INSURANCE COVERAGE FOR "PHISHING" LOSSES—MAKE SURE YOUR "NET" IS ADEQUATE BEFORE YOU GET CAUGHT*

February 2018

by Lisa M. Campisi
Blank Rome, LLP

Introduction

Lawyers and their clients alike have all heard about, and some are painfully familiar with, horror stories regarding losses resulting from so-called "phishing" or "social engineering" schemes. Broadly described, these schemes involve criminals using fraudulent emails, phone calls, copycat websites, or other deceptive communications to trick unwitting companies into sharing valuable personal or financial information, or into wiring money to sham bank accounts.[1] The scammers lure their targets into a false sense of security by spoofing trusted company logos or legitimate employee email addresses.

As these schemes become more common, clients may derive some comfort from having purchased both "cyber" and "computer fraud" coverage, believing that such policies most certainly protect and cover for such losses. Unfortunately, this comfort is often misplaced. While assuming that coverage exists for such "electronic" losses may seem reasonable, when it comes

*This article was originally presented at the 26th Annual Insurance Coverage Litigation Committee Mid-Year Meeting, Phoenix, Arizona (February 2018). It is reprinted here with permission of the American Bar Association Tort Trial and Insurance Practice Section.

[1] *See, e.g.,* https://www.consumer.ftc.gov/articles/0003-phishing (Federal Trade Commission).

to providing coverage under "off-the-shelf" cyber and computer fraud policies, insurance companies do not always see it that way, as shown by the emerging case law. Recent cases demonstrate that policyholders should carefully review their cyber and crime policies, and where needed, seek to negotiate more expansive, and express, coverage if possible. Insurance practitioners should also keep their eyes on key appellate decisions anticipated in 2018, including *Medidata Solutions Inc. v. Federal Insurance Co.,* in the U.S. Court of Appeals for the Second Circuit, and *American Tooling Center v. Travelers Casualty & Surety Co.,* in the U.S. Court of Appeals for the Sixth Circuit, which both involve computer fraud coverage under crime policies.

Insurance Law Essentials Deep Dives is published in association with *Insurance Law Essentials.* For subscription questions or problems, contact IRMI customer service at (800) 827–4242.

Published by IRMI:
International Risk Management Institute, Inc.
Jack P. Gibson, Publisher
Bonnie Rogers, IRMI Editor
12222 Merit Drive, Suite 1600
Dallas, TX 75251 • (972) 960–7693
www.IRMI.com

Medidata—Theft of an Insured's Own Funds From Phishing Covered

In cases involving losses to an insured's own funds due to "phishing," a key issue is whether coverage exists when the thief does not "hack" into the insured's computer system, but rather "spoofs" an email causing the insured to incur the loss. In the recent case of *Medidata Solutions, Inc. v. Federal Insurance Company,* 268 F. Supp. 3d 471 (S.D.N.Y. 2017) (appeal pending), the Southern District of New York agreed with the insured, finding coverage for such a phishing scam.

In *Medidata,* through a series of spoofed emails in 2014, in which a thief sent emails that appeared to be from the president of the insured company Medidata, the thief obtained a $4.8 million wire transfer from Medidata's bank account. *See id.,* 268 F. Supp. 3d at 473–74. Medidata's email addresses contained the domain name "mdsol.com," but the emails were routed through Google servers. Upon receiving an incoming email and identifying the sender's address as belonging to a Medidata employee, Google would automatically display the sender's name, email address, and picture in the "From" field as part of the message. *Id.* at 472. Apparently aware of this arrangement, the thief composed the emails outside of the company's email system and embedded a computer code to have Google incorrectly identify and display the email address as belonging to a Medidata employee. *Id.* at 476.

Medidata sought coverage under a $5 million insurance policy with Federal Insurance Company ("Federal") containing a "Crime Coverage Section" addressing loss for various criminal acts including Computer Fraud, Forgery, and Funds Transfer Fraud. The policy's Computer Fraud coverage protected the:

> … direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party.

