MANIER & HEROD

Social Engineering in the Age of Social Distancing – Recent Developments in Computer Crime Coverage

Since the onset of "computer crime" claims, a primary frustration for both insurers and fidelity practitioners has been inconsistent rulings from courts. Depending upon the jurisdiction, claims involving similar – if not virtually identical – facts and policy language have resulted in conflicting outcomes. As a result, there remains uncertainty as to what is and is not covered. The most recent rulings have done little to clarify the issue, and few "common themes" have been established.

After a number of inconsistent rulings from lower courts, the fidelity industry was hopeful that the Fifth Circuit's holding in *Apache Corp. v. Great American Ins. Co.*,[1] would conclusively establish that traditional social engineering schemes (also known as Business Email Compromise schemes, or BEC schemes) do not trigger coverage under a traditional "computer fraud" insuring agreement.[2] This hope was bolstered by the opinion in *InComm v. Great American Ins. Co.*,[3] which did not involve an email scam but nevertheless held that a computer crime loss did not result "directly" from the use of a computer. However, following *Apache* and *InComm* two other federal circuit court of appeals reached contrary conclusions under similar, but albeit not identical, facts.

[1] 662 Fed. App'x 252 (5th Cir. 2016) (applying Texas law).

[2] A common "computer fraud" insuring agreement states:

> We will pay for loss of, and loss from 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.

[3] 731 Fed. App'x 929 (11th Cir. 2018) (applying Georgia law).

In *Medidata Solutions, Inc. v. Federal Ins. Co.*,[4] the Second Circuit affirmed summary judgment for an insured that was tricked into wiring funds after receiving emails purporting to be from the insured's president. In *American Tooling Centers, Inc. v. Travelers Cas. & Sur. Co. of America*,[5] the Sixth Circuit rejected the insurer's assertion that "computer fraud" requires a "hack" or breach of the insured's system, and held that a BEC scam implicated coverage.

At this point, it was clear there was no "majority rule" or clear distinction between what is and is not covered. There was no "common theme" developing in the courts. The picture became cloudier when the Eleventh Circuit, in *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*,[6] ruled that an email scam was covered by the crime policy's "fraudulent instruction" insuring agreement. In what may be the perfect epitome of these inconsistent rulings, *InComm* and *Principle Solutions* were decided seven (7) months apart, by the same court, both applying Georgia law, and reached different conclusions. Shockingly, the *Principle Solutions* case does not address or cite to *InComm*, much less distinguish it.

Keeping with this theme, four (4) recent opinions from U.S. district courts reached different conclusions, further muddying the waters as to what is and is not covered. Addressing these cases chronologically, in *Tidewater Holdings, Inc. v. Westchester Fire Ins. Co.*,[7] the insured fell victim to a BEC scam when an accounts payable clerk received a fraudulent email instructing her to change the payment details for one of the insured's general contractors. Four (4) subsequent payments intended for the general contractor were transmitted to the wrongdoers' account. Upon

[4] 729 Fed. App'x 117 (2nd Cir. 2018) (applying New York law).
[5] 895 F.3d 455 (6th Cir. 2018) (applying Michigan law).
[6] 944 F.3d 886 (11th Cir. 2019) (applying Georgia law)
[7] 389 F. Supp. 3d 920 (W.D. Wash. 2019).

receipt of the claim, the insurer acknowledged coverage under a "supplemental funds transfer" insuring agreement that was substantially similar to a traditional "social engineering fraud" insuring agreement. However, the "supplemental funds transfer" insuring agreement had a lower limit of liability than the "computer fraud" insuring agreement, and the insured refused to accept the insurer's payment.

After the insured filed suit, the district court granted the insurer's motion to dismiss. The policy contained an exclusion essentially stating that any loss covered by the "supplemental funds transfer" insuring agreement was excluded under the "computer fraud" insuring agreement. The court correctly held that a social engineering fraud loss was properly analyzed under the "supplemental funds transfer" insuring agreement, and refused to extend the "computer fraud" insuring agreement to email scams that did not involve a hack or breach.

