UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

SJ COMPUTERS, LLC, Plaintiff, v. TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA, Defendant.	Case No. 21-CV-2482 (PJS/JFD) ORDER

Syed S. Ahmad, Kelly R. Oeltjenbruns, and Latosha M. Ellis, HUNTON ANDREWS KURTH LLP, for plaintiff.

Joel T. Wiegert, HINSHAW & CULBERTSON LLP, for defendant.

Plaintiff SJ Computers was defrauded when a bad actor tricked the company's CEO into wiring nearly $600,000 into the bad actor's bank account. After discovering the fraud, SJ Computers submitted a claim to defendant Travelers Casualty and Surety Company of America ("Travelers"), which had issued a crime-insurance policy to the company. That policy has two insuring agreements that are relevant to this lawsuit: a social-engineering-fraud agreement and a computer-fraud agreement. Those two agreements are mutually exclusive—i.e., a loss covered by one is not covered by the other.

The loss suffered by SJ Computers falls squarely within the social-engineering-fraud agreement. Indeed, when SJ Computers tendered its claim to Travelers,

SJ Computers did so *only* under the social-engineering-fraud agreement. But SJ Computers later realized that the policy limit applicable to a social-engineering-fraud claim is $100,000, while the policy limit applicable to a computer-fraud claim is $1,000,000. SJ Computers then made a series of arguments—ranging from creative to desperate—to try to persuade Travelers that its loss was not the result of social-engineering-fraud (as SJ Computers itself had initially said) but instead the result of computer fraud. Travelers rejected those arguments and agreed to pay the claim under the social-engineering-fraud agreement.

SJ Computers then brought this coverage action against Travelers, alleging breach of the insurance contract and breach of the duty of good faith and fair dealing. Compl. ¶¶ 59–75 [ECF No. 1]. This matter is now before the Court on Travelers' motion to dismiss. Because it is clear that SJ Computers was the victim of social-engineering fraud and not computer fraud, the Court grants the motion and dismisses SJ Computers' complaint with prejudice.

I. BACKGROUND

A. The Loss

SJ Computers routinely orders computer equipment from various vendors. The ordering process generally proceeds as follows: First, SJ Computers' purchasing manager issues a purchase order to the vendor. Then the vendor issues an invoice to

SJ Computers for the cost of the equipment ordered. After that, the purchasing manager confirms the accuracy of the invoice and forwards it to SJ Computers' CEO. Finally, after receiving the invoice from the purchasing manager, the CEO initiates a wire-transfer payment to the vendor. Compl. ¶¶ 20–23.

In March 2021, a bad actor (still unidentified) emailed fraudulent invoices to SJ Computers' purchasing manager, purportedly from one of SJ Computers' existing vendors, Electronic Recyclers International Direct ("ERI Direct"). The fraudulent invoices instructed SJ Computers to pay the invoices by making wire transfers to a bank-account number that was different from the bank-account number that ERI Direct had used in the past. That new account, of course, belonged to the bad actor.

After emailing the fraudulent invoices to the purchasing manager, the bad actor hacked into the purchasing manager's email account and, impersonating the purchasing manager, forwarded the invoices to SJ Computers' CEO for payment. *Id.* ¶¶ 26–27. Upon receipt of the emails (which appeared to come from the purchasing manager) and the fraudulent invoices (which included the new wire-transfer instructions), the CEO tried to call ERI Direct to confirm the change to the wire-transfer instructions. No one at ERI Direct answered the CEO's call, however, so he left a voice-mail message. ERI Direct did not return the CEO's call prior to the payment deadline that had been provided in the fraudulent invoices, so the CEO decided to move ahead

with paying the invoices before he spoke to ERI Direct. Following the new wire-transfer instructions, the CEO initiated two wire transfers totaling $593,555.00—payments that he thought he was making to ERI Direct, but that he was in fact making to the bad actor. *Id*. ¶ 28. SJ Computers discovered the fraud a few days later, after the bad actor had already withdrawn the funds that had been deposited in his account. *Id*. ¶¶ 30–31.

