AN A.S. PRATT PUBLICATION
JULY/AUGUST 2018
VOL. 4 • NO. 6

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

# Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 NUMBER 6 JULY/AUGUST 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 [167] (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 I

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

*In this first 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. The second part of the article, which will appear in an upcoming issue of* Pratt's Privacy & Cybersecurity Law Report, *continues the discussion of the case law on the subject. 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.*

Over the past decade, our society has seen a shift in the way that criminal activities target businesses. Criminals have engineered sophisticated methods of duping unsuspecting employees into wiring funds, often times in ways that wholly evade detection from the most intelligent cybersecurity software platforms. Where these criminal ploys successfully convince an individual to wire payment through decoy emails (sometimes in the tens of millions of dollars), insurance coverage is often denied because the "victim" knew or consented to the wire instructions that it was tricked into providing to its bank, rather than by way of third-party instructions impersonating the insured which would certainly have been covered by the company's traditional crime policy.

Policies have evolved and many carriers in the United States now offer coverage for email phishing scams. For instance, the Beazley Breach Response policy includes coverage for fraudulent instruction, as does Beazley's commercial crime policy. In addition, Marsh has created a CrimeBlock coverage form which adopts an "all risk" approach to coverage. Coverage under CrimeBlock is triggered by any fraudulent, criminal, dishonest, or malicious act committed by any natural person, and the form does not make any distinction between fraud committed by employees of an insured or third-parties.[1]

It should be noted that different insurance policies or coverage forms are intended (and priced) to cover different risks. While one incident may, based on the facts, trigger coverage under more than one policy or coverage form, the risks triggering each policy

* 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 the 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.

[1] But, unfortunately, no U.S. carriers have issued Marsh's CrimeBlock form on a primary policy basis.

or coverage form are typically different. There is often, by design, little overlap between the coverage available under one policy or coverage form and another (e.g., a cyber insurance policy and crime policy).

While commercial insurers have tended to modify the crime policies that they offer to cover risks like email phishing scams (and not cover such risks under the other policies and coverage forms that they offer), many older traditional crime policy forms may not provide coverage for such email phishing scams. This article will discuss the case law addressing coverage for these types of email phishing scams under the traditional crime policy forms. It will then discuss protocols and procedures that may be employed by companies to reduce the risk of falling victim to such scams. It concludes by suggesting that companies should assess whether they have adequate coverage for these types of email phishing scams.

## THE PLOY

Business operations have grown to use endless amounts of email in order to coordinate projects, collectively draft policies, confirm schedules, and request payments. The critical assumption underlying the reliance on email is that the person whose name is identified as the sender is actually the sender. Without some level of assurance in the authenticity of the sender's identity, no instruction or request set forth in the email could be followed without several additional levels of confirmation that the email is legitimate. Employing protocols that require additional steps to confirm that emails are legitimate, while advisable and necessary in certain instances, is counter to one of the principal reasons that we use email to begin with – ease of use and efficiency.

Thieves looking to steal company assets have begun exploiting the generally relaxed scrutiny that its employees tend to employ when they receive email instructions from those who they think are their superiors, or known business partners or vendors. Thieves are gaining access to legitimate email accounts, or sending emails made to appear legitimate, posing as senior members of the company, or vendors employed by the company, or the company's attorneys, or even important shareholders. The perpetrators often request that the company transfer funds to a bank account and then, after the transaction is complete, disappear with the money. This scheme can take the form of a vendor changing the bank account to wire payment for completed services; a senior member of the company requesting that a payment be sent to a particular account to complete a transaction; or the company's in-house or outside lawyer requesting funds to be transferred to a particular account for purposes of an alleged settlement or company transaction. In all of these cases, the requestor is not who he or she appears to be, and the scam is not realized until the funds are lost in whole or in substantial part.

Chubb has recently tracked this type of social engineering scheme. It calculated in 2017 that 15 percent of all cyber losses resulted from this variety of scam.[2] And it has gained popularity in 2018, rising to 21 percent of all cyber losses so far this year.[3] These types of social engineering attacks grew out of older "phishing"[4] and "spear phishing"[5] attacks, in which an electronic message would be sent with malicious code behind an innocuous link or file attached to, say, an email which would appear to be from a trusted source. Many other types of social engineering attacks exist, all following the same basic pattern, but few involve as narrow a focus as the sort of impersonations and fraudulent transfers that businesses have been encountering the past several years.[6]

Verizon, as part of its recent Data Breach Investigations Report, released data on social engineering scams in 2017, showing that 43 percent of data breaches involved social engineering attacks across all industries.[7] Thieves have attempted to find the easiest vector for attack, which is usually the people on the other side of the computer screen.

