AN A.S. PRATT PUBLICATION
SEPTEMBER 2018
VOL. 4 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 7 | SEPTEMBER 2018

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [209] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2018–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Cyber Phishing Scams: Do You Have Coverage? – Part II

James M. Westerlind, Eric A. Biderman, Adrienne M. Hollander, and Jake Gilbert*

In this second part of a two-part article, the authors discuss the case law addressing coverage for certain types of email phishing scams under the traditional crime policy forms. It then discusses protocols and procedures that may be employed by companies to reduce the risk of falling victim to such scams. The article concludes by suggesting that companies should assess whether they have adequate coverage for these types of email phishing scams. The first part of the article, which appeared in the July/August 2018 issue of Pratt's Privacy & Cybersecurity Law Report, *began the discussion of case law on the subject.*

This article continues a discussion on the case law addressing coverage for certain types of email phishing scams under the traditional crime policy forms.

CASES FINDING COVERAGE UNDER CRIME POLICIES

There are very few cases that have held that an email scam resulting in a loss to the insured company is covered under a fraud policy.

In *Medidata Solutions, Inc. v. Federal Ins. Co.*,[36] the insured used Google's Gmail platform for company emails. The insured's email address consisted of an employee's first initial and last name, followed by the domain name "mdsol.com" instead of "gmail.com." Emails sent to the insured's employees were routed through Google computer servers. Google processed and stored the emails. During processing, Google compared an incoming email address with the insured's employee profiles to find a match. When a match was found, Gmail displayed the sender's full name, email address, and picture in the "From" field of the email. After processing, the emails were displayed in the insured's employee's email account. The insured's employees used computers owned by the insured to access the emails that were processed and displayed by Google.

---

* James M. Westerlind (james.westerlind@arentfox.com) and Eric A. Biderman (eric.biderman@arentfox.com) are counsel in Arent Fox's litigation, insurance, cybersecurity and data protection, and automotive practice groups. Adrienne M. Hollander (adrienne.hollander@arentfox.com) is a senior associate in firm's litigation, white collar, antitrust, and business compliance practice groups. Jake Gilbert (jake.gilbert@arentfox.com) is an associate in the firm's litigation, insurance, and cybersecurity and data protection practice groups. (Footnotes continued from Part I.)

[36] 268 F. Supp. 3d 471 (S.D.N.Y. 2017) *aff'd*, No. 17-2492-cv (2d Cir. Jul. 6, 2018) (summary order).

In the summer of 2014, the insured notified its finance department that it may pursue an acquisition. Finance personnel were instructed to be prepared to assist with significant transactions on an urgent basis. Employee Evans worked in accounts payable.

On September 16, 2014, Evans received an email purportedly sent by the insured's president. The email contained the president's name, email address, and picture in the "From" field. It stated that the company was close to finalizing an acquisition, and that an attorney named Meyer would contact Evans. The email advised that the acquisition was strictly confidential and instructed Evans to devote her full attention to Meyer's demands. Evans responded that she would assist in any way that she could and make it a priority.

Later on September 16, Evans received a phone call from a man who claimed to be Meyer. He demanded that she process a wire transfer for him, and that a check would not suffice because of time constraints. Evans explained that she needed an email from the company's president requesting the wire transfer, and approval from Vice President Chin and Director of Revenue Schwartz.

Chin, Evans, and Schwartz then received a group email purportedly sent by the president stating: "I'm currently undergoing a financial operation in which I need you to process and approve a payment on my behalf. I already spoke with [Evans], she will file the wire and I would need you two to sign off." The email contained the president's email address in the "From" field and his picture next to his name. Schwartz and Chin approved the transfer, and Evans wire transferred over $4.7 million to a bank account identified by Meyer.

Two days later, Meyer contacted Evans again, asking for a second wire transfer. Evans initiated the second transfer, and Schwartz approved it. But Chin thought that the "Reply To" field in the email seemed suspicious. Chin discussed his concerns with Evans, and Evans composed a completely separate and new email to the president about the wire transfers. The president responded that he did not request the transfers.

