

> be a **Transfer Instruction** but, in fact, was not issued by a **Client**, **Employee** or **Vendor**; or
>
> b. a **Financial Institution** as instructed by 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 Computer Transfer Fraud provision provides:

> The Insurer will pay for loss of or loss from damage to **Covered Property** resulting directly from **Computer Transfer Fraud** that causes the 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.

Finally, the Funds Transfer Fraud provision provides:

> The insurer will pay for loss of **Money** or **Securities** resulting directly from the transfer of **Money** or **Securities** from a **Transfer Account** to a person, place, or account beyond the **Insured Entity's** control, by a **Financial Institution** that relied upon a written, electronic, telegraphic, cable, or teletype instruction that purported to be a **Transfer Instruction** but, in fact, was issued without the **Insured Entity's** knowledge or consent.

[Dkt. 93, Ex. B-51] (emphasis in original).

On December 12, 2017, the day after Lalley's conversation with Ludmila, MSH placed AXIS on notice of the $1,025,881.13 loss (the sum of the two transfers) in order to preserve MSH's right to seek coverage under the Policy. MSH then hired SecurIT360 to perform a forensic review of the events that had occurred. After receiving SecurIT360's written report, MSH submitted to AXIS a sworn Proof of Loss, which was signed by Lalley and stated that "bad actors breached the Mississippi Silicon computer system allowing them to monitor and redirect e-mail conversations going to and from Mississippi Silicon."

MSH contends that the underlying events entitle it to coverage under the Computer Transfer Fraud provision and/or the Funds Transfer Fraud provision of the Policy, each of which carry a $1,000,000.00 policy limit. AXIS, however, ultimately determined that the underlying events did not satisfy the requirements of either the Computer Transfer Fraud provision or the Funds Transfer Fraud provision. Rather, AXIS concluded that MSH was entitled to coverage only under the Social Engineering Fraud provision and accordingly mailed MSH a check for the $100,000.00 policy limit of that provision.

Aggrieved by AXIS' decision, MSH returned the $100,000.00 check and ultimately filed its Complaint [2] against AXIS on November 7, 2018, in the Circuit Court of Tishomingo County, Mississippi. In its Complaint, MSH seeks a declaratory judgment that it is entitled to coverage under the Computer Transfer Fraud provision and/or the Funds Transfer Fraud provision of the Policy, as well as damages for breach of contract. AXIS timely removed the action to this Court on the basis of diversity jurisdiction. *See* Notice of Removal [1]. The parties have now filed Cross Motions for Summary Judgment [93, 95], each requesting that the Court interpret the subject provisions in its favor.

Summary Judgment Standard

A party is entitled to summary judgment under Rule 56(a) of the Federal Rules of Civil Procedure when the "movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Summary judgment is appropriate "after adequate time for discovery and upon motion, against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S. Ct. 2548 (1986). In evaluating whether summary judgment is appropriate, the Court must review

all well-pleaded facts in the light most favorable to the nonmoving party. *Pratt v. City of Houston*, 247 F.3d 601, 606 (5th Cir. 2001).

The party moving for summary judgment "bears the initial responsibility of informing the district court of the basis for its motion, and identifying those portions of [the record] which it believes demonstrate the absence of a genuine issue of material fact." *Celotex*, 477 U.S. at 323, 106 S. Ct. 2548. The nonmoving party must then "go beyond the pleadings" and "designate 'specific facts showing that there is a genuine issue for trial.'" *Id*. at 324, 106 S. Ct. 2548. In reviewing the evidence, factual controversies are to be resolved in favor of the nonmovant, "but only when . . . both parties have submitted evidence of contradictory facts." *Little v. Liquid Air Corp.*, 37 F.3d 1069, 1075 (5th Cir. 1994) (en banc). The nonmoving party, however, cannot rely on conclusory allegations, speculation, unsubstantiated assertions, and legalistic arguments for showing a genuine issue for trial. *Id*.