Illegitimate email instructions to employees with authority to transfer company funds have resulted in millions of dollars of losses in numerous instances.[8] Many companies that have been victims of these scams have made claims for their losses under their traditional crime policies, often arguing that the "Computer Fraud" and "Funds Transfer Fraud" insuring agreement provisions should provide coverage. But most of these companies have faced resistance from their crime coverage insurers, and not found success in court.

---

[2] *See* https://chubbcyberindex.com/. Forbes estimates that phishing constitutes 77 percent of all socially based attacks, including fraudulent transfers (identified in the article as Business Email Compromise scams). *See* https://www.forbes.com/sites/laurashin/2017/01/04/be-prepared-the-top-social-engineering-scams-of-2017/#1a4db8377fec.

[3] *See* https://chubbcyberindex.com/.

[4] A "phishing" attack is an attempt through an electronic communication – typically email or instant message – to obtain sensitive personal information, such as usernames, passwords, and credit card or other financial information, by directing the recipient to a fake website that looks to be legitimate. *See* https://www.us-cert.gov/report-phishing.

[5] "Spear phishing" is a phishing attack directed to specific individuals or companies. *See* https://usa.kaspersky.com/resource-center/definitions/spear-phishing.

[6] For more examples and information, *see* https://www.incapsula.com/web-application-security/social-engineering-attack.html.

[7] *See* https://www.social-engineer.com/2017-verizon-dbir-social-engineering-breakdown/.

[8] The FBI reported that fraudsters sought to steal $5.3 billion through fraudulent email scams through the first half of 2017. Trend Micro, a digital security firm, has estimated that the number will be closer to $8 billion by the end of 2018. *See* https://documents.trendmicro.com/assets/TrackingTrendsinBusinessEmailCompromise.pdf. Sample attacks include Omaha, Nebraska's Scoular Co., which lost $17.2 million in fraudulent trade orders (http://www.omaha.com/money/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html), and Detroit's Talmer Bank, which nearly lost $20,000 (https://www.clickondetroit.com/news/bank-ceos-fake-email-and-the-russian-mob). More examples have been gathered by InfoSec Institute. *See* http://resources.infosecinstitute.com/5-real-world-examples-business-email-compromise/#gref.

A number of federal district courts have addressed whether a company is entitled to coverage under a crime policy's computer fraud, funds transfer fraud, and related coverage sections for a loss of funds which were transferred as a result of a third-party impersonating a senior member of the company. Generally, these courts have found that coverage is not available because the employee, who ultimately was duped into transferring the funds, had full authority to access the company's computer system and complete the transfer. In some of these cases, the fact that no actual access by the thief to the company's computer system had occurred was the deciding factor by virtue of the crime policy's language. As discussed in the second part of this article, a federal district court in New York has recently held that there is coverage for an email scam, but that decision may be limited to the facts of the case.

## CASES FINDING NO COVERAGE UNDER CRIME POLICIES

We begin our journey of the case law with *Pestmaster Servs., Inc. v. Travelers Cas. & Surety Co. of America*.[9] While this case did not involve an email spoof or phishing scam, it has been cited by a number of subsequent cases addressing email scams as legal precedent for the coverage analysis under a crime policy.

In *Pestmaster Services*, the insured, Pestmaster, hired Priority 1 (a vendor) to handle its payroll and payroll taxes.[10] In order to allow Priority 1 to perform these services, Pestmaster executed an ACH authorization which authorized Priority 1 to obtain payment of Priority 1's approved invoices by initiating ACH transfers of funds from Pestmaster's bank account to Priority 1's bank account. For each payroll period, Priority 1 would prepare and deliver invoices to Pestmaster reflecting amounts owed for employees' salaries and payroll taxes. Once Pestmaster approved payment of the invoices, Priority 1 would initiate an ACH transfer and move sufficient funds from Pestmaster's bank account to Priority 1's account in order to pay the amounts approved by Pestmaster. It was later discovered by Pestmaster that Priority 1 had wrongfully used such transferred funds for its own purposes, in violation of the parties' agreement. Pestmaster made a claim under its crime policy.

