Questions Remain On Computer Fraud Coverage For Phishing

By **Robert Callahan and Melissa D'Alelio** (August 26, 2022)

Robert Callahan

Melissa D'Alelio

Businesses are increasingly vulnerable to social engineering schemes, also known as email spoofing or phishing schemes.

Phishing schemes involve fraudulent attempts to obtain sensitive information and/or solicit payments from unsuspecting businesses, often using emails appearing identical to a trustworthy source to trick the victim into affirmatively revealing sensitive information or authorizing payment.

A phishing scheme is distinct from hacking, which involves a forceful intrusion of another's computer system to obtain sensitive information or direct payments without the victim's assistance.

In recent years, federal and state courts have wrestled over whether computer fraud coverage found in property insurance policies provide coverage for phishing scheme losses.

A common computer fraud coverage form provides, "[w]e will pay for loss ... resulting directly from ... 'Computer Fraud,'" and defines computer fraud as "'theft' of property following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside the 'premises' or 'banking premises' to a person ... outside those 'premises' or to a place outside those 'premises.'"[1]

While the purpose of this form was to cover losses resulting from hacking, businesses continue to seek coverage under the same form for phishing scheme losses.[2]

Against a backdrop of recent diverging case results and evolving fact patterns, questions regarding the applicability of computer fraud coverage to phishing scheme losses remain.[3]

Ernst & Haas: Muddying the Waters

On Jan. 26, policyholders celebrated the decision in Ernst & Haas Management Company Inc.. v. Hiscox Inc.,[4] where a U.S. Court of Appeals for the Ninth Circuit panel found computer fraud coverage in the context of a phishing scheme.

The panel departed from unpublished Ninth Circuit precedent established by two other panels — Pestmaster Services Inc. v. Travelers Casualty & Surety Company of America in 2016, and Taylor and Lieberman v. Federal Insurance Company in 2017 — that construed computer fraud coverage as limited to unauthorized computer use, such as hacking.[5]

Although the Ernst & Haas panel ordered its decision for publication, the fact remains that two other Ninth Circuit panels found in favor of insurers in similar contexts suggesting that computer fraud coverage cases involving phishing schemes will continue to have divergent outcomes even within the same jurisdiction.

Rather than clarifying the law on computer fraud coverage in the context of phishing schemes, the Ernst & Haas decision muddied the waters further.

Federal Court Decisions: Oceans Apart

While early computer fraud coverage cases involving phishing schemes hinted at cross-jurisdictional uniformity,[6] courts have now settled into two camps based largely on whether they believe a sufficient causal nexus exists between fraudulent instructions and the losses initiated by victims following those instructions.

In other words, courts disagree on whether phishing schemes, which require an affirmative act by the victim, qualify as computer fraud given the typical threshold conditions that computer fraud losses result directly from computer fraud, are directly related to the use of any computer and the use of any computer fraudulently caused a transfer.

In Ernst & Haas, the Ninth Circuit panel held that the victim's initiation of wire transfers to the fraudster was not an intervening event that severed causation between the fraudulent instructions and loss.[7]

The Ninth Circuit panel concluded that the loss resulted directly from the computer fraud where a victim's initiation of wire transfers was pursuant to fraudulent instructions.[8]

However, the U.S. Court of Appeals for the Fifth Circuit in Apache Corp. v. Great American Insurance Company cautioned against this interpretation in 2016, noting that construing computer fraud coverage provisions "to cover all transfers that involve both a computer and fraud at some point in the transaction" would convert such provisions into a "general fraud policy" — a point previously made the same year by a Ninth Circuit panel in Pestmaster Services Inc. v. Travelers Casualty & Surety Company of America.[9]

Other courts continue to follow the Fifth Circuit's Apache analysis, including the U.S. District Court for the District of New Jersey in the 2019 Children's Place Inc. v. Great American Insurance Company decision.[10]

In construing a computer fraud coverage provision requiring, among other conditions, the use of any computer to gain access to the policyholder's computer system, the Children's Place court noted Apache's warning that interpreting computer fraud coverage broadly would "effectively, convert it into a general fraud provision because 'few — if any — fraudulent schemes would not involve some form of computer-facilitated communication.'"[11]

The policyholder appealed the district court's decision, but dismissed its appeal on April 25. The dismissal deprived the U.S. Court of Appeals for the Third Circuit of an opportunity to join the evolving discourse by issuing its own decision on whether computer fraud coverage encompasses phishing scheme losses.

Westlake Chemical: A Different Fact Pattern

State courts are simultaneously evaluating whether phishing losses are covered by computer fraud coverage. For example, the appeal in Westlake Chemical Corporation v. Berkley Regional Insurance Company is pending before the Texas Court of Appeals for the First District.[12]

In Westlake Chemical, the policyholder sought computer fraud coverage after it paid fraudulent invoices to a shipping bag vendor it knew and trusted.

The fraudster established a trusting relationship by entertaining the policyholder's

employees with dinners and excursions for several years.

The fraudster exploited that trust by submitting fraudulent invoices by email for shipping bags he never delivered. The policyholder's losses exceeded $16 million before it discovered the scheme.

The fact that the policyholder knew and trusted the fraudster distinguishes this case from a typical phishing scheme where the unknown fraudster relies on impersonation.

