IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

OFFICE OF THE SPECIAL DEPUTY RECEIVER,	)	
Plaintiff,	)	No. 22-cv-03709
v.	)	Judge Andrea R. Wood
HARTFORD FIRE INSURANCE CO., et al.,	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

Plaintiff Office of the Special Deputy Receiver ("OSD"), an Illinois corporation that handles the estates of insolvent or troubled Illinois insurance companies, suffered a breach of its computer systems that led to the illicit transfer of millions of dollars in a social engineering scheme. OSD successfully halted some of the transfers but still could not recover millions of dollars. So, it sought coverage for the losses from two of its own insurers, Defendants Hartford Fire Insurance Company ("Hartford") and HSB Specialty Insurance Company ("HSB"), with which it had coverage applying to computer fraud and social engineering. Hartford denied OSD's claim entirely and HSB denied it in part. As a result, OSD seeks declaratory judgments and asserts claims for breach of contract against both insurers based on their refusal to provide coverage. Both Defendants have moved to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(6). (Dkt. Nos. 21, 27.) For the reasons that follow, Hartford's motion is granted but HSB's motion is denied.

BACKGROUND

For purposes of the motions to dismiss, the Court accepts all well-pleaded facts in the complaint as true and views those facts in the light most favorable to OSD as the non-moving

party. *Killingsworth v. HSBC Bank Nev., N.A.*, 507 F.3d 614, 618 (7th Cir. 2007). The Complaint alleges as follows.

I. Hack of OSD and Resulting Fraud

OSD, an Illinois non-profit corporation, administers receivership estates for insolvent or financially troubled Illinois insurance companies. (Compl. ¶¶ 9, Dkt. No. 1.) Gateway Insurance Company ("Gateway"), a commercial automobile insurer, and Affirmative Insurance Company ("Affirmative"), a personal automobile insurer, entered liquidation in March 2016 and June 2020, respectively. (*Id.* ¶¶ 2, 20.) After Gateway and Affirmative entered liquidation, OSD administered their receivership estates. (*Id.* ¶ 9.) That meant OSD "marshalled and managed" the two insurers' assets for distribution to consumers and creditors pursuant to various statutory claim procedures. (*Id.* ¶ 20.)

OSD contracted for insurance coverage from at least two firms: Hartford and HSB. (*Id.* ¶¶ 22, 25.) Hartford and HSB provided OSD with coverage that, among other things, covered loss due to computer fraud and social engineering.[1] (*Id.* ¶¶ 22–23, 25.) In June 2021, an unknown hacker perpetrated a "spear phishing" attack on OSD's then-Chief Financial Officer ("CFO"). (*Id.* ¶ 15.)[2] As a result of the attack, the hacker was able to access and review the CFO's OSD Outlook account and gain an understanding of OSD's key employees and its internal terminology. (*Id.* ¶ 15.) Posing as the CFO, the hacker emailed accounting and finance employees of OSD, requesting wire transfers from Gateway's and Affirmative's accounts,

[1] In this context, social engineering refers to "social methods (such as phishing) that are used to obtain personal or confidential information which can then be used illicitly." *Social engineering*, Merriam-Webster, https://www.merriam-webster.com/dictionary/social%20engineering (last visited March 28, 2025).

[2] Spear phishing is "a targeted attempt to trick a specific person into revealing personal or confidential information that can then be used illicitly." *Spear phishing*, Merriam-Webster, https://www.merriam-webster.com/dictionary/spear %20phishing (last visited March 28, 2025).

purportedly to fund new investments. (*Id.* ¶ 16.) The hacker managed to impersonate the CFO during eight separate transfers in part because they altered the Outlook rules on the CFO's account. (*Id.* ¶ 17.) Those rules allowed any e-mails regarding the eight transfers to circumvent the CFO's inbox—and, by extension, avoid the CFO's attention—so that the hacker could reply directly to the finance and accounting staff's questions. (*Id.*) The employees carried out the instructions, resulting in eight wire transfers between June 23, 2021 and July 14, 2021, totaling approximately $6.85 million. (*Id.* ¶ 18.) Upon discovering the scheme, OSD immediately informed its bank, Bank of America, which was able to halt some of the transfers and recover roughly $2.87 million. (*Id.* ¶ 19.) Another $3.98 million remains outstanding. (*Id.*) OSD notified Hartford and HSB of the incidents and sought coverage through its insurance broker, Alliant Insurance Services, Inc. ("Alliant"). (*Id.* ¶¶ 28, 38.)