Following an FBI investigation, it was learned that the thief had constructed the emails in Internet Message Format ("IMF"), which is like a physical letter containing a return address. The IMF message was transmitted to Gmail in an electronic envelope called a Simple Mail Transfer Protocol ("SMTP"). Much like a physical envelope, the SMTP Envelope contained a recipient and return address. To mask the true origin of the spoofed emails, the thief embedded a computer code. The computer code caused the SMTP Envelope and IMF Letter to display different addresses in the "From" field. The spoofed email showed the thief's true email address in the SMTP "From" field. When Gmail received the spoofed emails, the system compared the address in the IMF "From" field with a list of contacts within the insured's company and populated the president's name and picture. The recipients of the email only saw the information on the IMF "From" field.

The insured made a claim under its crime policy, seeking coverage under the (1) computer fraud, (2) funds transfer fraud, and (3) forgery coverage provisions. The computer fraud coverage applied to the "direct loss of Money, Securities or Property sustained by [the insured] resulting from Computer Fraud committed by a Third Party."[37] "Computer Fraud" was defined in the policy as "the unlawful taking of the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation."[38] A "Computer Violation" included both "the fraudulent: (a) entry of Data into . . . a Computer System; [and] (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format . . . directed against [the insured]."[39] "Computer System" was defined as "a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are: (a) owned and operated by [the insured] . . . ."[40] "Third party" was defined as "a natural person other than: (a) an Employee; or (b) a natural person acting in collusion with an Employee."[41]

The funds transfer fraud provisions provided coverage for the "direct loss of Money or Securities sustained by [the insured] resulting from Funds Transfer Fraud committed by a Third Party."[42] "Funds Transfer Fraud" was defined as "fraudulent electronic . . . instructions . . . purportedly issued by [the insured], and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by [the insured] at such institution, without [the insured's] knowledge or consent."[43]

The forgery coverage applied to "direct loss sustained by [the insured] resulting from Forgery or alteration of a Financial Instrument committed by a Third Party."[44]

With respect to computer fraud coverage, the *Medidata* Court held that there was coverage under the policy, relying principally on the New York Court of Appeals'[45] decision in *Universal Am. Corp. v. Nat'l Union Fire Ins. Co.*,[46] which involved a health insurance company that was defrauded by healthcare providers who submitted claims for reimbursement of services that were never rendered. The *Medidata* Court noted that the New York Court of Appeals held in *Universal* that "the unambiguous language of Universal's policy 'applie[d] to losses resulting from fraudulent content submitted to

---

[37] *Medidata*, 268 F. Supp. 3d at 474 (internal quotation marks and citation omitted).
[38] *Id.* (internal quotation marks and citation omitted).
[39] *Id.* (internal quotation marks and citation omitted).
[40] *Id.* (internal quotation marks and citation omitted).
[41] *Id.* (internal quotation marks and citation omitted).
[42] *Id.* (internal quotation marks and citation omitted).
[43] *Id.* (internal quotation marks and citation omitted).
[44] *Id.* (internal quotation marks and citation omitted).
[45] The New York Court of Appeals is New York's highest state court.
[46] 25 N.Y.3d 675 (2015).

the computer system by authorized users.'"[47] "Thus, *Universal* is more appropriately read as finding coverage for fraud where the perpetrator violates the integrity of a computer system through unauthorized access and denying coverage for fraud caused by the submission of fraudulent data by authorized users."[48]

The *Medidata* Court stated that the insurer's reliance on the district court's decision in *Pestmaster Services*[49] was misplaced, as that court had relied on *Universal* in explaining that "Computer Fraud occurs when someone hacks or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds."[50] The *Medidata* Court concluded that:

> [T]he fraud on [the insured] was achieved by entry into [the insured's] email system with spoofed emails armed with a computer code that masked the thief's true identity. *The thief's computer code also changed the true email address* to [the insured's] president's address to achieve the email spoof.[51]

Hence, the *Medidata* Court considered the computer code that the thief used to achieve the spoof akin to hacking into the insured's computer system, or violating the integrity of the insured's computer system through unauthorized access.