Analysis and Discussion

As illustrated by its payment of the $100,000.00 policy limit to MSH, AXIS concedes that the underlying facts give rise to coverage under the Social Engineering Fraud provision. MSH does not dispute that the Social Engineering Fraud provision is applicable but instead avers that it is also entitled to coverage under the Computer Transfer Fraud provision and/or the Funds Transfer Fraud provision. The crux of the parties' dispute therefore concerns only whether MSH is entitled to coverage under the Computer Transfer Fraud provision and/or the Funds Transfer Fraud provision, which would entitle MSH to the $1,000,000.00 policy limit which each of those provisions carries. Accordingly, to resolve this matter, the Court need only decide the applicability of those two provisions.[2]

[2] Relying on the "Limits of Insurance" section of the Policy, MSH contends that the simple fact that the Social Engineering Fraud section is applicable does not necessarily result in another section of the Policy

As a general matter regarding the interpretation of an insurance policy, "[a] policy must be considered as a whole, with all relevant clauses together." *Architex Ass'n, Inc. v. Scottsdale Ins. Co.*, 27 So.3d 1148, 1157 (Miss. 2010).[3] On numerous occasions, the Mississippi Supreme Court has instructed that "if a contract is clear and unambiguous, then it must be interpreted as written." *Id.* (quoting *U.S. Fid. & Guar. Co. v. Martin*, 998 So.2d 956, 963 (Miss. 2008)); *see also Phillips v. Enterprise Transp. Serv. Co.*, 988 So.2d 418, 421 (Miss. Ct. App. 2008) (citations omitted) ("If a contractual term is unambiguous and not subject to interpretation, then it will be enforced as written, without attempting to surmise some possible but unexpressed intent of the parties."). If no ambiguity exists, a reviewing court should not look beyond the document's four corners. *Lee v. South Miss. Elec. Power Ass'n*, 17 So.3d 597, 600 (Miss. Ct. App. 2009) ("If we find ambiguity that cannot be resolved by the four corners of the documents, we next resort to the discretionary application of the canons of construction[.]").

Importantly, "just because the parties disagree over how to interpret policy language does not mean the language is ambiguous." *Noble v. Wellington Associates, Inc.*, 145 So.3d 714, 719 (Miss. Ct. App. 2013) (citing *Architex*, 27 So.3d at 1157). Rather, "[a]n ambiguity is defined as a susceptibility to two reasonable interpretations." *Dalton v. Cellular South, Inc.*, 20 So.3d 1227, 1232 (Miss. 2009). An ambiguity only exists when "a policy can be logically interpreted in two or

containing a higher policy limit, such as the Computer Transfer Fraud and/or Funds Transfer Fraud provisions, automatically becoming inapplicable. In making this argument, MSH specifically relies upon the provision of the Policy providing 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." [Dkt. 93, Ex. B-51]. Consistent with the plain language of this section of the Policy, the Court finds that MSH is entitled to coverage under the provision which provides the highest limit. In other words, 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.

[3] Because this is a diversity jurisdiction action, Mississippi state substantive law should be applied. *McBeth v. Carpenter*, 565 F.3d 171, 176 (5th Cir. 2009) ("A federal court sitting in diversity applies state substantive law.").

more ways, where one logical interpretation provides for coverage." *Architex*, 27 So.3d at 1157 (quoting *Martin*, 998 So.2d at 963). If an ambiguity does in fact exist in an insurance policy, it must be "read to favor the insured[.]" *Hankins v. Maryland Cas. Company/Zurich American Ins. Co.*, 101 So.3d 645, 658 (Miss. 2012). Nevertheless, "a court must refrain from altering or changing a policy where terms are unambiguous, despite resulting hardship on the insured." *Architex*, 27 So.3d at 1157 (quoting *Martin*, 998 So.2d at 963).

I. Policy Language

Each party contends that both the Computer Transfer Fraud provision and the Funds Transfer Fraud provision unambiguously support their respective positions.[4] However, the Policy is not rendered ambiguous simply because the parties disagree as to the proper interpretation. *See Noble*, 145 So.3d at 719. Instead, in accordance with the above-referenced precedent, the Court will engage in its own interpretation of the Computer Transfer Fraud provision and the Funds Transfer Fraud provision and make an independent determination as to whether the provisions are ambiguous.

A. Computer Transfer Fraud provision

As set forth above, the Computer Transfer Fraud provision provides:

> The Insurer will pay for loss of or loss from damage to **Covered Property** resulting directly from **Computer Transfer Fraud** that causes the 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.

[4] MSH also alternatively contends that it must prevail if it can establish that an ambiguity exists because, under Mississippi law, ambiguities in an insurance policy must be interpreted in favor of the insured. *See Hankins*, 101 So.3d at 658.