II. Hartford Bond Coverage

Hartford issued an insurance policy to OSD in May 2021 with a $5 million aggregate liability limit ("Hartford Bond" or "Bond"). (*Id.* ¶ 23.) The particular type of Bond that Hartford issued is called a "Financial Institution Bond for Insurance Companies." (Compl., Ex. 1 ("Hartford Bond") at 5, Dkt. No. 1-1.[3]) During the claims process, OSD provided all requested information to Hartford, including several letters, reports from its information technology ("IT") specialist, a Proof of Loss form, and appendices. (*Id.* ¶ 33.) Two provisions of the Bond are relevant here: Rider 13, "Computer Systems Fraud Coverage," and Rider 17, "Electronic Mail Initiated Transfer Fraud Coverage." Both riders state in large, bold, capital letters that they

[3] OSD submitted twelve exhibits in one consecutively paginated document. The Court refers to exhibits by individual number, but the page number refers to the page number as shown in the ECF header.

"change[] the bond," and both apply to the Financial Institution Bond for Insurance Companies. (Hartford Bond at 37, 45.) Rider 13 adds coverage for the following:

> Loss resulting directly from a fraudulent
>
> (1) entry of Electronic Data or Computer Program into, or
>
> (2) change of Electronic Data or Computer Program within any Computer System operated by the Insured, whether owned or leased; or any Computer System identified in the application for this bond; or a Computer System first used by the Insured during the Bond Period, as provided by General Agreement B of this bond;
>
> provided that the entry or change causes
>
> (i) property to be transferred, paid or delivered,
>
> (ii) an account of the Insured, or of its customer, to be added, deleted, debited or credited, or
>
> (iii) an unauthorized account or a fictitious account to be debited or credited.

(Compl. ¶¶ 23–24; Hartford Bond at 37.) Hartford denied coverage under Rider 13, stating that the loss did not result directly from the entry of any data—such as the alteration of the ex-CFO's Outlook rules—but instead resulted from intervening human decision-making. (Compl. ¶¶ 35–36.)

Hartford also denied coverage under Rider 17, which includes two relevant provisions. (*Id.* ¶ 34.) First, Rider 17 states that the Bond does not cover "loss resulting directly or indirectly from the Insured having, in good faith, transferred or delivered Funds, Certificated Securities or Uncertificated Securities, in reliance upon a fraudulent instruction sent to the Insured through electronic mail, except when covered under the Electronic Mail Initiated Fraud insuring agreement." (*Id.* ¶ 24; Hartford Bond at 46.) In denying coverage, Hartford took the position that this exclusion in Rider 17 covered Rider 13—in other words, even if the claim fell within Rider 13, to be covered, the claim must satisfy the Electronic Mail Initiated Fraud insuring agreement.

(Compl. ¶ 34.) To satisfy the Electronic Mail Initiated Fraud agreement and fall outside of the exclusion—that is, to be covered—the following conditions must be met:

> Loss resulting directly from the Insured having, in good faith, transferred or delivered Funds, Certificated Securities, Uncertificated Securities, in reliance upon a fraudulent instruction sent to the Insured through electronic mail, and:
>
> (1) Which fraudulent instruction purports and reasonably appears to have originated from:
>
> (a) a Customer of the Insured, or
>
> (b) an Employee acting on instructions of such Customer, or
>
> (c) another financial institution acting on behalf of such Customer with authority to make such instructions;
>
> but, in fact, was not originated by the party referenced in (a)–(c) above whose identification it bears; and
>
> (2) the sender of the fraudulent instruction verified the instruction with the required password(s), PIN(s), or other security code(s) of such Customer; and
>
> (3) the fraudulent instruction was received by an Employee of the Insured specifically authorized by the Insured to receive and act upon such instructions; and
>
> (4) for any transfer exceeding $50,000, the instruction was verified by the Insured via a call-back to a predetermined telephone number set forth in the Insured's written account agreement with such Customer or other verification procedure set forth in the Insured's written agreement with such Customer and approved in writing by the Underwriter; and
>
> (5) the Insured preserved a contemporaneous record of the call back and of the instruction which verifies use of the authorized password(s), PIN(s), or other security code(s) of the Customer.