The *Medidata* Court also distinguished and rejected the U.S. Court of Appeals for the Fifth Circuit's decision in *Apache*.[52] Unlike *Apache*, where the fraudulent emails were invited by the insured and only one step in the middle of a multi-step process of the fraud (and, therefore, the use of a computer was deemed by the Fifth Circuit to not be the "direct cause" of the loss), the *Medidata* Court noted (a) that the insured's employees in this case did not invite the spoofed emails, and (b) the chain of events *began* with the spoofed emails. Further, the *Medidata* Court concluded that the Fifth Circuit's analysis was "unpersuasive": "To the extent that the facts of this case fit within *Apache*, the Court finds its causation analysis unpersuasive. The Court finds that [the insured's] employees initiated the transfer as a direct cause of the thief sending spoof emails posing as [the insured's] president."[53]

In addition, the *Medidata* Court distinguished the U.S. Court of Appeals for the Ninth Circuit's decision in *Taylor & Lieberman*.[54] First, in *Taylor & Lieberman*, the

---

[47] *Medidata*, 268 F. Supp. 3d at 477 (quoting *Universal*, 25 N.Y.3d at 680-81).

[48] *Medidata*, 268 F. Supp. 3d at 477-78 (citation omitted).

[49] *See* Part I of this article for a discussion of *Pestmaster Services.*

[50] *Medidata*, 268 F. Supp. 3d at 478 (quoting *Pestmaster Servs.,* (citing *Universal Am. Corp.*, 38 Misc. 3d 859 (N.Y. 2013), *aff'd*, 110 A.D.3d 434 (1st Dep't 2013), *aff'd*, 25 N.Y. 3d 675 (2015))).

[51] *Medidata*, 268 F. Supp. 3d at 478 (emphasis added).

[52] Discussed in Part I of this article.

[53] *Medidata*, 268 F. Supp. 3d at 479.

[54] Discussed in Part I of this article.

thief had stolen money from the insured's client, not the insured itself, which loss the insured was seeking to recover under its crime policy.[55] Second, in *Taylor & Lieberman*, the mere sending of emails from the client to the insured accounting firm did not constitute unauthorized entry into the accounting firm's computer system.[56] Here, by contrast, the insured was seeking to recover a loss of its own money, which was stolen as a direct result of spoofed emails armed with a computer code delivered into the email system that the insured used.[57] Indeed, the *Medidata* Court noted that both the district court and the Ninth Circuit in *Taylor & Lieberman* stated that if the subject funds had been held in an account owned or attributed to the insured, and a hacker had entered into the insured's computer system, then the insured would be correct in asserting coverage under the computer fraud coverage provisions of its crime policy.[58]

The *Medidata* Court also held that the insured was entitled to coverage under the funds transfer fraud provisions of its crime policy:

> In this case, it is undisputed that a third party masked themselves as an authorized representative, and directed [the insured's] accounts payable employee to initiate the electronic bank transfer. It is also undisputed that the accounts payable personnel would not have initiated the wire transfer, but for, the third parties' manipulation of the emails. The fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer depended upon several high level employees' knowledge and consent which was only obtained by trick. As the parties are well aware, larceny by trick is still larceny. Therefore, [the insured] has demonstrated that the Funds Transfer Fraud clause covers the theft in 2014.[59]

The *Medidata* Court distinguished *Pestmaster Services* on the funds transfer fraud coverage issue also, as in that case the insured had made valid transfers of funds to its payroll administrator who later misappropriated the funds: "The court [in *Pestmaster Services*] justified denial of coverage by pointing out, 'there is no evidence that . . . any third party, gained unauthorized entry into Pestmaster's bank's electronic fund transfer system *or pretended to be an authorized representative* or otherwise altered the electronic instructions in order to wrongfully divert money from the rightful recipient."[60]

Finally, the *Medidata* Court, consistent with the decisions discussed above, held that there was no coverage under the forgery coverage provisions of the crime policy because there was no financial instrument involved: "If forgery is viewed in isolation

---

[55] *Medidata*, 268 F. Supp. 3d at 479 (citations omitted).
[56] *Id.* (citation omitted).
[57] *Id.*
[58] *Id.* (citations omitted).
[59] *Id.* at 480.
[60] *Id.* (quoting *Pestmaster Servs.*, emphasis added by *Medidata* Court).

