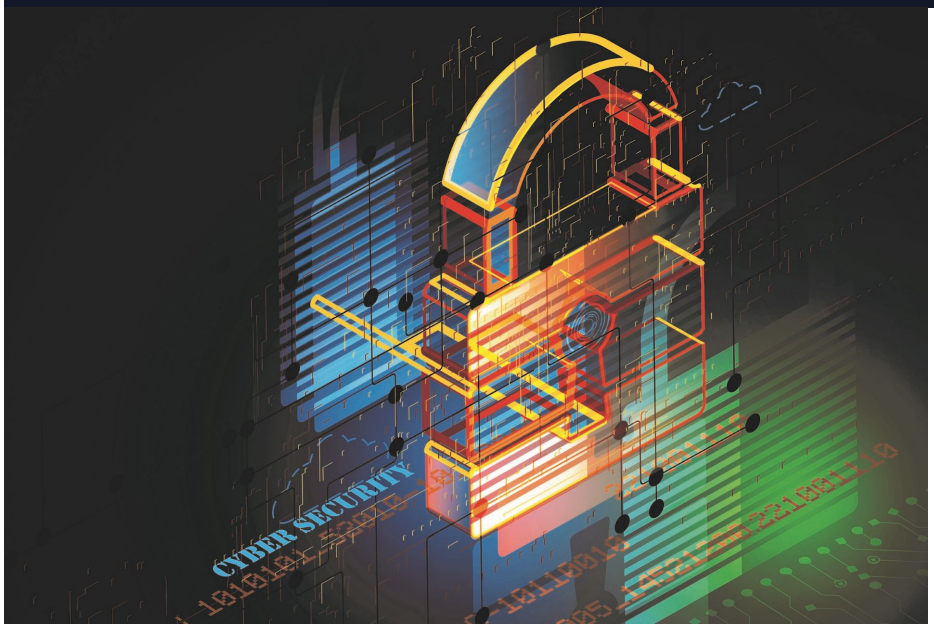
BARNES & THORNBURG LLP



Policyholders Hit With Ransomware Strike Insurance Coverage Oil In Indiana

October 15, 2021 | Policyholder Protection,Cyber Insurance,Insurance

Scott N. Godes
Partner
Data Security and Privacy Co-Chair, Insurance Recovery and Counseling Group Co-Chair

In *G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.*, --- N.E.3d ---, 2021 WL 1034982, 2021 Ind. LEXIS 182 (Ind. Mar. 18, 2021), the Indiana Supreme Court confirmed that "silent cyber" – the insurance industry's term for circumstances when losses due to cyberattacks are covered by policies not marketed as "cyberinsurance" – extends to losses due to ransomware. This article provides an overview of the holding of *G&G Oil* and why it was decided correctly.

The Ransomware Attack on G&G Oil and Its Efforts to Obtain Coverage

In late 2017, as G&G Oil stated in a letter to the insurance carrier, Continental Western Insurance Company ("Continental Western"), "It is our belief that the hijacker hacked into our system via a targeted spear-phishing email with a link that led to a payload downloading to our system and propagating through our entire network…" The spear-phishing email contained "a link that led to a payload downloading to [G&G Oil's] system and propagate[ed] [malware]

RELATED PRACTICE AREAS

Commercial General Liability
Copyright, Trademark, and Media Liability
Credit and Mortgage Insurance
Directors and Officers Liability
Employment Practices Liability
Fidelity Bonds and Commercial Crime Policies
First-Party Property
Insurance Recovery and Counseling
Ocean Marine and Cargo Coverage
Professional Liability
Representations and Warranties
Workers' Compensation and Employers' Liability

RELATED TOPICS

Cyber Insurance
Cybersecurity
Insurance Policy

through [the] entire network. This took place through a user SQL service "that is used for [G&G Oil's] accounting software."

The hackers accessed the network and locked it up so that G&G Oil was unable to use any of its computers. More specifically, on Nov. 17, 2017, "everything" on the computer network "had been encrypted at the hardware level including external hard drives used for backups."

G&G Oil did what many companies do in that situation: it communicated with the hackers in an effort to pay the demanded ransom and get its computers back to normal. The hackers demanded "three (3) bitcoins in order for the passwords to be given to [G&G Oil] to unlock all affected servers and software." That offer was a fraudulent inducement for G&G Oil to pay, because the hackers later demanded even more bitcoin to unlock the network fully.