(Compl. ¶ 24; Hartford Bond at 45.) Hartford contended that the loss at issue did not satisfy this five-part rubric. (Compl. ¶ 36.) Hartford also invoked two other exclusions, both found in Rider 13, to bar coverage: one that excludes loss "resulting directly or indirectly from . . . documents or other written instruments which bear a forged signature," and another that excludes "loss

resulting directly or indirectly from the theft of confidential information." (Compl. ¶ 37; Hartford Bond at 38.)

III. HSB Policy Coverage

HSB issued OSD a Cyber Insurance Policy that includes coverage for social engineering and computer fraud ("HSB Policy" or "Policy"). (Compl. ¶ 25.) While the Cyber Insurance Policy has an aggregate limit of $5 million, the social engineering and computer fraud clauses each are subject to a $250,000 sublimit. (*Id.* ¶ 26.)

The Computer Fraud coverage, found in Section I.E.2 of the Policy, applies to "Computer Crime Loss and Reward Expense Loss incurred by the Insured Organization as a direct result of Computer Crimes first discovered during the Policy Period." (*Id.* ¶ 27; Compl., Ex. 2 ("HSB Policy") at 59, Dkt. No. 1-1.) "Computer Crime," in turn, is defined as "the intentional, fraudulent, or unauthorized input, destruction, or modification of electronic data or computer instructions into Computer Systems by any entity which is not an Insured Organization or person who is not an Insured Person . . . ." (HSB Policy at 64.)

The social engineering coverage was amended in September 2019 to provide the following coverage:

> 1) Section I. Insuring Agreements, E. Financial Fraud, 1. Social Engineering, is deleted and replaced with the following:
>
> 1. Social Engineering
>
> We shall pay the Insured Organization for Fraudulent Inducement Loss and Reward Expense Loss incurred by the Insured Organization as a direct result of:
>
> a. Fraudulent Inducement Instructions it receives and accepts, and which are first discovered, during the Policy Period; or
>
> b. Fraudulent Inducement Instructions a Financial Institution receives and accepts, and which are first discovered, during the Policy Period.

(*Id.* at 114.) The amendment also added a definition for Fraudulent Inducement Instructions "[s]olely with respect to Insuring Agreement I.E.1, Social Engineering, part b." (*Id.*) That definition is not directly relevant here because OSD's loss arose under subpart (a), not subpart (b). (Compl. ¶ 39.) But the amendment did provide that "Fraudulent Inducement Instructions covered under Insuring Agreement I.E.1, Social Engineering, part b., does not mean or include Computer Fraud otherwise covered under Insuring Agreement I.E.2, Computer Fraud." (HSB Policy at 114.)

HSB acknowledged that subsection (a) of the Social Engineering coverage applied to OSD's loss, and issued a $250,000 check unaccompanied by a claim release to OSD in May 2022. (Compl. ¶¶ 40–41.) HSB had neither approved nor denied OSD's claim under the Computer Fraud coverage, so in June 2022, OSD inquired about HSB's position as to coverage under that provision. (*Id.* ¶ 41–42.) In its denial letter dated June 24, 2022, HSB responded that OSD's claim was not covered by the Cyber Insurance Policy because the fraud did not meet the definition of "Computer Crime" and the claim did not directly result from Computer Crimes. (*Id.* ¶ 43.)

IV. Procedural History

OSD filed this suit against Hartford and HSB asserting four counts. Count I seeks a declaratory judgment that the claim falls within the Hartford Bond's coverage. Count II asserts a breach of contract claim against Hartford, claiming that no exclusions within the Bond bar its claim. Count III seeks a declaratory judgment that the subject claim triggers the Computer Fraud coverage in the HSB Cyber Insurance Policy. And Count IV asserts a breach of contract claim against HSB for the same reasons. Hartford and HSB each have moved to dismiss the claims against them pursuant to Federal Rule of Civil Procedure 12(b)(6).

DISCUSSION

To survive a Rule 12(b)(6) motion, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). This pleading standard does not necessarily require a complaint to contain detailed factual allegations. *Twombly*, 550 U.S. at 555. Rather, "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Adams v. City of Indianapolis*, 742 F.3d 720, 728 (7th Cir. 2014) (quoting *Iqbal*, 556 U.S. at 678).