B. The Policy

At the time of the fraud, SJ Computers was insured under a Travelers Wrap+ crime-insurance policy (the "Policy"). *Id.* ¶ 10. The Policy provides SJ Computers with two types of fraud coverage relevant to this lawsuit: (1) coverage for losses caused by social-engineering fraud (with a single-loss limit of $100,000) and (2) coverage for losses caused by computer fraud (with a single-loss limit of $1,000,000). *Id.* ¶ 40; Policy Terms [ECF Nos. 1-2 and 1-3] at SJC-TravPolicy-7.[1]

The Policy's computer-fraud insuring agreement provides that Travelers will pay for a "direct loss . . . directly caused by **Computer Fraud**." Policy Terms at SJC-TravPolicy-65. The Policy defines computer fraud as "an intentional, unauthorized, and fraudulent entry or change of data or computer instructions directly into a **Computer**

[1]The Policy was attached to the complaint, with part of it filed under one docket entry (ECF No. 1-2) and the other part filed under a separate docket entry (ECF No. 1-3). To avoid confusion, the Court will cite pages of the Policy by Bates number.

System." *Id.* at SJC-TravPolicy-94. Critically, though, the Policy also provides that computer fraud does *not* include "such entry or change made by an **Employee** [or] **Authorized Person** . . . made in reliance upon any fraudulent . . . instruction," nor does it include "**Social Engineering Fraud**." *Id.*[2]

The Policy's social-engineering-fraud insuring agreement provides that Travelers will pay for a "direct loss . . . directly caused by **Social Engineering Fraud**." *Id.* at SJC-TravPolicy-93. Social-engineering fraud is defined as:

> the intentional misleading of an **Employee** or **Authorized Person** by a natural person impersonating:
>
> (1) a **Vendor**, or that **Vendor's** attorney;
> (2) a **Client**, or that **Client's** attorney;
> (3) an **Employee**; or
> (4) an **Authorized Person**,
>
> through the use of a **Communication**.

Id. The Policy provides that, solely for purposes of the social-engineering-fraud insuring agreement, coverage "will not apply to loss or damage due to . . . **Computer Fraud**." *Id.* at SJC-TravPolicy-95 (cleaned up). Thus, the two insuring agreements are mutually exclusive: A loss caused by social-engineering fraud is excluded from

---

[2]This definition of computer fraud is contained in the Social Engineering Fraud Insuring Agreement Endorsement ("Endorsement"), which is attached to the Policy. The definition in the Endorsement supersedes a different definition found elsewhere in the Policy. The parties agree that the quoted definition from the Endorsement is the one that applies here.

coverage under the computer-fraud agreement, and a loss caused by computer fraud is excluded from coverage under the social-engineering-fraud agreement.

Finally, the Policy includes an exclusion—Exclusion H[3]—that applies to all coverage provided under the Policy *except* the coverage provided under the social-engineering-fraud agreement (and three insuring agreements not relevant here). Exclusion H provides:

> This **Crime Policy** will not apply to loss resulting from forged, altered, or fraudulent negotiable instruments, securities, documents, or instructions used as source documentation to enter **Electronic Data** or send instructions, provided this does not apply to . . . the Social Engineering Fraud Insuring Agreement.

Id.

C. Present Dispute

After discovering the fraud, SJ Computers submitted a proof-of-loss statement to Travelers. Compl. ¶ 38. SJ Computers claimed coverage under only the social-engineering-fraud insuring agreement. *See* Compl. Ex. 9 [ECF No. 1-11] (Proof of Loss statement). Later, however, SJ Computers apparently realized that the computer-fraud agreement had a much higher liability limit than the social-engineering-fraud agreement. SJ Computers revised its claim to seek coverage under the computer-fraud

[3]This exclusion is contained in the Endorsement and replaces a different "Exclusion H" contained elsewhere in the Policy.

agreement. *See* Compl. Ex. 11 [ECF No. 1-13] (June 22, 2021, letter from SJ Computers' counsel to Travelers, seeking reconsideration of Travelers' denial of computer-fraud coverage).