G&G Oil paid the hacker one initial bitcoin to show its good faith in cooperating with the hackers' demand. The hackers sent multiple passwords in response. The hackers then "stated that [G&G Oil] would have to send the remaining two (2) bitcoin in order to receive all remaining passwords." That statement, however, was false. After G&G Oil sent the final two bitcoin in response to the demand, the hacker sent only some, but not all, of the passwords necessary to unlock the full network. The hacker required G&G Oil to pay another to provide the full set of passwords.

G&G Oil sought coverage from Continental. G&G Oil had purchased a broad-form commercial package policy from Continental Western. The policy included commercial crime coverage. Within the crime coverage part, G&G Oil purchased $100,000 of Computer Fraud coverage, with a $5,000 deductible. Computer Fraud coverage applies to losses "resulting directly from the use of any computer to fraudulently cause a transfer of" money, securities, or other property to someone else or somewhere off of G&G Oil's premises. That Computer Fraud coverage, as found within the commercial crime section of the insurance policy, was written on a form with a 2005 copyright.

The Commercial Crime Coverage section of the Policy provided, in part:

> **Computer Fraud**
>
> We will pay for loss or damage to "money", "securities" and "other property" resulting directly from 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".

Continental denied coverage for the matter. G&G Oil filed suit for breach of contract in Indiana state court. The trial court granted summary judgment to Continental and the Indiana Court of Appeals affirmed. The Indiana Supreme Court granted transfer of the case from the Court of Appeals, and reversed the grant of summary judgment for Continental, remanding for further proceedings.

The Indiana Supreme Court's Holding That Crime Insurance Could Apply to Ransomware Losses is Correct

First, *G&G Oil* affirms important rules of interpretation for insurance policies. Although insurance policies are contracts, the Indiana Supreme Court re-affirmed fundamental principles of insurance policy interpretation. That is, there are "specialized rules of construction in recognition of the frequently unequal bargaining power between insurance companies and insureds"; with one of those rules being that "courts construe ambiguous terms against the policy drafter and in favor of the insured." When "reasonably intelligent policyholders would honestly disagree on the policy language's meaning," the policy language is ambiguous and must be construed against the insurance carrier.

Second, *G&G Oil* found that the phrase "fraudulently cause a transfer" unambiguously can apply to a ransomware situation, explaining that "'fraudulently cause a transfer' can be reasonably understood as simply 'to obtain by trick.'" Although the Indiana Supreme Court stated in *G&G Oil* that not "every ransomware attack is necessarily fraudulent," such as situations in which there were no antivirus "safeguards" that "were put in place" on a network that would allow a hacker to get access without tricking a user first, the court suggested that a ransomware that originated from a spear phishing attack or other way of duping a user into taking action that starts the process of allowing malware to be downloaded would qualify as "fraudulently caus[ing] a transfer." The Indiana Supreme Court remanded for further factual investigation on the question of whether the ransomware ultimately originated from "a targeted spear-phishing email," a point that the court suggested was not undisputed.

Third, *G&G Oil* held "G&G Oil's losses 'resulted directly from the use of a computer.'" The Indiana Supreme Court applied an "immediate[] or proximate[]" cause test, and found that the test was satisfied, even though the "transfer was voluntary," and happened "after consulting with the FBI and other computer tech services."

The Indiana Supreme Court's construction of "resulting directly from the use of a computer" was correct, and it was a positive result for insureds to see the lower court decision overturned on this point. The loss was "resulting directly from" the use of a computer. As certain courts have recognized, "[r]esulting directly from" distinguishes between so-called "first party loss," where the insured loses its own money, and "third party loss," where the insured pays damages to a third party after an event. In *Tooling, Manufacturing & Technologies Association v. Hartford Fire Insurance Co.*, 693 F.3d 665 (6th Cir. 2012), the Sixth Circuit explained that "the Surety Association revised its standard fidelity-contract form to replace the term 'loss resulting through' with 'directly resulting from'. . . to combat court cases that found coverage under fidelity policies" for third-party liabilities, rather than a loss of the insured's own funds. Notably, other decisions have found that Computer Fraud coverage applies to third party liabilities as well, using a proximate cause analysis. Finding that G&G Oil's loss was direct was proper under the *Tooling, Manufacturing & Technologies* or proximate cause analysis, for example, because it was a loss of G&G's own funds that was proximately caused by computer fraud, and was not a payment of damages to satisfy a third-party liability.