Nonetheless, the Texas intermediate appellate court will consider whether computer fraud coverage exists given the victim's reliance on fraudulent email instructions to authorize payments.

The case is also interesting in that the court will apply Texas law against the backdrop of the Fifth Circuit's Apache decision, which also applied Texas law.[13] The parties are currently engaged in briefing and no oral argument has been scheduled as of this writing.

The Voluntary Parting Exclusion

Another important question left in the wake of Ernst & Haas is whether the panel would have reached a different result had it construed a policy with a voluntary parting exclusion.

Generally, voluntary parting exclusions preclude coverage for losses where the policyholder voluntarily parts with property if induced to do so by a fraudulent scheme, trick, device or false pretense. U.S. district courts across the nation have applied voluntary parting exclusions to bar computer fraud coverage for social engineering losses.[14]

In Ernst & Haas, the parties disputed whether a 2012 policy without a voluntary parting exclusion or a 2019 policy with a voluntary parting exclusion controlled.

The district court in Ernst & Haas avoided the question by finding that the policyholder did not establish coverage as a threshold matter under the 2012 policy it alleged controlled.

On appeal, the Ninth Circuit panel construed the 2012 policy only and left the district court to consider the 2019 policy — with its attendant voluntary parting exclusion — further on remand. However, on May 25, the parties filed a stipulation to voluntarily dismiss the case before the district court commenced further substantive proceedings.

Uncharted Waters for Computer Fraud Coverage

While policyholders initially heralded Ernst & Haas as a sea change in how courts view computer fraud coverage for phishing losses, the reality is other jurisdictions are finding no computer fraud coverage for such losses.

It also remains to be seen whether other federal and state appellate courts will follow Ernst & Haas's reasoning or heed Apache's warning about converting computer fraud coverage provisions into general fraud policies.

Eventually, a federal appellate court will address how voluntary parting exclusions apply to phishing scheme losses. With these outstanding questions, much remains to be clarified after Ernst & Haas.

Robert F. Callahan, Jr. is an associate and Melissa M. D'Alelio is a partner at Robins Kaplan LLP.

[1] See, e.g., 4 ISO CR 00 07 (10 90) (Form F).

[2] See Melissa D'Alelio, One Phish, Two Phish: Developments in the World of Computer Fraud Coverage, The Brief, Spring 2019 at 19 (citing Ins. Inst. of Am., Fidelity Bonds 179 (1992); IRMI, Computer Fraud Coverage Form 1/1 (2016)).

[3] While the scope of this article concerns cases involving claims under the Computer Fraud Coverage Form (Form F) and similar coverage language, some policies include specific social engineering coverage provisions under which insureds have sought coverage for phishing schemes. See, e.g., SJ Computers, LLC v. Travelers Casualty Surety Company of America, No. 21-CV-2482 (PJS/JFD), 2022 WL 3348330 (D. Minn. Aug. 12, 2022).

[4] Ernst and Haas Management Company, Inc. v. Hiscox, Inc., 23 F.4th 1195 (9th Cir. 2022).

[5] See Taylor and Lieberman v. Federal Insurance Company, 681 Fed. App'x. 627 (9th Cir. Mar. 9, 2017); Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America, 656 Fed. App'x. 332 (9th Cir. July 29, 2016).

[6] See Melissa D'Alelio, One Phish, Two Phish: Developments in the World of Computer Fraud Coverage, The Brief, Spring 2019 at 18-23.

[7] See Ernst and Haas, 23 F.4th at 1202.

[8] Id.

[9] See Apache Corp. v. Great American Insurance Co., 662 Fed. App'x. 252, 256-57 (5th Cir. Oct. 18, 2016) (quoting Pestmaster Services, 656 Fed. App'x 332, at *1).

[10] Children's Place, Inc. v. Great American Insurance Company, No. 18-11963 (ES) (JSA), 2021 WL 6932533 (D.N.J. Sept. 28, 2021).

[11] Id. (quoting Apache, 662 Fed. App'x. at 258).

[12] Westlake Chemical Corporation v. Berkley Regional Insurance Company, No. 01-21-00225-CV (Tex. App.).

[13] Even if the Court of Appeals of Texas rejects Apache, the Fifth Circuit's later decision in Mississippi Silicon Holdings, L.L.C. v. Axis Ins. Co., 843 Fed. App'x. 581 (5th Cir. Feb. 4, 2021), which found no coverage for phishing scheme losses under Mississippi law, suggests that the Fifth Circuit will continue to construe computer fraud coverage provisions narrowly.

[14] See, e.g., Midlothian Enterprises, Inc. v. Owners Ins. Co., 439 F. Supp. 3d 737 (E.D. Va. 2020), Schweet Linde & Coulson, PLLC v. Travelers Cas. Ins. Co. of Am., No. C14-

1883RSL, 2015 WL 3447242 (W.D. Wash. May 28, 2015), Schmidt v. Travelers Indem. Co. of Am., 101 F.Supp.3d 768 (S.D. Ohio 2015); Martin, Shudt, Wallace, DiLorenzo & Johnson v. Travelers Indem. Co. of Conn., No. 1:13-CV-0498 (LEK/CFH), 2014 WL 460045 (N.D.N.Y. Feb. 5, 2014).