Travelers accepted coverage for the loss under the social-engineering-fraud insuring agreement, but declined coverage under the computer-fraud agreement. Compl. ¶ 40. This lawsuit followed. The central question in this lawsuit is whether the loss suffered by SJ Computers is covered under the social-engineering-fraud insuring agreement (in which case Travelers has met its obligations under the Policy) or under the computer-fraud insuring agreement (in which case Travelers owes SJ Computers another $500,000 or so). *Id*. ¶¶ 61–64. Travelers has moved to dismiss, arguing that it is clear from the complaint and the documents attached to and embraced by the complaint that SJ Computers' loss is not covered under the computer-fraud agreement.

II. ANALYSIS

A. Standard of Review

In reviewing a motion to dismiss under Fed. R. Civ. P. 12(b)(6), the court must accept as true all of the factual allegations in the complaint and draw all reasonable inferences in the plaintiff's favor. *Du Bois v. Bd. of Regents*, 987 F.3d 1199, 1202 (8th Cir. 2021). Although the factual allegations in the complaint need not be pleaded in great

detail, they must be sufficient to "raise a right to relief above the speculative level." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

Ordinarily, if the parties present, and the court considers, matters outside of the pleadings, a Rule 12(b)(6) motion must be treated as a motion for summary judgment. Fed. R. Civ. P. 12(d). But the court may consider materials that are necessarily embraced by the complaint, as well as any exhibits attached to the complaint, without converting the motion into one for summary judgment. *Zean v. Fairview Health Servs.*, 858 F.3d 520, 526 (8th Cir. 2017).

Here, the parties submitted several documents for the Court to consider in ruling on Travelers' motion, including the Policy terms, the fraudulent invoices and emails, and communications between Travelers and SJ Computers. All of these documents were referred to, cited, or quoted in SJ Computers' complaint, so they are not deemed to be matters outside of the pleadings. *Id.* ("documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the pleadings" are nevertheless embraced by the complaint (quoting *Ashanti v. City of Golden Valley*, 666 F.3d 1148, 1151 (8th Cir. 2012))). Moreover, the parties agree that all of these documents are authentic. Accordingly, the Court will consider these documents without converting Travelers' motion to dismiss into a motion for summary judgment.

B. Computer-Fraud Coverage

"An insurance policy 'must be construed as a whole, and unambiguous language must be given its plain and ordinary meaning.'" *Midwest Fam. Mut. Ins. Co. v. Wolters*, 831 N.W.2d 628, 636 (Minn. 2013) (quoting *Henning Nelson Constr. Co. v. Fireman's Fund Am. Life Ins. Co.*, 383 N.W.2d 645, 652 (Minn. 1986)); *see also Eng'g & Constr. Innovations, Inc. v. L.H. Bolduc Co.*, 825 N.W.2d 695, 705 (Minn. 2013) ("[W]e read the terms of an insurance contract in the context of the entire contract[.]" (quotation omitted)). The goal "is to 'ascertain and give effect to the intentions of the parties as reflected in the terms of the insuring contract.'" *Eng'g & Constr. Innovations*, 825 N.W.2d at 704 (quoting *Jenoff, Inc. v. N.H. Ins. Co.*, 558 N.W.2d 260, 262 (Minn. 1997)). "Where the language of an insurance policy is clear and unambiguous, we effectuate the intent of the parties by interpreting the policy according to plain, ordinary sense." *Id.* (cleaned up).

Travelers offers several reasons why SJ Computers' loss is not covered under the computer-fraud agreement: First, the conduct in which the bad actor engaged was not computer fraud as that term is defined by the Policy. Second, even if the bad actor engaged in computer fraud, SJ Computers' loss was not "directly caused by" that computer fraud. Third, Exclusion H of the Policy explicitly precludes computer-fraud coverage for SJ Computers' loss. And finally, the conduct in which the bad actor engaged meets the definition of social-engineering fraud, and social-engineering fraud

is explicitly excluded from coverage under the computer-fraud agreement. For the reasons that follow, the Court agrees with Travelers on every point.