In the Indiana Court of Appeals' ruling against coverage, the court relied first on *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America,* 656 F. App'x 332 (9th Cir. 2016), a decision involving a fraud that could have been accomplished without the use of computers. *Pestmaster* was not a solid foundation on which to build Indiana law regarding Computer Fraud

coverage. Separate cases interpreting Computer Fraud coverage have distinguished *Pestmaster*. In each, the courts rejected the insurance companies' assertions that under *Pestmaster*, courts must interpret Computer Fraud coverage as applying only to circumstances in which a hacker caused money to be transferred from one computer to another.

The first was *American Tooling Center, Inc. v. Travelers Casualty & Surety Co.*, 895 F.3d 455 (6th Cir. 2018). In *American Tooling Center*, the policyholder received a phishing email, and, then sent money to the hacker as a result of the message. The U.S. Court of Appeals for the Sixth Circuit held that Computer Fraud covered the funds lost because the insured sent them to the hacker. Coverage was not limited to circumstances, as the insurer argued, "to hacking and similar behaviors in which a nefarious party somehow gains access to and/or control's the insured's computer." The court rejected the insurer's argument that Computer Fraud coverage "require[s] . . . that the fraud 'cause the computer to do anything.'" Rather, the phishing emails and subsequent sending of money to the hacker was sufficient for Computer Fraud coverage to apply. The Sixth Circuit distinguished *Pestmaster*, explaining, in part, that "in *Pestmaster*, everything that occurred using the computer was legitimate and the fraudulent conduct occurred without the use of a computer."

Similarly, in *Medidata Solutions, Inc. v. Federal Insurance Co.*, 268 F.3d 471, 478-79 (S.D.N.Y. 2017), aff'd, 729 F. App'x 117 (2d Cir. 2018), the District Court rejected Pestmaster's narrow interpretation of Computer Fraud, and ruled that a phishing email and subsequent sending of funds satisfied the definition of Computer Fraud. Finally, the District Court in *Cincinnati Insurance Co. v. Norfolk Truck Center, Inc.*, 430 F. Supp. 3d 116 (E.D. Va. 2019) considered whether Computer Fraud coverage applied to circumstances where the policyholder received a phishing email and sent money to the hacker six days later, and rejected the insurer's reliance on *Pestmaster* in arguing against coverage. It recognized that Computer Fraud coverage "does not require a fraudulent payment by computer; rather it requires a computer's use to fraudulently cause a transfer of money." In short, those courts recognize that Computer Fraud "coverage covers loss 'resulting directly from the use of any computer to fraudulently cause a transfer of [money.]' . . . Thus, the cause of the transfer must be fraudulent; however, the payment itself need not be fraudulent."

The Indiana Court of Appeals also cited *Pestmaster* for a public policy-based reason to deny coverage. The Court of Appeals stated a concern that a finding of coverage when a hacker did not transfer funds from one computer to another "would convert this Crime Policy into a 'General Fraud' Policy" on the basis that "computers are used in almost every business transaction." That could be seen as inconsistent with Indiana law, and, beyond Indiana law, could be rejected by other courts. Refusing to apply the plain language of an insurance policy, because of a public policy concern about insurance policies being read too broadly, violates the rule that Indiana courts do "not rewrite an insurance contract" or insert some sort of "'public policy' exception into" the insurance contract.

The Indiana Court of Appeals' decision in *G&G Oil* appears to result in a narrow interpretation of the insurance policy, a result that does not seem consistent with insurance coverage law stating that insurance policies should be interpreted broadly, particularly in light of the fact that insurance companies have the opportunity to narrow the scope of coverage when they write and sell the insurance policies at issue. If Continental had wanted to

narrow the scope of the insurance policy's Computer Fraud coverage to not apply to ransomware losses, then Continental could have written more restrictive policy language, and it could avoid future liability by using such language going forward. As the Indiana Supreme Court explained, updated policy terms, which are more restrictive, are evidence that an insurer could have engaged in "more careful drafting" if the insurer wanted to limit coverage. In *G&G Oil*, the loss took place in 2017, but the disputed insurance policy form dated to 2005. "Although [Continental] could have more clearly defined "[Computer Fraud]" . . ., it failed to do so. [Courts] cannot now re-write the insurance policy" to reflect the arguments of litigation counsel.