I. Ambiguity of Policies

In response to both motions to dismiss, OSD's first response is that Hartford and HSB improperly seek to adjudicate the merits of its case rather than challenge the sufficiency of the complaint. True, the purpose of a Rule 12(b)(6) motion to dismiss is to "test[] the sufficiency of the complaint, not the merits of the case," *McReynolds v. Merrill Lynch & Co.*, 694 F.3d 873, 878 (7th Cir. 2012), and the Court must accept all well-pleaded facts as true, *Iqbal*, 556 U.S. at 678. But OSD urges the Court to do more than accept its well-pleaded facts as true. For example, it argues that the Court must accept as true that both contracts are ambiguous because OSD alleges in its complaint that they are ambiguous. But whether a contract is ambiguous is a question of law for the Court to determine. *Kap Holdings v. Mar-Cone Appliance Parts Co.*, 55 F.4th 517, 526 (7th Cir. 2022) (citing *Quake Constr., Inc. v. Am. Airlines, Inc.*, 565 N.E.2d 990, 994 (Ill. 1990)). As it must at the motion to dismiss stage, the Court accepts well-pleaded facts as true but it does not accept the truth of "'a legal conclusion couched as a factual allegation,'" *Twombly*, 550 U.S. at 544 (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)), such as whether

a contract is ambiguous. Thus, OSD's threshold argument is not sufficient to preclude review of Hartford's and HSB's motions to dismiss.

II. Hartford's Motion to Dismiss

In support of its motion to dismiss, Hartford argues that OSD pleads facts that place its claim within the email fraud exclusion in Rider 17, which is a complete bar to recovery. OSD responds that it seeks recovery under Rider 13, not Rider 17; that it is ambiguous whether Rider 17's exclusion applies to coverage provided in Rider 13; and that Rider 13 is self-contained and does not, by its own terms, bar recovery.

"To ascertain the meaning of the policy's language and the parties' intent, the court must construe the policy as a whole." *Ill. Cas. Co. v. W. Dundee China Palace Rest., Inc.*, 49 N.E.3d 420, 424 (Ill. App. Ct. 2015) (citing *Travelers Ins. Co. v. Eljer Mfg., Inc.*, 757 N.E.2d 481 (Ill. 2001); *Outboard Marine Corp. v. Lib. Mut. Ins. Co.*, 607 N.E.2d 1204 (Ill. 1992)). A rider is "an attachment . . . that amends or supplements the document." *Rider*, Black's Law Dictionary (11th ed. 2019). In Illinois, "an insurance contract includes the printed form policy, declarations, and any endorsements, and . . . endorsements do not themselves represent a completely new policy." *Alshwaiyat v. Am. Serv. Ins. Co.*, 986 N.E.2d 182, 191 (Ill. App. Ct. 2013) (internal quotation marks and citations omitted). The *Alshwaiyat* court further noted that endorsements "ha[ve] been defined as being merely an amendment to an insurance policy; a rider." *Id.* (internal quotation marks omitted). In other words, Riders 13 and 17 are not treated as independent insurance policies. Rather, as they each state in large, bold capital letters, the "rider changes the bond." (Hartford Bond at 37, 45.) In other words, where a Rider states that a section of the main Bond is amended to add certain text, that text becomes part and parcel of the Bond and applies as would any original text in the Bond, and it is in construed in relation to the policy as a whole.

The Court begins with Rider 17, which Hartford argues bars any and all coverage under the Bond. Rider 17 states: "***This bond*** does not cover loss resulting directly or indirectly" from a good-faith transfer by OSD "in reliance upon a fraudulent instruction sent to [OSD] through electronic mail, except when covered under the Electronic Mail Initiated Transfer Fraud insuring agreement." (Hartford Bond at 46 (emphasis added).) This language is not ambiguous: if a claim meets the exclusion, coverage is provided only if the Electronic Mail Initiated Transfer Fraud insuring agreement applies. To that end, Hartford argues that the exclusion applies to the Bond as a whole; while OSD contends that the exception only applies to Rider 17 itself.