The U.S. Court of Appeals for the Ninth Circuit agreed with the district court that fund transfers that had been authorized by Pestmaster were not covered under either (1) the funds transfer fraud provisions, or (2) the computer fraud provisions of the crime policy, concluding that the intent of the policy was not to provide such broad coverage:

> First, Pestmaster argues that the transfer of funds from its bank account to Priority 1's bank account is covered by the Funds Transfer Fraud provision. The district

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

[10] The facts are set forth in the district court's decision, No. 13-cv-5039-JFW (MRWx) (C.D. Cal. Jul. 17, 2014). The Ninth Circuit's Memorandum decision does not recite the underlying facts in detail.

> court found that this provision "does not cover authorized or valid electronic transactions . . . even though they are, or may be, associated with a fraudulent scheme." We agree that there is no coverage under this clause when the transfers were expressly authorized.
>
> Second, Pestmaster seeks coverage under the Computer Fraud provision. The Policy defines Computer Fraud as "[t]he use of any computer to fraudulently cause a transfer. . .." We interpret the phrase "fraudulently cause a transfer" to require an unauthorized transfer of funds. When Priority 1 transferred funds pursuant to authorization from Pestmaster, the transfer was not fraudulently caused. Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a "General Fraud" Policy. While Travelers could have drafted this language more narrowly, we believe protection against all fraud is not what was intended by this provision, and not what Pestmaster could reasonably have expected this provision to cover.[11]

But the Ninth Circuit vacated that portion of the district court's decision that related to certain unauthorized transfers of funds, and remanded to the district court to determine if those unauthorized transfers were covered under the funds transfer fraud or computer fraud provisions of the crime policy.[12]

Next, the U.S. Court of Appeals for the Fifth Circuit, in *Apache Corp. v. Great American Ins. Co.*,[13] found that $2.4 million paid to thieves who were impersonating the insured's vendor was not covered under the Computer Fraud section of Apache Corp.'s crime-protection policy. In *Apache Corp.*, an Apache employee in Scotland received a telephone call from a person identifying herself as a representative of Petrofac, a vendor for Apache. The caller instructed Apache to change the bank account information for its payments to Petrofac. The Apache employee replied that the change-request could not be processed without a formal request on Petrofac letterhead.

A week later, Apache's accounts-payable department received an email from a "petrofac*ltd*.com" address. But Petrofac's authentic email domain name was "petrofac.com" (*i.e.*, without the "ltd" part). The criminals had created the "petrofacltd.com" domain name to send the fraudulent email. The email stated that Petrofac's account details must be changed immediately, and all future payments were required to be paid to the new account. As noted in the email, an attachment to it was a signed letter on Petrofac letterhead providing both the old and new bank account information, including the new bank account number, with instructions to use the new bank account immediately.

---

[11] *Pestmaster*, 656 F. App'x at 333.

[12] *Id.*

[13] 662 F. App'x 252 (5th Cir. 2016).

In response, an Apache employee called the fake telephone number provided on the letterhead (rather than looking in the company's records or some independent source for the real telephone number) to verify the request and confirm the authenticity of the change request. Next, a different Apache employee approved and implemented the change. A week later, Apache was transferring funds for payment of Petrofac's invoices to the new (fraudulent) bank account.

Within a month, however, Apache received notification that Petrofac had not received approximately $7 million that Apache has transferred to the new (fraudulent) bank account. After an investigation determined that the criminals were likely based in Latvia, Apache recouped a substantial portion of the funds, but suffered a loss of approximately $2.4 million.

The court, reading the policy under Texas rules of insurance contract interpretation,[14] found that for coverage to exist, the policy required "computer fraud," which the crime policy defined as "[t]he use of any computer to fraudulently cause a transfer." While the court concluded that the "computer use" was the fraudulent email, it held that the email was *incidental* to the occurrence of the authorized transfer of money:

> The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would, as stated in *Pestmaster II*, convert the computer-fraud provision to one for general fraud. We take judicial notice that, when the policy was issued in 2012, electronic communications were, as they are now, ubiquitous, and even the line between "computer" and "telephone" was already blurred. In short, few—if any—fraudulent schemes would not involve some form of computer-facilitated communication.
>
> This is reflected in the evidence at hand. Arguably, Apache invited the computer-use at issue, through which it now seeks shelter under its policy, even though the computer-use was but one step in Apache's multi-step, but flawed, process that ended in its making required and authorized, very large invoice-payments, but to a fraudulent account.
>
> * * *
>
> Moreover, viewing the multi-step process in its simplest form, the transfers were made not because of fraudulent information, but because Apache elected to pay