The Indiana Court of Appeals also had cited to the trial court decision in *InCOMM Holdings, Inc. v. Great American Insurance Co.*, 2017 WL 1021749 *10 (N.D. Ga. Mar. 16, 2017) for the principle that Computer Fraud coverage requires a "hacking where a computer is caused to cause another computer to make an unauthorized, direct transfer of property or money." In that case, the U.S. Court of Appeals for the Eleventh Circuit, however, had rejected the District Court's decision to "impose[]additional conditions not required by the policy's plain language" – that is, restricting coverage in a way not found in the policy – and determined that there was fraudulent use of computers under Computer Fraud coverage. *Interactive Communications, Int'l, Inc. v. Great Am. Ins. Co.*, 731 F. App'x 929, 930, 931-32 (11th Cir.) (per curiam). The court ultimately denied coverage because there was a four-step process before the insured suffered a loss, and each one of the thousands of transactions led to a "loss [that] was temporally remote: days or weeks – even months or years – could pass between" the original computer fraud and the loss, and because there was a four-step attenuated process before the insured suffered a loss. Id. at 931, 935.

Even if the narrow coverage interpretations in those cases were seen as reasonable, they nonetheless should not have supported a denial of coverage. Under Indiana law, when there is a split in authority, that is evidence of ambiguity in an insurance policy. As detailed above, the decisions on which the Court of Appeals relied have been distinguished, criticized, or rejected. That reflects a split in authority and shows that there is more than one reasonable way to interpret Computer Fraud coverage. Accordingly, the Court of Appeals' reliance on those cases to deny coverage was misplaced.

Fourth, the Indiana Supreme Court was not persuaded by Continental's argument that because G&G Oil did not purchase "computer virus and hacking coverage" under another coverage part of the policy, then G&G Oil could not recover under the disputed coverage part (that G&G Oil had purchased). That's the correct result. It is not uncommon, let alone a bar to coverage, for different lines of insurance to provide overlapping coverage for the same events or the same loss. Indeed, "courts have found that existence of other coverage alone does not 'win the day for [the insurer] if the [contested policy] could be construed to cover the same risks.'"

Overall, this is the right result for insurance policyholders. As computer-based risks have expanded, courts around the country have construed Computer Fraud coverage in a number of contexts, and have determined that Computer Fraud covers a variety of risks; the coverage is not limited to situations in which a hacker uses a computer to transfer funds from one computer to another.

Coverage for a "business email compromise" – losses suffered when an

insured is phished and sends money to hackers as a result – is an on-point example. Multiple courts have held that Computer Fraud coverage applies to business email compromises that started with phishing attacks; they rejected insurers' arguments that Computer Fraud coverage is restricted to instances in which a hacker uses one computer to transfer funds to a second computer, rather than circumstances when the insured affirmatively sends money to the hackers.

Variations of Computer Fraud coverage have been found to cover other cyberattacks. In *Retail Ventures, Inc. v. National Union Fire Insurance Co.*, 691 F.3d 821 (6th Cir. 2012), the court analyzed whether a variation of a crime policy's Computer Fraud coverage ("Computer & Funds Transfer Fraud Coverage") applied to damages owed as a result of a hack of a credit card server. Hackers accessed the policyholder's server and viewed credit card numbers; they did not steal money or transfer it from one computer to the other. The policyholder had a multimillion-dollar liability to its credit card processor for resulting "charge backs, card reissuance, account monitoring, and fines imposed by VISA/MasterCard." The Sixth Circuit recognized that coverage applied, and that the damages owed as a result of the hack "resulted directly" from the computer fraud.

In *E & A Industries, Inc. v. Federal Insurance Company*, No. 49D04-1503-CT-009175, slip op. (Marion Sup. Ct. June 21, 2016) (order granting sum. j.), vacated by settlement, slip op. (Feb. 16, 2017), the court considered whether the crime policy's Computer Fraud coverage applied to losses after "a cyber-attack on [the insured's] computer network, data servers, and individual computers . . . made multiple servers and hard drives inoperable and destroyed unknown quantities of data." The court ruled that "[t]he plain language of Computer Fraud coverage applies, or, alternatively, the language is ambiguous and shall be construed in [the insured's] favor."

These cases demonstrate that Computer Fraud coverage has been interpreted as applying in a variety of circumstances involving some form of fraud via a computer, and that coverage is not limited to situations in which a hacker uses one computer to transfer funds to a second computer.