Id. at 474.

"Computer Fraud" was in turn defined as:

> … the fraudulent: (a) entry of Data into or deletion of Data from a Computer System" [or] (b) change to Data elements or program logic of a Computer System … directed against an Organization.

Id. at 474, 476.

In arguing against coverage, Federal contended that the thief did not obtain access to Medidata's computer system, as required by the Computer Fraud provision, because the thief simply submitted messages containing fraudulent content from emails prepared outside Medidata's system. The court disagreed, finding that that the policy did not go so far as to require that a thief hack into a company's computer system and execute a bank transfer on their own in order to trigger insurance coverage. *Id.* at 477. The court thus held that because a thief fraudulently "entered" and changed data in Medidata's computer system by altering the "From" field of the spoofed emails, Medidata was covered for Computer Fraud.

As of this writing, the *Medidata* case is on appeal before the Second Circuit, with briefing complete and oral argument requested.

American Tooling—Theft of an Insured's Own Funds From Phishing Not Covered

Unlike the court in *Medidata,* other courts have found that computer fraud coverage does not cover thefts of an insured's own funds resulting from phishing. *American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America,* 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017) is a recent example of such reasoning. In *American Tooling,* the insured ("ATC") received fraudulent emails that spoofed the email address of one of the insured's trusted vendors. In response to those fraudulent emails the insured authorized payments to a bank account it believed belonged to the vendor, but in reality belonged to the fraudster. *American Tooling* at *1. The insurer denied ATC's claim for coverage under the "computer fraud" provision of its insurance policy, asserting that the insured did not incur a covered loss under the policy. *Id.*

On cross motions for summary judgment, the district court upheld the insurer's denial of coverage. In reaching its conclusion, the court noted that the fraudulent email pretending to be from the insured's vendor asked the insured to send payment to a new bank account, but that the insured only verified certain production milestones and did not verify the vendor's supposed "new" bank account information. *Id.* at *1, *2. The court found that because of these "intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds, it cannot be said that ATC suffered a 'direct' loss 'directly caused' by the use of any computer." *Id.* at *2. The court also found that "*Medidata* is distinguishable because the insurance policy [in *Medidata*] does not include the language at issue here, which requires the 'direct loss' to be 'directly caused by Computer Fraud.'" *Id.* at *2 n.1.

In reaching its conclusion that for a loss to be "direct" there cannot be any "intervening events," the *American Tooling* court pointed to Sixth Circuit precedent finding that under Michigan law "direct" is to be "defined as 'immediate,' without anything intervening." *Id.* at *2 (citing *Tooling, Manufacturing & Technologies Ass'n v. Hartford Fire Ins. Co.,* 693 F.3d 665, 673 (6th Cir. 2012)). Relying on this precedent, the *American Tooling* court held that "intervening events between ATC's receipt of the fraudulent emails and the transfer of funds (ATC verified production milestones, authorized the transfers, and initiated the transfers without verifying bank account information) preclude a finding of 'direct' loss 'directly caused' by the use of any computer." *Id.*

It is important to note that the *American Tooling* court overlooked that the precedent upon which it relied to construe the term "direct" to mean "immediate" dealt with a policyholder seeking coverage not for its own losses, but for losses incurred by a third-party. *See Tooling, Mfg. & Techs. Ass'n,* 693 F.3d 665 at 673 (no coverage where policyholder incurred liability to third party entity from which policyholder's employee stole funds). In *American Tooling,* however, there was no question that the insured, and not a third party, suffered the loss. Nor was there any question that but for the email scheme, the policyholder would not have wired the funds and suffered that loss. By applying the reasoning of cases addressing coverage for third party losses under first party policies to a true first party loss, the *American Tooling* case suggests that, even where a loss is suffered directly by the insured, coverage will depend on a specific temporal proximity or immediacy between that loss and the theft.