[14] "[T]he Texas Supreme Court has stressed its policy preference for 'uniformity when identical insurance provisions will necessarily be interpreted in various jurisdictions.' *McGinness* [*Indus. Maint. Corp. v. Phoenix Ins. Co.*], 477 S.W.3d [786,] 794 [(Tex. 2015)] (responding to Fifth Circuit certified question). And, even when uniformity is made impossible by jurisdictional splits, Texas courts 'strive for uniformity as much as possible'. *Id.* (internal quotation marks omitted) (quoting *Trinity Universal Ins. Co. v. Cowan*, 945 S.W.2d 819, 824 (Tex. 1997))." *Apache Corp.*, 662 F. App'x at 255.

> legitimate invoices. Regrettably, it sent the payments to the wrong bank account. Restated, the invoices, not the email, were the reason for the funds transfers.[15]

In *Taylor & Lieberman v. Federal Ins. Co.*,[16] the insured accountant firm was duped by fake emails instructing it to direct its client's bank to wire funds to an account controlled by a thief. The insured sought coverage under: (1) the forgery coverage; (2) computer fraud coverage; and (3) funds transfer fraud coverage provisions of its crime policy. The Ninth Circuit rejected all three of the insured's arguments.

With respect to the forgery coverage, the policy provided coverage for the insured's direct loss "resulting from Forgery or alteration of a Financial Instrument by a Third Party."[17] Since the emails instructing the insured to wire money were not Financial Instruments (such as checks), the forgery coverage was not triggered.

For the computer fraud coverage, the insured contended that there was coverage because the emails constituted an unauthorized (1) "entry into" its computer system, and (2) "introduction of instructions" that "propogate[d] themselves" through the computer system.[18] The Court held that sending an email, without more, does not constitute an unauthorized entry into the recipient's computer system.[19] In addition, "the [email] instructions did not, as in the case of a virus, propagate themselves throughout [the insured's] computer system; rather, they were simply part of the text of three emails."[20] Hence, there was no computer fraud coverage.

Finally, the funds transfer fraud coverage provisions applied to "fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions issued to a financial institution directing such institution to transfer, pay or deliver *Money* or *Securities* from any account maintained by an *Insured Organization* at such Institution, without an *Insured Organization's* knowledge or consent."[21] The court held that these coverage provisions were not triggered because (a) the insured knew about the wire transfers (indeed, the insured requested them, albeit pursuant to fraudulent instructions), and (b) the insured, as an accounting firm, was not a financial institution.[22]

In *Interactive Communications Int'l, Inc. v. Great American Ins. Co.*,[23] the insured, InComm, was in the debit card processing business. It had a processing system

---

[15] *Apache Corp.*, 662 F. App'x at 258-59 (citation omitted).

[16] 681 F. App'x 627 (9th Cir. 2017).

[17] *Taylor & Lieberman*, 681 F. App'x at 628 (internal quotation marks omitted).

[18] *Id.* at 629 (internal quotation marks omitted).

[19] *Id.* (citing *Intel Corp. v. Hamidid*, 71 P.3d 296, 304 (Cal. 2003) and *Spam Arrest, LLC v. Replacements, Ltd.*, No. C12-481RAJ (W.D. Wash. Aug. 29, 2013)).

[20] *Taylor & Lieberman*, 681 F. App'x at 629.

[21] *Id.* (internal quotation marks omitted).

[22] *Id.* at 629-30.

[23] No. 17-11712 (11th Cir. Mar. 10, 2018).

vulnerability by which a debit card holder could cause credit to be loaded onto his/her debit card in multiples of the credit amount purchased.