Conclusion

The Indiana Supreme Court's decision in *G&G Oil* should help policyholders and insureds trying to get coverage for losses due to ransomware attacks; it consists of a thoughtful analysis that reaffirms key principles of insurance policy interpretation. The court refused to apply a narrow reading of the insurance policy, rejected the argument that a failure to buy coverage elsewhere eliminated coverage under the disputed policy part, and engaged in a plain reading of crime insurance to cover ransomware losses.

This article was originally published in the Journal on Emerging Issues in Litigation.

---

[1] Scott Godes and Andy Detherage were counsel to United Policyholders, which submitted an amicus brief in favor of granting transfer and reversing the lower court decision, in the Indiana Supreme Court decision referenced in this article. Messrs. Godes and Detherage are partners in Barnes & Thornburg LLP.

[2] G&G Oil, slip op. at 8.

[3] The hacking "technique known as 'spear phishing'" references a situation

*in which the hacker "sends the targeted individual an email specifically crafted from the information previously gathered to induce that individual to take some action that will lead to the compromise of their computer." Microsoft Corp. v. Does 1-2, No. 117CV01224TSEMSN, 2018 WL 6186826, at *3 (E.D. Va. Oct. 31, 2018) (quoting complaint), report and recommendation adopted sub nom. Microsoft Corp. v. Does, No. 1:17CV1224, 2018 WL 6183279 (E.D. Va. Nov. 27, 2018). "In the phishing emails, there are file attachments or links that lead to malicious executable code." Id. "When the targeted individual clicks on one of these links or opens the files, it causes the malware to be installed on that individual's Windows-based computer." Id.*

[4] Appellant's App. 3:154.

[5] Id.

[6] Id.

[7] See generally id.

[8] Id.

[9] See id. at 3:154-155.

[10] Id. at 3:155.

[11] Id.

[12] See id.

[13] See id.

[14] See id.

[15] See id. at 3:62.

[16] See id.

[17] Id. at 3:67.

[18] See id.

[19] G&G Oil, slip op. at 2-3.

[20] G&G Oil, slip op. at 5.

[21] G&G Oil, slip op. at 6.

[22] G&G Oil, slip op. at 8.

[23] G&G Oil, slip op. at 9.

[24] G&G Oil, slip op. at 9.

[25] G&G Oil, slip op. at 11.

[26] G&G Oil, slip op. at 11.

[27] Id. at 674.

[28] See, e.g., Retail Ventures, Inc. v. National Union Fire Insurance Co., 691 F.3d 821 (6th Cir. 2012).

[29] Specific to Indiana law, over 40 years ago, the Court of Appeals has held "direct" to be ambiguous in the context of what consists of "direct loss" in an insurance policy. See Farmers Mut. Aid Ass'n. v. Williams, 386 N.E.2d 950,

952 (Ind. Ct. App. 1979).

*[30] In Pestmaster, the policyholder made legitimate payments to its vendor, so that the vendor could pay Pestmaster's taxes for it. Pestmaster, 2014 WL 3844627, at *1-2 (C.D. Cal. July 17, 2014), aff'd in part and vacated in part, 656 F. App'x 332, 333 (9th Cir. 2016). After Pestmaster wired money for authorized legitimate transactions, the vendor failed to make tax payments for Pestmaster, and kept the money instead. Id. The vendor's "fraudulent conduct" was when it misused funds that it obtained by legitimate means, and was not dependent on the use of a computer to complete the scheme. Id. at *7. Thus, the fraud in Pestmaster could have happened without a computer – the vendor could have misused money deposited by checks – so it is of no moment that the courts refuse to read Computer Fraud coverage as applying. Here, by contrast, the ransomware only works when computers are involved and the user was tricked into downloading malware to let the ransomware take over the network.*

[31] The Indiana Supreme Court found this case to be "distinguishable-though factually similar" to G&G Oil. G&G Oil, slip op. at 8. There was no explanation given as to why the case was "distinguishable."

*[32] "Phishing 'is a method of . . . using deceptive e-mails . . .' to 'trick an e-mail recipient into believing that the message is something they want or need from a legitimate or trustworthy source and to subsequently click on [a] link or download an attachment.'" Jantzer v. Elizabethtown Cmty. Hosp., No. 819CV00791BKSDJS, 2020 WL 2404764, at *1 (N.D.N.Y. May 12, 2020) (quoting complaint in motion to dismiss). After the user clicks on the fraudulent link, "'the credentials are then used to gain unauthorized access into a system.'" Id.*

[33] Id. at 462.