1. The Policy Precludes Computer-Fraud Coverage for SJ Computers' Loss

To begin, the Court agrees with Travelers that the conduct that caused SJ Computers' loss does not satisfy the Policy definition of computer fraud. That definition explicitly excludes any "entry or change [of data or computer instructions] made by an **Employee** [or] **Authorized Person** . . . made in reliance upon any fraudulent . . . instruction." Policy Terms at SJC-TravPolicy-94. That is *precisely* what happened here. The CEO of SJ Computers is an "Employee" of the company. He made an "entry or change" of data into SJ Computers' computer system—specifically, he used the computer system to change the wire-payment instructions for ERI Direct and initiate wire transfers to what he thought was ERI Direct's bank account. And he did so "in reliance upon any fraudulent instruction"—specifically, the fraudulent instructions that had been provided in the fake invoices.

SJ Computers works hard to avoid the plain language of the Policy. SJ Computers argues that it was actually the victim of *two* distinct fraudulent acts: (1) the bad actor hacking into SJ Computers' email system and forwarding the fraudulent invoices from the purchasing manager's email account to the CEO; and (2) the CEO acting on those fraudulent invoices and emails by initiating the wire

transfers to the bad actor's account. SJ Computers concedes that the latter—the CEO's initiation of the wire transfers—is excluded from the definition of computer fraud, for the reasons just explained. But SJ Computers argues that the former—the bad actor's emailing the fake invoices to the CEO—is not excluded from the definition of computer fraud, because the bad actor was not an "Employee [or] Authorized Person," and because the bad actor was not acting "in reliance upon any fraudulent instruction."

SJ Computers' argument is creative but ultimately unavailing. The Court seriously doubts whether a single course of fraud can be fragmented into separate fraudulent acts, as SJ Computers proposes. Putting that aside, however, even if the bad actor's hacking of the purchasing manager's email account is viewed in isolation and deemed to be an act of computer fraud, that hacking did not "directly cause[]" a "direct loss" to SJ Computers, as is required by the computer-fraud insuring agreement. *See id.* at SJC-TravPolicy-65 ("The Company will pay the **Insured** for the **Insured's** direct loss . . . directly caused by **Computer Fraud**.").

No Minnesota court has yet interpreted what "direct" or "directly caused" means in the context of computer and social-engineering fraud, and the Minnesota cases cited by SJ Computers are easily distinguishable. *See, e.g.*, *Mork v. Eureka-Sec. Fire & Marine Ins. Co.*, 42 N.W.2d 33 (Minn. 1950) (discussing causation in context of fire damage); *George v. Est. of Baker*, 724 N.W.2d 1 (Minn. 2006) (discussing causation in wrongful-

death action arising out of traffic accident); *Osborne v. Twin Town Bowl, Inc.*, 749 N.W.2d 367 (Minn. 2008) (discussing causation in dram-shop action).

The only cases either party cites (or that the Court has been able to find) that analyze the concept of direct causation in the context of computer or social-engineering fraud are from other jurisdictions. *See, e.g.*, *Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc.*, 23 F.4th 1195 (9th Cir. 2022) (insured's loss "result[ed] directly" from computer fraud when an employee unwittingly initiated a payment, relying on a fraudulent email); *Miss. Silicon Holdings, L.L.C. v. Axis Ins. Co.*, 843 Fed. App'x 581 (5th Cir. 2021) (insured cannot recover under Computer Transfer Fraud provision of policy because transfers were not made without the insured's knowledge or consent); *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455 (6th Cir. 2018) (insured suffered a "direct loss" that was "directly caused by" computer fraud when it authorized wire transfers to an impersonator).

But those cases are distinguishable in a crucial respect: None of them analyze an insurance policy that covers *both* computer fraud *and* social-engineering fraud—much less an insurance policy that makes clear that computer fraud and social-engineering fraud are mutually exclusive categories.

Some Minnesota cases do suggest that, in other circumstances, directness might be a relatively broad concept. *See, e.g.*, *Lipshultz v. Gen. Ins. Co. of Am.*, 96 N.W.2d 880,

885 (Minn. 1959) (where "the chain of events culminating in the loss . . . was set in motion by a windstorm" the loss was a "direct loss by windstorm" within meaning of insurance policy). The fact remains, however, that the meaning of "direct" in *this* Policy must be determined "in the context of [this] entire contract." *Eng'g & Constr. Innovations*, 825 N.W.2d at 705 (quoting *Emp'r Mut. Liab. Ins. Co. of Wis. v. Eagles Lodge of Hallock, Minn.*, 165 N.W.2d 554, 556 (Minn. 1969)).