[(*i.e.*, without requiring that a financial instrument be involved, as required by the policy provisions)], the Policy would certainly be converted to a general crime policy."[61] This was not the intent of the policy, according to the *Medidata* Court, as evidenced by the requirement of a financial instrument in the insuring agreement provisions of this coverage part.

In addition, since the publication of Part I of this article, the U.S. Court of Appeals for the Sixth Circuit decided *American Tooling Center, Inc. v. Travelers Cas. & Surety Co. of Am.*, reversing the district court's decision finding no coverage, and concluding that the insured was entitled to coverage under each of the provisions of the Travelers crime policy in dispute.[62] Briefly as way of background, the insured, American Tooling Center, Inc. ("ATC"), is a tool and die manufacturer in Michigan that outsources some of its manufacturing orders to YiFeng, a Chinese company. ATC asked YiFeng via email for all of its outstanding invoices. A thief somehow intercepted this email, impersonated the intended recipient at YiFeng, and instructed ATC to wire payments to a different account than usual, which was controlled by the thief. ATC followed its normal internal payment protocols, and wired payments to the thief. When YiFeng inquired about payment for the outstanding invoices, ATC realized that it had been duped.

The first series of coverage issues arose out of the "Computer Fraud" provisions of the crime policy, which stated that: "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*."[63]

The first coverage issue was whether the wire transfers to the thief constituted a "direct loss" of ATC's money. In *Acorn Investment Co. v. Michigan Basic Prop. Ins. Ass'n*,[64] the Michigan Court of Appeals (the highest Michigan court to interpret the phrase "direct loss" in an insurance dispute) stated that a "direct" loss is one resulting from an "'immediate' or 'proximate' cause, as distinct from remote or incidental causes." But in *Tooling, Manufacturing & Technologies Ass'n v. Hartford Fire Ins. Co.*,[65] a case involving employee-fidelity bonds, the Sixth Circuit more narrowly stated that "direct is direct," and that "direct" means "immediate." In *American Tooling Center*, the Sixth Circuit stated that ATC suffered a "direct loss" under either definition under the facts of this case because it "immediately lost its money when it transferred the approximately $834,000 to the impersonator; there was no intervening event."[66] The court utilized the following analogy in response to Travelers' argument that no "direct loss" had occurred:

---

[61] *Medidata*, 268 F. Supp. 3d at 480.

[62] 895 F.3d 455 (6th Cir. 2018). In Part I of this article, we noted that the district court decision had been appealed to, but not decided by, the Sixth Circuit as of the date of that publication. Pratt's Privacy & Cybersecurity Law Report, Vol. 4, No. 6 p. 179 n.28 (July/August 2018).

[63] *American Tooling Center*, 895 F.3d at 459 (citations omitted; italicized terms defined in policy).

[64] No. 284234 (Mich. Ct. App. Sep. 15, 2009).

[65] 693 F.3d 665, 676 (6th Cir. 2012).

[66] *American Tooling Center*, 895 F.3d at 460 (citation omitted).

> A simplified analogy demonstrates the weakness of Travelers' logic. Imagine Alex owes Blair five dollars. Alex reaches into her purse and pulls out a five-dollar bill. As she is about to hand to Blair the money, Casey runs by and snatches the bill from Alex's fingers. Traveler's theory would have us say that Casey caused no direct loss to Alex because Alex owed that money to Blair and was preparing to hand him the five-dollar bill. This interpretation defies common sense.[67]

The next coverage issue was whether the definition of "Computer Fraud" in the crime policy required a computer to fraudulently cause the transfer. Travelers contended that it was insufficient to simply use a computer and have a transfer that is fraudulent. "Computer Fraud" was defined as:

> The use of any computer to fraudulently cause a transfer of *Money*, *Securities* or *Other Property* from inside the *Premises* or *Financial Institution Premises*:
>
> 1. to a person (other than a *Messenger*) outside the *Premises* or *Financial Institution Premises*.
> 2. to a place outside the *Premises* or *Financial Institution Premises*.[68]

The Sixth Circuit distinguished *Pestmaster Services, Inc. v. Travelers Cas. & Surety Co. of Am.*,[69] on its facts. In *Pestmaster*,[70] the insured's vendor, a payroll tax services company, had received the insured's money using computers legitimately and then misappropriated that money; "[i]n contracts, here [in *American Tooling Center*] the impersonator sent ATC fraudulent emails using a computer and these emails fraudulently caused ATC to transfer the money to the impersonator."[71] Since there was no limitation in the Travelers crime policy requiring that fraud cause the computer to do anything, Travelers' argument in this regard was rejected by the Sixth Circuit.