[34] Id.

[35] See id. at 463; see also Ubiquiti Networks v. Nat'l Union Fire Ins. Co., No. 18CV322879, slip op. at 7 (Cal. Super. Ct. July 30, 2018) (rejecting insurer's argument that "courts have consistently interpreted this language as covering losses occurring when a 'scheming third-party hacker [breaks] into the computer to directly cause the transfer via the computer'").

[36] 895 F.3d at 461.

[37] Id. at 131.

[38] Id. at 131 n. 11 (emphasis in original).

[39] Slip op. at 10.

[40] Keckler v. Meridian Sec. Ins. Co., 967 N.E.2d 18, 28 (Ind. Ct. App. 2012) (quoting Bowen v. Monroe Guar. Ins. Co., 758 N.E.2d 976, 980 (Ind. Ct. App. 2001)).

[41] State Mut. Ins. Co. v. Flexdar, Inc., 964 N.E.2d 845, 852 (Ind. 2012).

[42] Appellant's App. 3:67, 3:154.

[43] Michigan Mut. Ins. Co. v. Combs, 446 N.E.2d 1001, 1007 (Ind. Ct. App. 1983).

[44] G&G Oil, Court of Appeals slip op. at 10-11.

[45] The policyholder changed its name by the time of the appeal.

[46] The Eleventh Circuit's unpublished holding in Interactive Communications (sub nom. as InComm) has been distinguished in the context of other Computer Fraud cases when there was not such an attenuated chain of events as there was in InComm. See Am. Tooling, 895 F.3d at 462-63 (noting that losses from phishing attack were more direct than the four steps before loss in InComm); accord Norfolk Truck, 430 F. Supp. 3d at 126-27, 130-31 (declining to follow InComm). In fact, in the published decision of Principle Solutions Group, LLC v. Ironshore Indemnity, Inc., 944 F.3d 886 (11th Cir. 2019), a decision regarding crime insurance for a business email compromise, the Eleventh Circuit did not even mention IncComm's analysis for direct loss.

[47] Under Indiana law, when there is a split in authority, that is evidence of ambiguity in an insurance policy. See, e.g., Travelers Indem. Co. v. Summit Corp. of Am., 715 N.E.2d 926, 938 (Ind. Ct. App. 1999) ("This disagreement among the courts further indicates the ambiguity of the personal injury provisions.").

[48] See Am. Tooling, 895 F.3d at 462; Medidata, 268 F.3d at 478-79; Norfolk Truck, 430 F. Supp. 3d at 131

[49] G&G Oil, slip op. at 6.

[50] See, e.g., Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 801-02, 804-05 (8th Cir. 2010) (holding that the underlying plaintiff's claim was covered under two different insurance policies).

[51] Capital Environ. Serv., Inc. v. N. River Ins. Co., 536 F. Supp. 2d 633, 644 (E.D. Va. 2008) (quoting Prisco Serena Sturm Architects, Ltd. v. Liberty Mut. Ins. Co., 126 F.3d 886, 893 (7th Cir. 1997)).

[52] The F.B.I. defines a business email compromise as follows: "criminals send an email message that appears to come from a known source making a legitimate request" https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise. Like here, a business email compromise starts with a "phishing scheme," "persuading an employee to" take action (often to wire money to the hacker). See, e.g., Principle Solutions Group, LLC v. Ironshore Indemnity, Inc., 944 F.3d 886, 888 (11th Cir. 2019).

[53] See Am. Tooling, 895 F.3d at 462 (6th Cir. 2018) (computer fraud coverage applied to losses resulting from a phishing attack when the policyholder later sent the hacker money and rejecting argument that Computer Fraud coverage applies only to hacking and when a hacker "somehow gains access to and/or controls the insured's computer"); Medidata, 268 F.3d at 478-79, aff'd, 729 F. App'x 117 (2d Cir. 2018) (same); Norfolk Truck, 430 F. Supp. 3d at 130-31 (same); see also Ubiquiti, slip op. (denying insurer's demurrer and finding that Computer Fraud coverage could apply to business email compromise losses after an initial phishing email).

[54] See id. at 824.

[55] Id. at 824-25.

[56] See id. at 827-28, 831-32.

[57] Slip op. at 2.

[58] Slip op. at 12.