Debit card holders purchased "chits" from retailers, such as CVS or Walgreens, to add prepaid funds onto their debit cards. Each chit represented the amount purchased (plus a service fee), to be redeemed once. From November 2013 to May 2014, there was a code error in InComm's Interactive Voice Response ("IVR") system. The error permitted chits to be redeemed more than once, allowing cardholders to obtain more chit credit than they had paid and were entitled. To obtain multiple redemptions of a single chit, cardholders used more than one telephone simultaneously to access InComm's IVR system to request redemption of the same chit. The simultaneous redemption requests exploited InComm's coding error, allowing cardholders to redeem the same chit multiple times using the simultaneous phone call scheme. The unauthorized redemptions caused InComm to transmit close to $11.5 million to various debit card issuers (with approximately $10.8 million being transferred to Bancorp alone), which card issuers would, in turn, hold the funds and later transfer them to merchants to pay for purchases made with the cards.

InComm sought coverage for its losses under the computer fraud provisions of its crime policy, which would "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 of those premises; or (b) to a place outside those premises."

The district court below had granted summary judgment to Great American Ins. Co. on the question of whether the loss was covered under the computer fraud provisions of the crime policy on grounds that (1) the fraudulent scheme did not involve the "use" of a computer, and (2) the loss did not "result directly" from the use of a computer. On appeal, the U.S. Court of Appeals for the Eleventh Circuit held that the fraudulent scheme did involve the "use" of a computer, but agreed with the district court that the loss had not "resulted directly" from the use of a computer.

On the first ("use") issue, the Eleventh Circuit concluded that the plain dictionary definitions utilized by the district court in its analysis supported the insured's contention that the fraudsters had used a computer in their scheme, and the fact that the fraudsters may not have known that they did so was irrelevant to the coverage question:

> The question is whether the fraudsters "use[d]" both phones and computers to perpetrate their scheme—namely, *using* the phones to manipulate—and thereby *use*—the IVR computers. In rejecting InComm's argument, the district court seems to have imposed additional conditions not required by the policy's plain language—for instance, that the computer "use" be knowing. *See, e.g.*, Dist. Ct. Op. at —("There is no record evidence that cardholders even realized their telephone calls resulted in interaction with a computer.").

> But the plain meaning of the word "use"—indeed, as evidenced in the very definitions cited by the district court—comfortably supports an understanding that encompasses the callers' access and manipulation of InComm's IVR system. The district court, for instance, cited both the Oxford Dictionaries' online definition of the term "use" to mean "take, hold, or deploy (something) as a means of accomplishing or achieving something; employ," and *Webster's Encyclopedic Unabridged Dictionary*'s definition to mean "to employ for some purpose; put into service; make use of." *Oxford Dictionaries*, https://en.oxforddictionaries.com/definition/use; *Webster's Encyclopedic Unabridged Dictionary of the English Language* 2097 (2001). Those definitions, it seems to us, fit like a glove. Here, the callers clearly "deploy[ed]"—or "employ[ed]"—the IVR computer system "as a means of accomplishing or achieving" fraudulent duplicate redemptions of InComm chits. *See Oxford Dictionaries,* https://en.oxforddictionaries.com/definition/use. So too, under the district court's Webster's-based definition, the callers "used" the IVR system, "employ[ing]" it "for some purpose; put[ting it] into service; mak[ing] use of" it. *See Webster's Encyclopedic Unabridged Dictionary of the English Language* (2001).
>
> Other dictionaries confirm what the district court's own indicate. *Webster's Second New International Dictionary*, for instance, defines "use" as "to convert to one's service; to avail oneself of; to employ." *Webster's New International Dictionary* at 2806 (2d ed. 1939). There simply can be no doubt that the fraudsters "convert[ed]" InComm's IVR computer system to their service and "avail[ed]" themselves of it by submitting fraudulent reload requests to the computer system in a way that yielded duplicate chit redemptions. To be clear, it is not the case, as the district court suggested, that the IVR system was just "somehow involved" in the fraudsters' scheme, or that the system was merely "engaged at any point in the causal chain." Rather, the fraudsters interfaced directly with the IVR computer system to effectuate their duplicate redemptions. Thus, we conclude that the fraud against InComm *was* perpetrated through the "use of a[ ] computer" within the terms of its insurance policy.[24]

On the second ("result directly") issue, the Eleventh Circuit again utilized dictionary definitions of the word "directly" to "hold that, for purposes of InComm's policy, one thing 'results' directly from another if it follows straightaway, immediately, and without intervention or interruption."[25] In analyzing the facts of this case, the Eleventh Circuit considered (1) the steps involved in the fraudulent transfer, and (2) temporal aspects of the scheme.