OSD repeatedly argues that the Riders should be read as walled-off policies that do not interact with the Bond as a whole. For example, it contends that because Rider 13 is "self-contained and not modified at all by the exclusions in any other riders," the Bond is ambiguous and should be construed in its favor and against Hartford. (OSD Hartford Resp. at 9, Dkt. No. 31.) But OSD misunderstands what makes a policy ambiguous. A policy is ambiguous only "if the words in the policy are susceptible to more than one reasonable interpretation," in which case the policy is "construed in favor of the insured and against the insurer who drafted the policy." *Outboard Marine*, 607 N.E.2d at 1212. True, Rider 13 does not expressly state that it is subject to subsequent Riders. But Rider 13 is part of the Bond. *See Alshwaiyat*, 986 N.E.2d at 191. So is Rider 17. *Id.* Both modify the Bond as a whole. OSD offers no reasonable explanation as to why Hartford must spell out, in every section of the Bond, that exclusions added to the Bond apply.

Moreover, Rider 13 ***does*** do what OSD urges should be done. At the end of Rider 13 is the following clause: "The exclusion below, found in Financial Institution Bond for Non-Bank Lenders and Real Estate Investment Trusts and Financial Institution Bond For Investment Firms ***does not apply*** to the Computer Systems Fraud Insuring Agreement," followed by the relevant

non-applicable exclusion. (Hartford Bond at 39 (emphasis added).) OSD offers no explanation as to why a reasonable person would read Rider 13, see that a specific exclusion in the Bond is made inapplicable to Rider 13, and be confused as to whether other exclusions in the Bond apply to Rider 13. Nor is there any explanation as to why, in light of this provision, Rider 17's lack of similar language would be meaningless. Because Rider 17 "modifies insurance provided under . . . Financial Institution Bond For Insurance Companies" (Hartford Bond at 45), without stating that it does not apply to Rider 13, the only reasonable interpretation of Rider 17 is that it—and its exclusions—apply to Rider 13.

It is quite straightforward to identify the section of the Bond to which the e-mail fraud exclusion, and several other exclusions, were added. It is also quite straightforward to identify the section to which Rider 13 added the Computer Systems Fraud coverage. (Hartford Bond at 5, 37.) Neither OSD's tortured reading of the Riders nor its allegations circumvent the Bond's clear text. OSD pleads no facts that support an inference that its loss satisfies the Electronic Mail Initiated Transfer Fraud insuring agreement, in which case the exclusion at issue would not apply. In particular, it does not allege that it verified the fraudulent instruction with "the required password(s), PIN(s), or other security code(s) of such Customer," that it verified the transfer request "via a call-back to a predetermined telephone number set forth in the Insured's written agreement with such Customer," or that it "preserved a contemporaneous record of the call back and of the instruction which verifies use of the authorized password(s), PIN(s) or other security code(s) of the Customer." (Hartford Bond at 45.) On the other hand, it has pleaded facts that fall squarely within Rider 17's exclusion: that the "loss result[ed] directly or indirectly from the Insured having, in good faith, transferred or delivered Funds . . . in reliance upon a fraudulent instruction sent to the Insured through electronic mail." (*Id.* at 46.)

In short, OSD has alleged facts that fall squarely within the unambiguous exception found in Rider 17 and bar coverage. For that reason, Hartford's motion to dismiss is granted. Counts I and II are dismissed.

III. HSB's Motion to Dismiss

Unlike Hartford, HSB has already provided some coverage to OSD for the hack, tendering $250,000 to OSD in May 2022 pursuant to the Cyber Insurance Policy's Social Engineering Coverage. (Compl. ¶¶ 40–41.) But OSD had also sought to invoke the Policy's Computer Fraud Coverage, which claim HSB denied in June 2022. (*Id.* ¶ 43.) HSB reasoned that "the fraud scheme at issue did not meet the definition of Computer Crimes in the HSB Specialty Policy and the subject claim did not directly result from Computer Crimes." (*Id.*)

HSB raises three arguments in support of its motion to dismiss. First, it argues that the loss suffered by OSD did not directly result from a Computer Crime. Second, it argues that the Social Engineering and Computer Fraud coverages are mutually exclusive. And third, it argues that OSD has simply not alleged facts that fall within the Computer Fraud Coverage. The Court considers each in turn.