The Policy clearly anticipates—and clearly addresses—precisely the situation that gave rise to SJ Computers' loss, and the Policy bends over backwards to make clear that this situation involves social-engineering fraud, not computer fraud. The Policy defines social-engineering fraud as "the intentional misleading of an **Employee** . . . by a natural person impersonating . . . a **Vendor** . . . [or] an **Employee** . . . through the use of a **Communication**." Policy Terms at SJC-TravPolicy-93. That is exactly what happened here. The Policy also *excludes* from the definition of computer fraud "[an] entry or change made by an **Employee** . . . made in reliance upon any fraudulent . . . instruction." *Id.* at SJC-TravPolicy-94. Again, that is exactly what happened here. And the Policy makes abundantly clear that social-engineering fraud and computer fraud are mutually exclusive categories. *See id.* at SJC-TravPolicy-94, -95. In short, the drafters of the Policy anticipated precisely the type of fraud that victimized SJ Computers, defined

that fraud as social-engineering fraud, and, for good measure, excluded that fraud from the definition of computer fraud.

SJ Computers' argument that, notwithstanding these Policy provisions, the company was actually the victim of computer fraud is premised on its position that one aspect of the fraudulent scheme—the bad actor's using the purchasing manager's email account to forward the fraudulent invoices to the CEO—should be viewed in isolation. But what is good for the goose is good for the gander. If that aspect of the fraudulent scheme is going to be viewed in isolation, then that aspect needs to be viewed in isolation for all purposes.

The bad actor's use of the purchasing manager's email account to forward the fraudulent invoices to the CEO—*when viewed in isolation*—did not "directly cause[]" a "direct loss" to SJ Computers. *See id.* at SJC-TravPolicy-65 ("The Company will pay the **Insured** for the **Insured's** direct loss . . . directly caused by **Computer Fraud**."). SJ Computers did not suffer a penny of financial loss when the bad actor hit "send" on his email messages. And SJ Computers would *never* have suffered a penny of financial loss if the CEO had not opened those email messages, or if the CEO had asked the purchasing manager about them, or if ERI Direct had answered its phone when the CEO called, or if ERI Direct had promptly returned the voice-mail message left by the CEO, or if the CEO had waited to hear from ERI Direct before paying the invoices. If

the fraudulent scheme that victimized SJ Computers is going to be fragmented into pieces and each piece viewed in isolation, then what "directly caused" loss to SJ Computers was not the piece involving the bad actor's use of the purchasing manager's account to send the fake invoices, but rather the piece involving the CEO's use of his computer to *act* on the fake invoices. *That* piece—the piece that *did* "directly cause[]" a "direct loss" to SJ Computers—was social-engineering fraud, not computer fraud, as even SJ Computers concedes.

That finding, in and of itself, requires dismissal of SJ Computers' complaint. To be thorough, however, the Court will address the other arguments made by Travelers, each of which provides an independent basis for granting its motion to dismiss.

2. Exclusion H Also Precludes Coverage

Even if SJ Computers had been victimized by computer fraud—and even if its claim met all of the requirements of the computer-fraud insuring agreement—Exclusion H would nevertheless wipe out that coverage. Exclusion H provides that the Policy (including the computer-fraud insuring agreement) does not apply to "loss resulting from forged, altered, or fraudulent . . . instructions used as source documentation to enter **Electronic Data** or send instructions[.]" *Id.* at SJC-TravPolicy-95. Again, that is exactly the type of loss that is at issue in this case: SJ Computers' loss resulted from "fraudulent instructions" that its CEO "used as source documentation" to

"send instructions" to SJ Computers' bank to wire money to the bad actor's account. Accordingly, the unambiguous language of Exclusion H bars SJ Computers from recovering under the computer-fraud agreement.