With respect to the steps involved, the court stated as follows:

---

[24] *Id.*
[25] *Id.*

[S]everal steps typically intervened between the fraudulent manipulation of the IVR system to enable duplicate chit redemptions, on the front end, and InComm's ultimate loss, on the back. Here is a timeline of sorts:

- **Step 1:** The fraudsters manipulate InComm's IVR system to enable a duplicate chit redemption. For each fraudulently redeemed chit, a fraudster's debit card is immediately credited with purchasing power, but InComm's funds are neither transferred, nor disturbed, nor altered in any way.
- **Step 2:** Shortly after processing a redemption call through the IVR system, InComm transfers money (equal to the amount of the redeemed chits) to an account at Bancorp for the purpose of paying debts incurred by debit card holders. Bancorp maintains the account "for the benefit of" InComm as "holder[ ] of the Cardholder Balances for the benefit of [Debit] Cardholders." Although InComm is contractually obligated to transfer funds to the Bancorp account within 15 days of making the corresponding purchasing power available on debit cards, as a matter of regular business practice it transfers the money to Bancorp within 24 hours. The funds remain in the Bancorp account until needed to cover purchases made on a consumer's debit card.
- **Step 3:** A debit card user makes a purchase from a merchant, incurring debt to be paid from the InComm-earmarked Bancorp account.
- **Step 4:** Bancorp transfers money from the account to the merchant to cover the purchase made by the cardholder.

InComm insists that its loss occurred at Step 2—and is thus "directly" the result of the Step-1 fraud. In particular, InComm says that upon transfer of funds to the account held by Bancorp, it lost both ownership and control of those funds. But the facts of the case demonstrate otherwise—that, in fact, InComm retained at least some control over the funds held by Bancorp even after the Step-2 transfer, and could prevent their loss by intervening to halt the disbursement of money from the Bancorp account to merchants at Step 4. On one particular occasion, after identifying fraud associated with $1.9 million in duplicate redemptions by some debit card holders, InComm stepped in to prevent the cards from engaging in further transactions. InComm did so unilaterally, and indeed did not even inform Bancorp that it had done so for nearly a month. That $1.9 million was not "los[t]"; rather, it remains to this day in the InComm-earmarked account held by Bancorp.

Accordingly, InComm's loss did not occur with the Step-2 transfer of funds to the account held by Bancorp. Rather, the loss did not occur until—at Step 4—Bancorp actually disbursed money from the InComm-earmarked account to pay merchants for purchases made by cardholders. That was the point at which InComm could not recover its money. That was the point of no return.[26]

[26] *Id.* (footnote omitted).

On the temporal aspect, the court concluded that the loss in the scheme of events was not immediate:

> Far from being immediate, the loss was temporally remote: days or weeks—even months or years—could pass between the fraudulent chit redemption and the ultimate disbursement of the fraud-tainted funds from InComm's Bancorp account. And it is not just that the loss was remote in time; the chain of causation involved intervening acts and actors between the Step-1 fraud and the Step-4 loss. Even after a chit was fraudulently redeemed, each of the following had to occur: (1) InComm had to transfer money to the Bancorp account; (2) the cardholder had to make a purchase using fraudulently obtained funds; and (3) Bancorp had to disburse money from InComm's account to cover the purchase and pay the merchant. It was only at that point that InComm's loss truly materialized. The lack of immediacy—and the presence of intermediate steps, acts, and actors—makes clear that the loss did not "result[ ] directly" from the initial fraud.[27]

In *American Tooling Center, Inc. v. Travelers Cas. and Surety Co. of Am.*,[28] the insured was a tool and die manufacturer that had outsourced some of its work to another die manufacturer in China. In March 2015, the insured's President/Treasurer sent an email to his contact at the vendor located in China requesting copies of all outstanding invoices. In response, the insured received an email, purportedly from the contact, but which was actually sent by a thief. (The thief made the response email appear to be from the contact by using the "yifeng-*rn*ould.com" domain, which was apparently manufactured for the spoof and easily confused with the correct domain: "yifeng-*m*ould.com). The thief, pretending to be the vendor contact, instructed the insured to send payment for several legitimate outstanding invoices to a new bank account. Without verifying the new banking instructions, the insured wired approximately $800,000 to a bank account that was not controlled by the vendor. By the time that the fraud was detected, the funds had been transferred and the wire transfers could not be retracted.