Not surprisingly, the insurer in *Medidata* has now relied on the *American Tooling* decision to argue that the insured did not suffer a direct loss because of the remote intervening events occurring between the fraudulent emails and the wire transfer, including a telephone call from the thief posing as an outside attorney requesting the transfer. *See* Second Cir. Case No. 17-2492, Dkt. 55 at 11 (Dec. 4, 2017).

Taylor & Lieberman—Theft of Funds Belonging to the Insured's Client from Phishing

In *Medidata,* the court emphasized that the case before it—which involved coverage for the theft of the insured's ***own*** funds under a first party policy—was distinguishable from cases involving theft of the funds of an insured's client, or use of an insured's client's email address. *Medidata,* 268 F. Supp. 3d at 479. Coverage for such losses under a computer fraud policy can turn on this distinction, with the insured on the losing end, as shown in the recent case of *Taylor & Lieberman v. Federal Insurance Company,* 681 Fed. Appx. 627 (9th Cir. 2017).

The insured in *Taylor* was an accounting firm that performed services such as business management, account oversight, and tax planning and preparation. One of its clients was hacked by a perpetrator who fraudulently took hold of the email account of the insured's client and sent multiple wire payment instructions to the insured accounting firm. The accounting firm's employee believed the instructions to be from the client, so she requested the transfers. *See Taylor & Lieberman v. Fed. Ins. Co.,* No. CV 14-3608 RSWL SHX, 2015 WL 3824130, at *1 (C.D. Cal. June 18, 2015).

Upon discovering the scheme, the accounting firm was able to recover some, but not all, of the funds. It tendered its losses to Federal Insurance Company, which had sold to the firm a policy containing crime coverage. Federal denied coverage for the claim, and the lawsuit ensued. *Id.* at *2.

In the District Court, the insured argued that Federal breached its insurance contract under three different coverage sections: Forgery Coverage (because the emails constituted a forged signature); Computer Fraud Coverage (because the emails constituted a computer violation); and Funds Transfer Coverage (because the policy covered "fraudulent written electronic instructions issued to a financial institution"). *Id.* at *2-*3.

The District Court disagreed, holding that because each section covered only "direct loss sustained by an Insured," coverage could be properly denied in full. The court reasoned that the fraudulent emails did not result in a loss of the insured's own funds, but rather resulted in losses the insured owed to the client. *Id.* at *3 -*4. In so holding, the lower court in *Taylor* relied on a line of prior cases finding that as used in some crime policies, the term "direct loss" requires that the insured itself suffer an immediate and direct loss rather than losses stemming from liability to a third-party. *See Taylor* at *3 (citing, *inter alia, Vons Companies, Inc. v. Fed. Ins. Co.,* 212 F.3d 489 (9th Cir. 2000)) (no coverage for company's settlements with investors who alleged fraud by company's employee)); *Lynch Properties, Inc. v. Potomac Ins. Co. of Illinois,* 140 F.3d 622, 629 (5th Cir. 1998). *See also Hantz Fin. Servs., Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.,* 130 F. Supp. 3d 1089,

1090 (E.D. Mich. 2015), *aff'd on other grounds,* 664 F. App'x 452 (6th Cir. 2016) (no coverage for employee theft of client funds). These cases reason that insurer's agreement to cover a company's "direct" losses means the company's "immediate" loss and not its "proximate."

By contrast, in interpreting a computer fraud endorsement, some courts, including the Sixth Circuit applying Ohio law, have found that the term "direct loss" should be construed under a "proximate cause" standard. *See Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.,* 691 F.3d 821, 824 (6th Cir. 2012) (proximate cause standard applied to determine coverage under computer fraud endorsement for insured's liability to customers whose credit card and checking account information was stolen by hackers into DSW shoe store computer system). *See also Graybar Elec. Co., Inc. v. Fed. Ins. Co.,* 567 F.Supp.2d 1116, 1127 (E.D. Mo. 2008) (employee's forgery of executive's signature on contract between insured and customer was proximate cause of loss); *Frontline Processing Corp. v. Am. Econ. Ins. Co.,* 335 Mont. 192, 149 P.3d 906, 911 (2006); *Auto Lenders Acceptance Corp. v. Gentilini Ford, Inc.,* 181 N.J. 245, 854 A.2d 378 (2004); *Scirex Corp. v. Federal Ins. Co.,* 313 F.3d 841, 848–50 (3d Cir. 2002).