The Policy specifically defines "Computer Transfer Fraud" as used in the above-quoted provision as "the fraudulent entry of Information into or the fraudulent alteration of any Information within a Computer System."

The parties' disagreement as to the interpretation of the Computer Transfer Fraud provision largely concerns two portions of the provision itself: (1) the applicable causation standard, more specifically, whether a "hacking" must directly cause the loss in order to trigger coverage; and (2) the "without the Insured Entity's knowledge or consent" portion of the provision.[5]

As to the causation standard, AXIS contends that coverage does not exist because "nothing 'entered' into or 'altered' within [MSH's] Computer System (here the [MSH] email system) directly caused the transfer of any Money. Only John Lalley . . . acting in concert with two additional (required) colleagues, caused the transfer of the Money[.]" [Dkt. 101, p. 22]. Thus, AXIS takes the position that because the fraudulent email did not itself manipulate MSH's computer system, but instead simply requested that MSH take affirmative action, a "Computer Transfer Fraud" did not *directly* cause the transfers. In essence, AXIS contends that the affirmative conduct of Lalley, McPheters, and Boardwine, broke the causal connection between the fraudulent email and the loss, rendering the Computer Transfer Fraud provision inapplicable.

On the other hand, MSH contends that the fraudulent email, which ultimately caused Lalley to act, is sufficient to trigger coverage. MSH contends that it may recover because the covered peril "was the dominant and efficient cause of [MSH's] loss." [Dkt. 96, p. 29]. Thus, MSH urges the Court to apply a "proximate cause" standard.

[5] The parties also dispute other portions of the provision, such as whether a "hack" must have occurred in order to trigger coverage, and have engaged experts to opine as to whether the underlying facts satisfy the definition of "Computer Transfer Fraud" contained in the Policy. However, for the reasons set forth below, the Court need not decide these additional disagreements in order to adequately resolve the parties' dispute.

The Court finds telling the inclusion of the word "directly" in the provision. Black's Law Dictionary defines "directly" as "1. In a straightforward manner. 2. In a straight line or course. 3. Immediately." Black's Law Dictionary (11th ed. 2019); *see Noxubee County Sch. Dist. v. United Nat. Ins. Co.*, 883 So.2d 1159, 1165 (Miss. 2004) ("[W]hen the words of an insurance policy are plain and unambiguous, the court will afford them their plain, ordinary meaning and will apply them as written."). The Court finds it undeniable that the October 23 email set in motion a series of events which ultimately led to the loss. It is also clear that the emails from "Olga Rozina" did not themselves manipulate MSH's system and automatically transfer the funds. Rather, the emails requested that MSH engage in affirmative conduct, particularly, initiating a transfer to the Bulgarian-American Credit Bank account listed on the attachment. The Court finds this distinction critical, in light of the specific language of the provision.

While the Court recognizes and appreciates MSH's argument in favor of a "proximate cause" standard, it cannot be ignored that the provision itself specifically requires that the fraudulent act *directly* cause the loss. And it further cannot be ignored that MSH's employees, not the fraudulent emails themselves, actually initiated the transfer. If a proximate cause standard or some other more expansive coverage was intended, that language undoubtedly could have been included in the Policy. However, it was not.

The Court also notes that the causation standard *might* be rendered ambiguous in the absence of the explicit use of the term "directly" in the provision. If so, it would, as noted above, entitle MSH, as the insured, to an interpretation in its favor. *See Hankins*, 101 So.3d at 658. However, the provision clearly and unambiguously requires that the loss result *directly* from "Computer Transfer Fraud that causes the transfer. . ." And, as noted above, this plain language

simply is not satisfied, as the MSH employees, not the fraudulent emails, actually initiated and authorized the transfers.

Although the Court finds that the loss did not result directly from "Computer Transfer Fraud," the Court will also consider the parties' dispute regarding the provision's "without the Insured Entity's knowledge or consent" language. Arguing that the provision is not satisfied, AXIS emphasizes that three separate MSH employees had knowledge of, and explicitly authorized, the transfers, thereby precluding coverage. According to AXIS, the inclusion of the "without the Insured Entity's knowledge or consent" language, clearly establishes that there is no coverage "where an insured knowingly wires money to another (later determined to be [a] fraudster). Rather, in order for a loss to be covered under this insuring agreement, the fraudster must cause the transfer of currency, through a hack, and without the insured being aware." [Dkt. 94, p. 27].