The third coverage issue was whether the loss was "directly caused" by computer fraud. Here, the court distinguished the facts of this case from those in *Interactive Communications Int'l, Inc. v. Great Am. Ins. Co*.[72] In *American Tooling Center*, "ATC employees received the fraudulent email at step one. ATC employees then conducted a series of internal actions, all induced by the fraudulent email, which led to the transfer of the money to the impersonator at step two. This was 'the point of no return,'

---

[67] *Id.* at 461.

[68] *Id.* (citation omitted).

[69] 656 F. App'x 332 (9th Cir. 2016).

[70] We discussed the *Pestmaster* decision in detail in Part I of this article.

[71] *American Tooling Center*, 895 F.3d at 461-62 (citation omitted).

[72] No. 17-11712 (11th Cir. May 10, 2018). We discussed the Eleventh Circuit's decision in *Interactive Communications Int'l* in detail in Part I of this article.

because the loss occurred once ATC transferred the money in response to the fraudulent emails. Thus, the computer fraud 'directly caused' ATC's 'direct loss.'"[73]

In *Interactive Communications Int'l*, by contrast, the "point of no return" was not at step two, when money was transferred, but rather at step four. Step one in *Interactive Communications Int'l* was when bad actors manipulated the insured's computer system to allow for double-redemption on credit cards; step two was the transfer of money by the insured; step three was the purchases by the bad actors with the credit cards; and step four was when the third-party deducted the amount of the purchase from the insured's account. Since, in *Interactive Communications Int'l*, the insured was able to freeze the accounts by step four, the chain of events was too attenuated. That was not the case, according to the Sixth Circuit, in *American Tooling Center*.

Further, despite the fact that the district court never addressed the issue of Traveler's coverage defenses premised on exclusions in the policy, the Sixth Circuit addressed each of the three exclusions relied on by Travelers and rejected each argument by the insurer.

Thus, there have been far less court decisions finding coverage in spoofing scenarios under crime policies than court decisions finding no coverage for such scams under such policies.[74] In short, most crime policies were not designed to provide coverage for cyber losses such as these. But crime policies should be modified to provide coverage for

---

[73] *American Tooling Center*, 895 F.3d at 463.

[74] *See Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, No. 11-cv-6187 (D. N.J. Mar. 29, 2012), wherein the court allowed a suit against an insurer to survive a motion to dismiss:

> The policy provides, in the relevant part, that Defendant will insure the Plaintiff against losses "following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside the 'premises' . . . to a person outside those premises." ([Policy] §§ II.E(1)-(2)). This plausibly encompasses insurance against the transfer of use of the servers to a person outside Plaintiff's premises. This is especially true when read against the second portion of this provision, which provides that Plaintiff is insured against losses caused by fraudulent computer use that results in "a transfer of that property from inside the 'premises' . . . to a place outside those premises." (*Id.*). Defendant's reading of the insurance contract, which would require the physical transfer of the property to outside the premises for Plaintiff to have a valid claim, would seemingly make subsection II.E(1) of the contract superfluous. This Court must read the insurance agreement as a whole and give effect to all of its parts. Therefore, Plaintiff's reading of the contract in this regard appears plausible.