The insured's policy provided computer crime coverage as follows: "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*."[29]

---

[27] *Id.*

[28] No. 16-cv-12108 (E.D. Mich. Aug. 1, 2017). The district court's decision in *American Tooling Center* has been appealed to the Sixth Circuit Court of Appeals, No. 17-2014 (Aug. 29, 2017), which appeal remains pending as of this writing.

[29] *American Tooling Center*, No. 16-cv-12108 (internal quotation marks omitted).

"*Computer Fraud*" was defined in the policy 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*; or
> 2. to a place outside the *Premises* or *Financial Institution Premises*.[30]

The insurer contended that the insured did not suffer a direct loss that was directly caused by the use of any computer. The district court agreed:

> Given the intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds, it cannot be said that [the insured] suffered a "direct" loss "directly caused" by the use of any computer. The Sixth Circuit, applying Michigan law, has noted that "direct" is defined as "immediate" without anything intervening. [Citation]. Rather, intervening events between [the insured's] receipt of the fraudulent emails and the transfer of funds ([the insured] 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.[31]

The district court relied on the Fifth Circuit's decision in *Apache*, discussed above, in support of its conclusion that the use of emails and computers in the fraudulent scheme were merely incidental.[32]

The district court in *American Tooling Center* also held that the fraudulent emails, without more, did not constitute the "use of any computer to fraudulently cause a transfer." Absent infiltration or hacking, the sending of bogus instructions alone were insufficient to trigger the computer fraud coverage provisions of the policy. According to the court, allowing such emails to do so, without more, would convert a crime policy into a general fraud policy:

> Although fraudulent emails were used to impersonate a vendor and dupe ATC into making a transfer of funds, such emails do not constitute the "use of any computer to fraudulently cause a transfer." 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. The Ninth Circuit has interpreted the phrase "fraudulently cause a transfer" to "require the unauthorized transfer of funds." *Pestmaster Servs., Inc. v. Travelers Casualty & Surety Co. of America*, 656 Fed. Appx. 332 (9th Cir. 2016). "Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some

[30] *Id.* (internal quotation marks omitted).
[31] *Id.* (citation and footnote omitted).
[32] *Id.*

> point in the transaction would convert this Crime Policy into a 'General Fraud' Policy." *Id. See also In[C]omm Holdings, Inc. v. Great American Ins. Co.*, . . . (N.D. Ga. Mar. 16, 2017) (noting that "courts repeatedly have denied coverage under similar computer fraud provisions, except in cases of hacking where a computer is used to cause another computer to make an unauthorized, direct transfer of property or money").[33]

In *Posco Daewoo Am. Corp. v. Allnex, Inc.*,[34] the insured supplied Allnex with product for which it was owed payment. An imposter, posing as an employee of the insured's accounts receivable department, sent fraudulent emails to Allnex requesting wire payments to four Wells Fargo bank accounts to satisfy outstanding receivables owed by Allnex to the insured. Allnex complied with the requests and wired the funds. Allnex then claimed that it had satisfied its debt obligations to the insured.

The insured sought coverage for the misplaced payments under the computer fraud coverage provisions of its crime policy. The court granted the insurer's motion to dismiss on the ground that the insured had failed to allege *ownership* of the money at issue:

> [T]he plain language of the Policy's Ownership provision limits covered property to three scenarios. The first is when [the insured] holds property for others. This provision is inapplicable here. The second is property for which [the insured] is "legally liable." Again, this is inapplicable. The final provision concerns property that [the insured] "owns or leases." Leased property is not at issue, so [the insured] only had coverage if it "own[ed]" the property, that is, if [the insured] owned the money that Allnex wired to [the thief's] Wells Fargo accounts.
>
> * * *
>
> The Court agrees with Travelers that before [the insured] actually received the monies due, [the insured] owned a receivable, or a right to payment, as well as a potential cause of action for payment if it was not made. In other words, [the insured] did "own" something of value, but it was not the cash in the Wells Fargo accounts.[35]

***

The second part of this article, which will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report*, continues the discussion of case law on the subject, discusses protocols and procedures that may be employed by companies to reduce the risk of falling victim to such scams, and suggests that companies should assess whether they have adequate coverage for these types of email phishing scams.

---

[33] *Id.*

[34] No. 17-cv-483 (D. N.J. Oct. 31, 2017).

[35] *Posco Daewoo Am. Corp.*, No. 17-cv-483 (citation omitted).