To the contrary, MSH contends that "[a] plain reading of [the Computer Transfer Fraud provision] dictates that coverage is available for losses arising out of 'Computer Transfer Fraud' (defined as the fraudulent entry of electronic information into the insured's computer system, or the fraudulent alteration of any information within a computer system) that causes the insured to unwittingly or non-consensually misdirect property or funds." [Dkt. 96, p. 23]. To this end, MSH avers that coverage is not precluded "merely because the insured was aware of the transfer." *Id*. MSH instead argues it is more logical that the "knowledge or consent" requirement be read to require the insured to have "'actual' knowledge of material facts like the transferee's true identity or . . . consent to the transfer in light of the true facts and circumstances." *Id*. at p. 26-27.

In the Court's view, the inclusion of the "knowledge or consent" requirement is telling as to the coverage that was intended. Had the provision been intended to cover losses which were specifically authorized by MSH's employees acting in reliance upon false or fraudulent

information, the "without the Insured Entity's knowledge or consent" language could have been omitted altogether. The inescapable fact, however, is that the "without the Insured Entity's knowledge or consent" language is included in the provision, and coverage therefore clearly and unambiguously only applies for losses that occur without MSH's knowledge or consent.

If the Court read the provision to provide coverage in this context, when MSH's own employees were aware of, and explicitly authorized, the transfers, the Court would effectively substitute its own judgment in place of the plain language of the provision. Interpreting a contract in such a manner is prohibited under Mississippi law. *See Storey v. Williamson,* 101 So.3d 662, 668 (Miss. Ct. App. 2012) (quoting *Miss. Farm Bureau Cas. Ins. Co. v. Britt*, 826 So.2d 1261, 1266 (Miss. 2002)) ("This Court is 'bound to enforce contract language *as written* and give it its plain and ordinary meaning if it is clear and unambiguous.'") (emphasis added).

MSH also contends that the "knowledge or consent" requirement should be read to require "actual knowledge of material facts like the transferee's true identity or . . . consent to the transfer in light of the true facts and circumstances." [Dkt. 96, p. 26-27]. Other than MSH's desire that such language be included, MSH provides no legitimate reason for this heightened requirement to be read into an otherwise unambiguous provision. MSH has made no reference to this heightened "knowledge or consent" requirement elsewhere in the Policy, and the Court simply lacks authority to re-write the subject provision in such a manner. *See Storey*, 101 So.2d at 668.

Finally, although the availability of coverage under the Social Engineering Fraud provision of the Policy does not preclude coverage under another provision, such as the Computer Transfer Fraud provision, the language contained in the Social Engineering Fraud provision provides guidance. Had the Computer Transfer Fraud provision been intended to cover a loss occurring when a funds transfer was effectuated by an employee acting in good faith reliance upon an

electronic instruction which was ultimately determined to be fraudulent (exactly what occurred in this case), the same language used in the Social Engineering Fraud provision could have been incorporated into the Computer Transfer Fraud provision. As noted above, the Social Engineering Fraud provision specifically provides the following coverage:

> 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**; or
>
> b. a **Financial Institution** as instructed by 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 Social Engineering Fraud provision clearly authorizes coverage when an employee relies on information that is later determined to be false or fraudulent. In contrast, the Computer Transfer Fraud provision, rather than specifically extending coverage when an employee in good faith relies upon fraudulent information and inflicts a loss, specifically states that coverage is only available when the loss occurs "without the Insured Entity's knowledge or consent." The Court finds the inclusion of this language, as well as the failure to incorporate the same language as the Social Engineer Fraud provision, persuasive.

Ultimately, at least three MSH employees had knowledge of, and specifically authorized, the transfers. MSH cannot escape that reality, and its attempts to invoke coverage despite its employees' undisputed knowledge and explicit authorization of the transfers bends the language

of the Computer Transfer Fraud provision beyond the breaking point. The Computer Transfer Fraud provision is inapplicable.

B. Funds Transfer Fraud provision

The Funds Transfer Fraud provision states as follows:

> The insurer will pay for loss of **Money** or **Securities** resulting directly from the transfer of **Money** or **Securities** from a **Transfer Account** to a person, place, or account beyond the **Insured Entity's** control, by a **Financial Institution** that relied upon a written, electronic, telegraphic, cable, or teletype instruction that purported to be a **Transfer Instruction** but, in fact, was issued without the **Insured Entity's** knowledge or consent.