A. Direct Result of a Computer Crime

HSB's argument centers on the human element involved in this fraud. As OSD alleges, an executive's Outlook account was breached, the account's rules were changed, and emails were sent by bad actors purportedly from the executive. (Compl. ¶ 2.) Deceived by those emails, finance and accounting employees transferred millions of dollars out of Gateway's and Affirmative's accounts and into the hands of the bad actors. HSB urges that the interim step—that humans transferred money in response to emails rather than, for example, a hacker installing code that forced transfers—establishes that OSD has failed to allege facts showing that its loss directly resulted from a Computer Crime as defined in the Policy.

The Policy's Computer Fraud Coverage applies to claims for loss "incurred . . . as a ***direct result*** of Computer Crimes." (HSB Policy at 59 (emphasis added).) The Policy, in turn, defines a Computer Crime as "the intentional, fraudulent, or unauthorized input, destruction, or modification of electronic data or computer instructions into Computer Systems by any entity which is not an Insured Organization or person who is not an Insured Person." (*Id.* at 64.) HSB's argument centers on whether the loss was the direct result of the Computer Crime, even assuming that there was a Computer Crime (which it does not concede).

HSB argues that the loss is the direct result of OSD's employees' actions. In response, OSD points to four out-of-circuit cases for the proposition that other courts have found that social engineering triggered similar computer fraud coverage clauses. In one, for example, Computer Fraud is broadly defined, covering in part "[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property . . . ." *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455, 461 (6th Cir. 2018) (internal quotation marks omitted). On a plain reading, requiring the use of a computer to trigger the coverage appears to cover the same ground as requiring the "input, destruction or modification of electronic data into computer systems." (HSB Policy at 64.) Indeed, it is hard to imagine ways in which one can use a computer that do not involve inputting, destroying, or modifying data.[4]

While the Seventh Circuit has not addressed the issue, several courts have found that "direct loss" does not require that the underlying computer crime (or computer fraud, as some contracts call it) be the sole cause of the loss. In *Ernst & Haas Management Co., Inc. v. Hiscox,*

[4] At least one other court has construed similar language to the Policy quite narrowly. *Cachet Fin. Servs. v. Berkeley Ins. Co.*, Case No. 2:22-cv-01157-SPG-JEM, 2023 WL 2558413 (C.D. Cal. Jan. 20, 2023). But there, the relevant policy covered "loss resulting directly from a ***fraudulent*** [e]ntry . . . or [c]hange of 'electronic data or 'computer program.'" *Id.* at *3. Here, in contrast, "fraudulent" does not modify the Computer Crime definition.

Inc., 23 F.4th 1195 (9th Cir. 2022), a computer fraud provision stated: "The Company will pay the Insured for the Insured's direct loss of, or direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud." *Id.* at 1201 (internal quotation marks omitted). A fraudster had sent an email similar to those sent here, purportedly from an employee's supervisor requesting that she transfer funds, which the employee did. *Id.* at 1197. The Ninth Circuit held that events between the fraud and the loss—namely, the authorization of a transfer of funds pursuant to a fraudulent email—were not intervening events that broke the chain of direct causation. *Id.* at 1201–02. The Ninth Circuit relied on *American Tooling*, which involved a word-for-word identical computer fraud coverage provision. *Am. Tooling*, 895 F.3d at 459. The *American Tooling* court held that loss was directly caused by computer fraud, despite a series of internal actions after receipt of a fraudulent email, because the series of internal actions was "induced by the fraudulent email, which led to the transfer of the money to the impersonator." *Id.* at 463.

HSB contends that finding direct loss here would improperly substitute a proximate cause analysis for a direct loss analysis, "which is a much narrower concept than 'proximately caused loss.'" *RBC Mortg. Co. v. Nat'l Union Fire Ins. Co. of Pittsburgh*, 812 N.E.2d 728, 734–35 (Ill. App. Ct. 2004). But the Illinois Appellate Court in *RBC Mortgage* takes pains to specify that its direct-cause analysis applies only to fidelity bonds,[5] going so far as to disregard arguments that analogized to casualty insurance causation. *Id.* at 735–36, 736 n.4. Indeed, the Seventh Circuit pointed out that "[t]he standard financial-institution bond is a unique insurance instrument with a long and detailed history." *First State Bank of Monticello v. Ohio Cas. Ins. Co.*, 555 F.3d 564,

[5] Fidelity bonds are also called financial institution bonds and bankers blanket bonds. *Universal Mortg. Corp. v. Württembergische Versicherung AG*, 651 F.3d 759, 761 (7th Cir. 2011).