The court also stated that the insured's allegations of loss of use of the full capacity of its servers as a result of the hacker's conduct was sufficient to allege a loss of property under the policy. *Id. See also Owens, Schine & Nicola, P.C. v. Travelers Cas. & Surety Co. of Am.*, No. CV095024601 (Super. Ct. Conn. Sep. 20, 2010), where the Connecticut state court initially found that the insured's crime policy was ambiguous with respect to its "Computer Fraud" definition, therefore construing it against the carrier and in favor of the insured and coverage. The court also stated that direct causation in a crime policy under Connecticut law is equivalent to "proximate cause;" hence, the emails which led to the fraudulent transfers "proximately caused" them. But the decision was subsequently vacated by order and stipulation. *Owens, Schine & Nicola, P.C.*, (Super. Ct. Conn. Apr. 18, 2012).

incidents like these, as they are a risk that has now become prevalent and there is a need in the market for such coverage. With proper pricing data, insurers should certainly be in a position to provide appropriate coverage for such losses. The risk here is not a type of moral hazard that should be borne by the insured for public policy reasons.

PROCEDURES AND PROTOCOLS THAT COMPANIES CAN EMPLOY TO REDUCE LOSS INCIDENTS

Companies should consider employing the following procedures and protocols to avoid a loss caused by a phishing or spoof scam described above, especially considering that such a loss, depending on the facts of the case, may not be covered under the insured's crime or other[75] insurance policies:

- Employees should be trained on how to detect and avoid phishing and spear phishing email scams through real examples. This would include the fact patterns of the cases discussed above, as well as training sessions with experts in the industry. Real life examples can also be found at US Berkley's Phish Tank[76] and Cornell's Phish Bowl.[77] An employee will probably learn better from real life examples than from generic instructions like, "Never click on a link in, or an attachment to, a suspicious email."
- Employees should be regularly updated as to new phishing techniques being used by criminals. One of the reasons that it is impossible to create an all-inclusive list of ways to avoid phishing scams is because the scams are constantly changing and evolving. So training sessions for employees on this subject need to be updated regularly.
- Companies should require the installation of anti-phishing toolbars, which run checks on sites that your employees visit and compare them to lists of known phishing sites, which lists are updated regularly. The tool bar should alert your employee of the fact that a site he/she wants to go to is on the danger list.
- Train your employees to make sure that websites are secure, which can be evidenced by the site's URL beginning with "https" and a closed-lock icon near the address bar.
- Make sure that security patches are installed regularly by your employees. Make sure that your employees log off at the end of each day, and log back on the next day, so that new patches are installed and functioning.

---

[75] Such losses would likely not be covered under most cyber insurance policies either. While there is no standard cyber insurance policy form as of yet, most of the cyber insurance policy forms that the authors of this article have seen would likely not provide coverage for many of the fact patterns described in the cases discussed above.

[76] *See* https://security.berkeley.edu/resources/phishing/phish-tank.

[77] *See* https://it.cornell.edu/phish-bowl.

- Use desktop firewalls, as well as network firewalls. Use anti-virus software. Block pop-ups from unknown sites.
- Employees who receive email requests to transfer company funds to a third party (especially via wire transfer) should compose a separate, and completely new email in response to the sender, confirming the request. The employee should also call the person purportedly sending the email, and do so with a phone number confirmed by a source other than the email making the request.
- Test your employees with simulated phishing campaigns. These can be done internally, depending on the sophistication of your company, or through vendors, such as KnoBe4[78] and Gophish,[79] which can perform targeted campaigns and record the results of your employees' reactions.
- Use the data from employee testing to identify particularly vulnerable areas and employees, and then adjust your business processes to reduce these vulnerabilities.
- Keep lines of communication open with your employees so that questions and concerns are easily answered and addressed.
- Reward your employees for actively reporting suspected phishing scams to your IT Department (and not falling for the scam), and successfully avoiding a simulated phishing scam, as described above.

CONCLUSION

As evident from the case law discussed above, an email scam resulting in loss to a company may not be insured by that company's existing crime or other insurance policy(ies). As such, companies should assess their existing insurance policies to determine whether they have a gap in coverage for these types of risks. Companies should also create written procedures and protocols and be diligent about training their employees to reduce the likelihood of one or more of its employees falling for one of these extremely deceptive scams. Furthermore, companies should seriously explore whether blockchain[80] technology is a viable option to reduce exposure to an email scam.

---

[78] *See* https://www.knowbe4.com/phishing-security-test-offer.

[79] *See* https://getgophish.com/.

[80] "Blockchain" is defined as "a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network; also: the technology used to create such a database." https://www.merriam-webster.com/dictionary/blockchain.