Notably, Exclusion H explicitly provides that it "does not apply to . . . the Social Engineering Fraud Insuring Agreement." *Id.* This is yet another way—at this point, the fourth or fifth—in which the Policy makes clear that the type of fraud experienced by SJ Computers is social-engineering fraud, not computer fraud.

In an attempt to avoid the plain language of Exclusion H, SJ Computers makes a rather tortured argument: SJ Computers notes that Exclusion H does not apply to the social-engineering-fraud agreement. That is true. SJ Computers also notes that the definition of "computer fraud" that applies in this case is located within the social-engineering-fraud agreement. That too is true. SJ Computers concludes by arguing that, because the definition of "computer fraud" is found in the social-engineering-fraud agreement, and because Exclusion H does not apply to that agreement, Exclusion H does not exclude coverage under the computer-fraud agreement. That is not true.

Exclusion H applies to *all* of the coverage provided under the Policy—including the coverage provided under the computer-fraud agreement—with a very limited exception: Exhibit H does not apply to the coverage provided under the social-

engineering-fraud agreement. As SJ Computers would have it, however, because the *definition of a term* ("computer fraud") is found in the social-engineering-fraud agreement, Exclusion H does not apply to *any* insuring agreement within the Policy that uses that term.

That would be a bizarre way to write—or to interpret—the Policy. Insurers are obligated to pay claims by insuring clauses, not by definitional clauses, and Exclusion H clearly excludes coverage of SJ Computers' loss under the computer-fraud insuring clause.

3. The March 2021 Fraud Is Social-Engineering Fraud

As the Court has already explained, the fraud described in the complaint fits squarely within the Policy's definition of social-engineering fraud. The fraud involved (1) "the intentional misleading of an **Employee**" (the CEO of SJ Computers) (2) "by a natural person" (the bad actor) (3) "impersonating a **Vendor**" (ERI Direct) or "an **Employee**" (the purchasing manager of SJ Computers) (4) through the use of a **Communication** (the fake invoices and emails). Policy Terms at SJC-TravPolicy-93.

SJ Computers desperately attempts to avoid this obvious conclusion and, for reasons that escape the Court, attempts to prolong a lawsuit that it is destined to lose. Specifically, SJ Computers argues that, based on the face of the complaint and other documents before the Court, the Court cannot rule *at this time* that ERI Direct was a

"Vendor" or that SJ Computers' own purchasing manager was an "Employee." The Court will address these arguments in turn.

a. Impersonation of a Vendor

In its complaint, *SJ Computers itself* identifies ERI Direct as one of its "vendors." *See* Compl. ¶¶ 24, 33. That would seem to be the end of that matter. In order to stave off dismissal, however, SJ Computers now argues that its complaint was just using the "plain reading" of the term "vendor" and that the Policy's definition of the term "require[s] more." Pl. Memo. at 6 n.2 [ECF No. 19].

The Policy defines vendor as "an entity . . . that has provided goods or services to the **Insured** under a genuine, pre-existing, written agreement or other agreed-upon arrangement." Policy Terms at SJC-TravPolicy-93. It is true that the complaint does not explicitly allege that SJ Computers had a "genuine, pre-existing" arrangement with ERI Direct before it was defrauded. But that is made unmistakably clear by what *is* explicitly alleged in the complaint.

The complaint alleges that "on or before March 23, 2021"—that is, about a week before SJ Computers was defrauded—SJ Computers had received a legitimate invoice from ERI Direct and had paid that invoice by making a wire transfer to ERI Direct's account. *See* Compl. ¶¶ 24–25. A "few days later"—that is, a few days after SJ Computers completed a legitimate transaction in which it purchased goods from

ERI Direct—the bad actor sent fake invoices to the purchasing manager's account and then used the purchasing manager's account to forward the invoices to the CEO. *Id.* ¶ 26. The complaint alleges that the CEO was concerned about the "request[] to *change* account information"—meaning that SJ Computers *had* account information for ERI Direct—and that the CEO therefore called "SJ Computers' contact at ERI Direct"—meaning that SJ Computers *had* a contact at ERI Direct. *Id.* at ¶ 28 (emphasis added). These allegations make clear that ERI Direct was "an entity" that had previously "provided goods or services to [SJ Computers]" and had done so "under . . . [an] agreed-upon arrangement." Although the terms of that "arrangement" are not explicitly alleged, ERI Direct obviously did not randomly send goods to SJ Computers, without any kind of understanding about what goods it would send or what SJ Computers would pay for those goods.