568 (7th Cir. 2009). *First State Bank*, on which HSB also relies, likewise analyzes a fidelity bond. *Id.* at 570 ("Indeed, loss causation has been a sometimes-misunderstood concept in the caselaw interpreting financial-institution bonds."). OSD alleges that the Hartford Bond, but not the HSB Policy, is a financial institution bond. (Compl. ¶¶ 1, 22.)

Beyond the difference in the type of insurance at issue here, the chain of causation is far shorter than in either Illinois case HSB cites. In *RBC Mortgage*, "the language of the bond ma[de] clear that indemnification is restricted to only those losses occurring as [a] 'direct' result of the employee's fraudulent acts." *RBC Mortg.*, 812 N.E.2d at 734–35. There, a loan officer at First City, a bank and loan broker, prepared fraudulent loan packages for himself and—to disguise his fraud—for other borrowers; submitted the packages as a broker to a mortgage company, EMMC; EMMC funded the loans, paid a brokerage fee to First City, and sold the loans to third-party investors. *Id.* at 730. A warranty agreement between First City and EMMC "guaranteed that the loan packages submitted . . . would not contain any untrue statements," and that First City would indemnify any of EMMC's losses caused by untrue statements. *Id.* After discovering the fraud, EMMC sued. *Id.* at 731. RBC, of which First City was a wholly-owned subsidiary, entered into a settlement with EMMC in which RBC paid for EMMC's losses and agreed to indemnify future losses. *Id.* at 731. RBC then sought indemnification from its insurer who refused to pay. The court found that RBC's losses did not flow directly from the fraud: they flowed from the contract RBC had with EMMC, which set out the liability under which RBC suffered any loss. *Id.* at 735. Moreover, RBC suffered no losses until the settlement, which occurred a year and a half after the conduct that set the chain into action. *Id.*

RBC Mortgage's chain of causation involves far more links than here. While there, the fraud kicked off the chain of events, subsequent choices immediately caused the loss. The chain

of causation included First City's no-fraud guarantee; EMMC's review and purchase; EMMC's sale of the packages; RBC's decision to indemnify; and EMMC's decision to sue. Here, a fraudster repeatedly sent emails purporting to be the CFO directing OSD to make payments. OSD made those payments, suffering loss. Further, the Computer Crime occurred simultaneously with (or quite close to) the loss, not a year and a half later. Indeed, this case more closely resembles *First State Bank*, in which the Seventh Circuit found that the loss resulted directly from fraud because a fraudster cashed checks at First State Bank drawn on a frozen and empty account in a different bank, First State Bank disbursed money to him based on that lie, and First State Bank lost money because the account on which the checks were drawn was empty. *First State Bank*, 555 F.3d at 571.

The Court does not find HSB's analogy to *RBC Mortgage* on point. Even narrowly construing the Computer Crime solely as the single act of altering the CFO's Outlook rules, OSD has pleaded facts that show a direct link between the loss and the Computer Crime; in this narrow construction, the Computer Crime enabled a fraudster to send emails to the CFO's subordinates who transferred the money. But it is also a plausible reading of the Policy that each fraudulent email was a Computer Crime. Sending an email requires the input of "electronic data or computer instructions" (HSB Policy at 64), and while not expressly alleged, it is a reasonable inference that OSD's allegation regarding the CFO's altered Outlook rules means that each email, to and from the fraudster, routed through the OSD-owned account. (Compl. ¶ 17.) OSD has alleged that the fraudster was not an Insured Person, a requirement for a Computer Crime to occur. As such, every email sent and received by the fake CFO may fit the definition of a Computer Crime. And funds were transferred as a direct response to those emails. Therefore, OSD has adequately alleged that Computer Crimes directly caused the loss.

B. Mutual Exclusivity

HSB next argues that the Social Engineering coverage—under which it ***did*** indemnify OSD—is mutually exclusive from the Computer Fraud coverage. HSB's argument centers on an amendment to the Policy that bifurcated the Social Engineering coverage into two subsections, (a) and (b). Subsection (a) covers instances in which the Insured Organization receives fraudulent instructions; subsection (b) covers instances in which a financial institution receives the fraudulent instructions. (HSB Policy at 114.) Here, because OSD received the instructions, HSB paid out its claim under subsection (a).