As for *Taylor* case, the Ninth Circuit ultimately affirmed the District Court's finding of no coverage, but on other grounds. Instead of solely addressing the "direct loss" issue, the appellate court engaged in an analysis of the three policy sections at issue. As to Computer Fraud Coverage, the court found that there was no "unauthorized entry" into the accounting firm's email system, nor an "introduction of instructions" that "propogate[d] themselves" through its computer system – both of which were required to be shown under the language of the Computer Fraud provision. *Taylor,* 681 Fed. Appx. at 629. Notably, the American Tooling court also relied on the absence of any "hacking" or "infiltration" into the insured's computers as an additional basis for finding that the computer fraud coverage did not apply. *See American Tooling,* 2017 WL 3263356, at *3 ("There was no infiltration or 'hacking' of ATC's computer system. The emails themselves did not directly cause the transfer of funds; rather, ATC authorized the transfer based upon the information received in the emails.").

Generic Cyber Insurance May Not Be the Answer for Phishing Losses Either

Although the *Taylor* court's holding that coverage for phishing was unavailable was under a crime policy, a policyholder may not always count on its "off-the-shelf" cyber insurance policies either. Generally, cyber liability insurance is intended to cover a company's liability for a data breach in which a third-party's confidential information is exposed or stolen. Such cyber insurance often seeks to fill a gap left by a compa-

ny's commercial general liability (CGL) policy, which may exclude liabilities stemming from the loss of electronic data despite the coverage generally available for "property damage." However, because issuers of cyber insurance policies presume that CGL policies will step in to provide coverage for "bodily injury" and "property damage," cyber insurers often include express exclusions for these losses. Thus, if social engineering results in "bodily injury" or "property damage," multiple insurers may point the finger at one another, with neither accepting coverage.

The potential gaps in cyber coverage, as well as in crime coverage as shown in *American Tooling* and *Taylor,* highlight importance of securing coverage that specifically identifies or targets social engineering and phishing activities. Policyholders should not buy narrowly tailored crime policies off-the-shelf, and hope that they find themselves in the "right" jurisdiction, but instead should seek to negotiate more expansive coverage tailored to their business. For example, if a core part of an insured's business involves the handling of client funds, there are policy forms potentially available that expressly provide coverage for losses sustained by the insured's "Clients" (as defined by the policy).

In addition, "Social Engineering Fraud Coverage" language that is potentially available based on existing policy forms includes:

- "loss resulting from an Organization having transferred, paid or delivered any Money or Securities as the direct result of Social Engineering Fraud committed by a person purporting to be a Vendor, Client, or an Employee who was authorized by the Organization to instruct other Employees to transfer Money or Securities"

- "direct loss from the transferring, paying or delivering of Money or Securities, directly caused by Social Engineering Fraud"

- "the Loss of Assets, excess the applicable deductible, resulting directly from Agent Theft, Computer Fraud, Dishonesty, Forgery, Funds Transfer Fraud, Impairment, Fraudulently-Induced Instruction or Non-Payment of Money order/Counterfeit Paper currency, which is first discovered by the Insured pursuant to clause [ ] Discovery of Loss of this Loss of Assets Coverage Section"

The conclusion to be drawn from the case law and the policy language is not new, and cannot be stated often enough: policyholders can and should read their policies carefully, and consult with their brokers and outside insurance counsel to negotiate the best language possible ***before*** there is a loss.

* * *

Lisa M. Campisi
Blank Rome, LLP
The Chrysler Building
405 Lexington Avenue
New York, NY 10174
Direct: 212-885-5378

For more information on Ms. Campisi, see her profile on the Blank Rome website.