Similar to its argument in connection with the Computer Transfer Fraud provision, AXIS emphasizes the "knowledge or consent" requirement of the Funds Transfer Fraud provision and asserts that coverage is therefore not available.

A review of the plain language of the provision reveals that, in order for coverage to exist, the following requirements must be satisfied: (1) a loss; (2) resulting directly from; (3) the transfer of money to a person, place, or account beyond the Insured Entity's control; (4) by a Financial Institution that relied upon a written, electronic, telegraphic, cable, or teletype instruction that purported to be a Transfer Instruction; (5) but which actually was issued without the Insured Entity's knowledge or consent. In the case at bar, a loss undeniably occurred when Trustmark Bank transferred funds to the Bulgarian-American Credit Bank account in accordance with the specific instructions and authorization provided by MSH's employees. However, the impediment to coverage is that the transfer instruction upon which Trustmark Bank relied in order to complete the transfer was not "actually . . . issued without the Insured Entity's knowledge or consent." In fact, there has been no contention whatsoever that Lalley, McPheters, or Boardwine did not actually issue the transfer instruction. Rather, the undisputed evidence establishes that all three

employees, acting independently of each other, authorized Trustmark Bank to complete the transfers.

Despite this reality, MSH nevertheless seeks to invoke coverage because neither Lalley, McPheters, nor Boardwine were aware that the October 23 or the November 17 emails from "Olga Rozina" were fraudulent at the time they provided their authorization and consent. As with its argument concerning the Computer Transfer Fraud provision, however, MSH provides no legitimate basis for the Court to impose a heightened "knowledge or consent" standard, in light of its absence from the provision itself. For the same reasons set forth above in connection with MSH's arguments on that point in connection with the Computer Transfer Fraud provision, the Court views MSH's argument on this point as an effort to circumvent the clear language of the provision in order to achieve a desired result.

MSH also argues that AXIS' proposed interpretation of the Funds Transfer Fraud provision should be rejected because, if it were adopted, there would be no distinction between the coverage provided under the Computer Transfer Fraud provision and the Funds Transfer Fraud provision. According to MSH, this would render the Funds Transfer Fraud provision mere "surplusage."

Even a cursory review of the provisions reveals that the coverage provided under each provision is distinguishable. The Computer Transfer Fraud provision covers a loss that occurs when funds are transferred, paid, or delivered to a person, place, or account beyond the insured's control without the insured's knowledge or consent. While the coverage afforded under the Funds Transfer Fraud provision is similar, that provision requires that the loss involve a financial institution's reliance on an instruction by the insured which was actually issued without the insured's knowledge or consent. The Computer Transfer Fraud provision would apply when the insured's system is manipulated without the insured's knowledge and effectuates a transfer, while

the Funds Transfer Fraud provision is only applicable when the financial institution relies upon an instruction from the insured which was ultimately not provided by the insured. Thus, although the provisions provide similar coverages, the Court's interpretation does not create redundant coverage or mere surplusage, and MSH's argument on this point is therefore rejected.

Ultimately, the Funds Transfer Fraud provision unambiguously requires that the loss occur as a result of a financial institution's reliance upon an instruction which was actually issued without the insured's knowledge or consent. The undisputed facts of this case establish that three MSH employees were aware of and specifically authorized the transfer. The Funds Transfer Fraud provision is inapplicable.[6]

II. Case Law

As previously noted, if the Court determines that the subject provisions are unambiguous, it need not look beyond the Policy's four corners. *Langston v. Taylor*, 766 So.2d 66, 67 (Miss. Ct. App. 2000). Nevertheless, despite the fact that the parties have not referenced, and the Court has not located, any cases interpreting identical policy language, the Court has reviewed other cases interpreting insurance policies regarding computer transfer fraud.