The amendment also defines Fraudulent Instructions and provides an exclusion: "Fraudulent Inducement Instructions covered under Insuring Agreement I.E.1, Social Engineering, part b., does not mean or include Computer Fraud as otherwise covered under Insuring Agreement I.E.2, Computer Fraud." (*Id.*) As HSB points out, courts have read similar language to establish mutually exclusive categories. *See SJ Computs., LLC v. Travelers Cas. & Sur. Co. of Am.*, No. 21-CV-2482 (PJS/JFD), 2022 WL 3348330, at *5 (D. Minn. Aug. 12, 2022) ("[T]he Policy makes abundantly clear that social-engineering fraud and computer fraud are mutually exclusive categories."). And on a plain reading, the Court agrees that the Policy's Computer Fraud coverage is mutually exclusive from Social Engineering coverage under subsection (b). But OSD alleges that its coverage arose under subsection (a), not (b). By specifying that only subsection (b) is mutually exclusive from the Computer Fraud coverage, the HSB Policy indicates that subsection (a) is ***not*** mutually exclusive from the Computer Fraud coverage. And to the extent there is any ambiguity, the Court must construe the policy "in favor of the insured and against the insurer who drafted the policy." *Outboard Marine*, 607 N.E.2d at 1212. As such, for purposes of this motion to dismiss, that OSD recovered under subsection (a)

of the Social Engineering coverage does not, by itself, bar recovery under the Computer Fraud coverage.

C. Pleading Computer Fraud Coverage

Finally, HSB raises a two-part argument that the Computer Fraud coverage does not apply. First, it argues that OSD's loss results from social engineering and nothing more; and second, it argues that OSD simply does not allege either a computer fraud or computer crime. The Court disagrees.

As OSD argues, the colloquial label—or even the title of a Policy section—does not guide whether an act is covered. Rather, the Policy's language guides the inquiry. This means that while one might, in conversation, say that social engineering caused OSD's loss, that does not mean that only Social Engineering Coverage is available to indemnify OSD. And for reasons discussed in relation to HSB's mutual exclusivity argument, nothing in the Policy precludes recovery under both clauses. That an event occurred that plausibly falls within multiple clauses does not, without more, mean that an insured must pick one to the exclusion of others. Instead, the relevant question is whether OSD has alleged facts that plausibly fall within the Computer Fraud coverage. As discussed above, it does.

HSB next argues that the fraudster's alteration of the ex-CFO's Outlook rules and sending of fraudulent emails "does not amount to the requisite input, destruction, or modification of electronic data or computer instructions into computer systems to establish a "Computer Fraud" or "Computer Crimes" loss under the policy." (HSB Br. at 11, Dkt. No. 28.) While it is true that the broader network was not breached, and no server, computer, or other hardware was burglarized or altered, HSB does not explain why such results must occur in order for an act to qualify as "input, destruction, or modification of electronic data or computer instructions." (HSB Policy at 64.) To the contrary, the ordinary meaning of this language would seem to include

altering Outlook rules and sending illicit emails from an account owned by an executive at OSD. Hacking into an account and sending a fraudulent email would seem to qualify as "fraudulent[] or unauthorized . . . input . . . of electronic data." (*Id.*) Likewise, illicitly altering Outlook rules to disguise an ongoing fraud scheme would appear to be the "intentional, fraudulent, or unauthorized . . . modification . . . of computer instructions." (*Id.*)

At most, the Policy is ambiguous as to whether OSD has alleged a Computer Crime that directly caused Computer Fraud because the Policy is subject to more than one reasonable interpretation. *Outboard Marine*, 607 N.E.2d at 1212. "'If the language of an alleged contract is ambiguous regarding the parties' intent, the interpretation of the language is a question of fact which a [] court cannot properly determine on a motion to dismiss.'" *Kap Holdings*, 55 F.4th at 526 (quoting *Quake Constr.*, 565 N.E.2d at 994). Because OSD has alleged facts that could plausibly state a claim for coverage under the Computer Fraud Coverage, HSB's motion to dismiss is denied.

CONCLUSION

Hartford's motion to dismiss Counts I and II (Dkt. No. 21) is granted, and HSB's motion to dismiss Counts III and IV (Dkt. No. 27) is denied.

ENTERED:

Dated: March 31, 2025

Andrea R. Wood
United States District Judge