In short, the allegations of the complaint leave no reasonable doubt that ERI Direct was a "Vendor" as that term is defined in the Policy.

b. Impersonation of an Employee

The Policy defines social-engineering fraud as involving not only the misleading of an employee by a person impersonating a "Vendor," but also the misleading of an employee by a person impersonating an "Employee." And thus, even if the bad actor had not impersonated a "Vendor" (ERI Direct), he nevertheless impersonated an

"Employee" (the purchasing manager), and thus he engaged in social-engineering fraud. *Id*. ¶ 27.

At the hearing on Travelers' motion, SJ Computers suggested that maybe its purchasing manager was not really its "Employee" and maybe the bad actor had not really "impersonated" the purchasing manager. (Apparently SJ Computers wants to put the Court and Travelers through the expense of discovery so it can discover whether its own purchasing manager was its employee.) These arguments are frivolous. The Policy's definition of employee is extremely broad, providing that an "Employee" is, among others, "any natural person" who is compensated by the insured and "who the **Insured** has the right to direct and control while performing services for the **Insured**." *See* Policy Terms at SJC-TravPolicy-70, -71.

Admittedly, the complaint does not explicitly state that the purchasing manager was compensated or that SJ Computers had the right to control him, just as the complaint does not explicitly state that the purchasing manager was a natural person. But in ruling on a motion to dismiss, the Court is permitted to use a modicum of common sense and consider not just what is said explicitly, but what is clearly implied. It is absurd to suggest that SJ Computers did not have the "right" to control its own purchasing manager or that it did not compensate its purchasing manager in any way—even though, according to the complaint, the purchasing manager had

responsibility for managing the company's invoices, *see* Compl. ¶¶ 22–23, and had an email address hosted at the company's domain, *see* Compl. Ex. 2 [ECF No. 1-4]. Equally absurd is the suggestion that the bad actor was not "impersonating" the purchasing manager when he hacked into the purchasing manager's account so that he could send email messages that appeared to come from the purchasing manager when in fact they came from the bad actor.

It bears repeating that, after it discovered the fraud, SJ Computers represented to Travelers that it was entitled to recover under the social-engineering-fraud agreement. In other words, *SJ Computers itself* concluded that ERI Direct was a "Vendor" and that its purchasing manager was an "Employee" for purposes of the Policy. SJ Computers was right the first time.

Because the fraud that caused SJ Computers' loss plainly meets the definition of social-engineering fraud, that fraud cannot also meet the definition of computer fraud. The Policy could not be clearer on this point: "**Computer Fraud** does not include **Social Engineering Fraud**[.]" Policy Terms at SJC-TravPolicy-94.[4]

* * *

[4]SJ Computers points out that the Policy contains a general provision that contemplates that a loss might be covered under more than one of the various insuring agreements. *See* Policy Terms at SJC-TravPolicy-81, -82. But that provision does not trump the multiple specific provisions that make clear that a loss caused by social-engineering fraud is not covered under the computer-fraud agreement.

In sum, it is clear from the complaint and the documents attached to and embraced by the complaint that SJ Computers' loss is covered under the social-engineering-fraud agreement and not under the computer-fraud agreement. Travelers' motion to dismiss is therefore granted.

ORDER

Based on the foregoing, and on all of the files, records, and proceedings herein, IT IS HEREBY ORDERED THAT defendant's motion to dismiss [ECF No. 13] is GRANTED and plaintiff's complaint [ECF No. 1] is DISMISSED WITH PREJUDICE AND ON THE MERITS.

LET JUDGMENT BE ENTERED ACCORDINGLY.

Dated: August 12, 2022

s/Patrick J. Schiltz
Patrick J. Schiltz, Chief Judge
United States District Court