Following *Tidewater Holdings*, in *Sanderina LLC v. Great American Ins. Co.*,[8] the insurer was awarded summary judgment when the insured was tricked (via email) into transferring funds to fraudsters. Notably, the insuring clause differed from the traditional "computer fraud" language, providing coverage for loss:

> [R]esulting directly from the use of any computer to impersonate you, or your authorized officer or employee, <u>to gain direct access to your computer system</u>, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money …."[9]

This "gain direct access to" language emphasizes that a fraudulent email scam is not intended to be covered, and may have been implemented in response to the inconsistent rulings discussed

[8] 2019 WL 4307854 (D. Nev. Sept. 11, 2019).
[9] *Id*. (emphasis added).

above. In *Sanderina*, the insured was unable to conclusively establish that its system was accessed by the fraudster, which precluded a finding of coverage. The insured argued there was a "'high likelihood' that the perpetrator may have accessed Sanderina's computer system to 'case the joint' because the emails were signed "Vic" and sent during the CEO's vacation."[10] The court held that this speculation, while plausible, was insufficient to establish "direct access to your computer system," and ruled in favor of the insurer.

The case of *Miss. Silicon Holdings LLC v. Axis Ins. Co.*[11] is similar to *Tidewater Holdings* in that the district court held that an email scam was covered by the "social engineering fraud" insuring agreement (which was subject to a $100,000 limit of liability), but not the "computer transfer fraud" insuring agreement (which was subject to a $1 million limit of liability). The court adopted a "direct means direct" approach to causation, holding that the fraudulent email(s) – while "set[ting] in motion a series of events which ultimately led to the loss" – did not directly cause the transfer of funds.[12] The district court was also persuaded by the "computer transfer fraud" insuring agreement requiring the transfer be made "without the Insured Entity's knowledge or consent."[13] It was undisputed that several of the insured's employees had knowledge of, and were involved in effectuating, the transfer(s) (even if they were tricked into effectuating the transfers).

Following three (3) decisions favorable for insurers, in *Cincinnati Ins. Co. v. Norfolk Truck Center, Inc.*[14] the district court held that an email scam (that did not involve a hack or breach)

[10] *Id*. at *3.
[11] 2020 WL 869974 (N.D. Miss. Feb. 21, 2020) (currently on appeal).
[12] *Id*. at *5.
[13] *Id*. at *6-7.
[14] 2019 WL 6977408 (E.D. Va. Dec. 20, 2019).

implicated coverage under a traditional "computer fraud" provision. The parties stipulated to all facts and stipulated that the sole issue for the court to decide was the proper interpretation of "direct loss." The court disagreed with the holding in *Apache* and held that the loss resulted "directly" from the use of a computer, even if the fraudulent emails only set in a motion a series of events that ultimately resulted in a loss.[15]

Most recently, the case of *G&G Oil Co. v. Cont'l W. Ins. Co.*[16] involved the unusual circumstances of an insured seeking coverage for a ransomware attack under a traditional "computer fraud" insuring agreement. The court correctly affirmed summary judgment for the insurer, as loss associated with ransomware attacks should be analyzed under a cyber policy or other product specifically designed to address such loss. The Indiana Court of Appeals held that the "computer fraud" insuring agreement required an unauthorized transfer of the insured's funds, as opposed to an authorized transfer even if procured by fraud. The court held:

> Here, the hijacker did not use a computer to fraudulently cause G&G to purchase Bitcoin to pay as ransom. The hijacker did not pervert the truth or engage in deception in order to induce G&G to purchase the Bitcoin. Although the hijacker's actions were illegal, there was no deception involved in the hijacker's demands for ransom in exchange for restoring G&G's access to its computers. For all of these reasons, we conclude that the ransomware attack is not covered under the policy's computer fraud provision.[17]

This is not intended to be an exhaustive discussion of recent developments in the world of "computer crime" under fidelity policies. Practitioners and insurers are also reminded to carefully analyze the policy language, as certain cases (favorable or unfavorable) may be distinguishable

[15] *Id*. at *12-13
[16] 2020 WL 1528095 (Ind. Ct. App. Mar. 31, 2020).
[17] *Id*. at *4.

based upon the underlying facts and the specific insuring agreement. A jurisdiction's interpretation of "direct loss" also has a significant bearing on whether coverage is implicated. These cases emphasize an ongoing theme that courts disagree on how insuring agreements should be interpreted and whether computer crime claims are covered.

REQUIRED DISCLAIMER

This guidance is for general, educational purposes and not intended to be legal advice. Seek separate legal advice on your specific question. The legal analysis of your specific question depends on facts which might alter, or completely change, what you read above. Please contact Jeffrey Price or Justin Wear with any questions. Manier & Herod is ready to serve you while respecting and protecting your health and safety.