The Court finds noteworthy a case involving somewhat similar facts where the Fifth Circuit deemed an insurance policy's "Computer Fraud" provision inapplicable. *Apache Corp. v.*

[6] The Court also notes that the parties had a discovery dispute as to whether MSH was entitled to certain discovery relating to a subsequent change which AXIS made to its form policy after MSH made its claim forming the basis of this action. The parties raised the issue before Magistrate Judge Sanders who ultimately entered an Order [70] determining that MSH was not entitled to the requested discovery, largely based upon Rule 407 of the Federal Rules of Evidence. MSH filed an Objection [76], requesting that the Magistrate Judge's decision be overruled. In light of the Court's determination that the subject provisions are clear and unambiguous, the Court need not look beyond the four corners of the Policy. *See Lee*, 17 So.3d at 600. Accordingly, the Court finds that the Objection [76] need not be addressed.

Great American Ins. Co., 662 F. App'x 252 (5th Cir. 2016).[7] In *Apache*, the plaintiff company, an oil-production company located in Houston, Texas, received a telephone call from an individual purporting to be one of the plaintiff's vendors and requesting that the plaintiff change the bank account information for its future wire payments to the vendor. *Id*. at 253. A representative from the plaintiff company requested that the vendor send a formal request containing the new bank account information on the vendor's letterhead. *Id*. The fraudulent actor obliged and emailed the plaintiff company a document which contained the fraudulent actor's banking information on fake letterhead. *Id*. After wiring funds to the account listed on the document, the plaintiff company later became aware that it had been the victim of fraud. *Id*. The company thereafter made a claim on its insurance policy, requesting that it be provided coverage under the policy's "Computer Fraud" provision, which provided:

> [The insurer] will pay for loss of, and loss from damage to, money, securities and other property resulting directly form 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.

Id. Ultimately, the Fifth Circuit, after providing an overview of various cases from across the country addressing similar policy language, determined that the "Computer Fraud" provision was inapplicable, specifically holding that "[t]he 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

[7] In addition to noting that the Fifth Circuit applied Texas law in *Apache*, the Court also recognizes that the case is not published. 662 F. App'x at 253. However, the Court does not solely rely upon *Apache* for reaching its decision but nevertheless finds the Fifth Circuit's analysis and reasoning instructive.

was part of the process would . . . convert the computer-fraud provision to one for general fraud." *Id*. at 258.[8]

Although the underlying facts in this case are not identical to *Apache*, particularly the fact that the *Apache* plaintiff specifically requested that the fraudulent actor send the email which ultimately contained false information, the Fifth Circuit's analysis supports the Court's conclusion in this case. Here, as in *Apache*, the transfer of funds was initiated and authorized by an employee of MSH. And as noted by the Fifth Circuit in *Apache*, an application of a "computer fraud" insurance provision in circumstances where an employee explicitly authorized the subject transfer in response to an email would effectively convert all provisions of this type into general fraud provisions, especially considering that a large percentage of fraudulent schemes will likely involve a computer in one way or another. Like the Fifth Circuit in *Apache*, this Court declines to adopt such an expansive interpretation of this type of provision, particularly considering the Policy's clear and unambiguous language to the contrary.

Ultimately, MSH's position, similar to the argument made by the plaintiff in *Apache*, ignores the plain and unambiguous language and intent of the subject provisions and should not be judicially sanctioned.

[8] Among other cases, the Fifth Circuit's analysis in *Apache* considered *Pestmaster Services, Inc. v. Travelers Cas. and Sur. Co. of America*, 2014 WL 3844627 (C.D. Cal. July 8, 2014). In *Pestmaster*, the District Court for the Central District of California held that an insurance policy containing similar language to the Policy at issue here was not applicable because the subject transfers had actually been authorized. *Id*. at *5. Specifically, the district court provided that "[t]he Funds Transfer Fraud Insuring Agreement does not cover authorized or valid electronic transactions, such as the authorized ACH transfers in this case, *even though they are, or may be, associated with a fraudulent scheme*." *Id*. (emphasis added). The district court's analysis on this issue was affirmed by the Ninth Circuit. *See Pestmaster Services, Inc. v. Travelers Cas. and Sur. Co. of America*, 656 F. App'x 332 (9th Cir. 2016). Although the underlying facts of *Pestmaster* are not factually identical to the case at bar, the analysis is instructive.

Conclusion

For the reasons set forth above, MSH's Motion for Summary Judgment [95] is DENIED, and AXIS' Motion for Summary Judgment [93] is GRANTED. MSH's claims are dismissed *with prejudice*. This case is CLOSED.

SO ORDERED, this the 21st day of February, 2020.

/s/ Sharion Aycock
UNITED STATES DISTRICT JUDGE