AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2018
VOL. 4 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 9 | NOVEMBER-DECEMBER 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 [281] (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.

As Email Spoofing and Hacking Continue Unabated, Courts Decide Questions of Insurance Coverage for Computer Fraud

By Jay D. Kenigsberg*

Incidents of cyber fraud affecting U.S. businesses are reaching unprecedented levels. At the same time, courts around the country are issuing more and more decisions – not all of them reaching the same result – examining whether computer fraud provisions in their insurance policies cover their losses.

The sophistication of criminal networks today knows no bounds.

Consider, for example, the international cybercrime and hacking group known as "Fin7" (also known as the "Carbanak Group" and the "Navigator Group," among other names). According to the U.S. Department of Justice,[1] three members of Fin7 operating out of Eastern Europe – Ukrainian nationals Dmytro Fedorov, Fedir Hladyr, and Andrii Kolpakov – recently were arrested and charged with 26 felony counts in the U.S. District Court for the Western District of Washington. The government alleged that they engaged in computer hacking, access device fraud, aggravated identity theft, wire fraud, and conspiracy.

Since at least 2015, the government said, Fin7 members have conducted a highly sophisticated malware campaign to attack more than 100 U.S. companies, predominantly in the restaurant, gaming, and hospitality industries. As set forth in the indictments, Fin7 has hacked into thousands of computer systems and has stolen millions of customer credit and debit card numbers. To do so, the authorities said, Fin7 carefully crafted email messages that would appear legitimate to a company's employee, and accompanied those emails with telephone calls intended to further legitimize the emails. Once an attached file was opened and activated, Fin7 would use a version of the Carbanak malware in addition to an arsenal of other tools to ultimately access and steal payment card data for the company's customers. Many of the stolen payment card numbers have been offered for sale through online underground marketplaces, according to the government.

---

* Jay D. Kenigsberg, senior counsel at Rivkin Radler LLP, represents major domestic insurance carriers in a wide variety of coverage disputes. He has handled numerous reinsurance disputes before arbitration panels and state courts and has written extensively on cyber related issues and the blockchain. Mr. Kenigsberg may be reached at jay.kenigsberg@rivkin.com.

[1] *See*, U.S. Department of Justice Press Release, "Three Members of Notorious International Cybercrime Group 'Fin7' in Custody for Role in Attacking Over 100 U.S. Companies," *available at* https://www.justice.gov/usao-wdwa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over.

In the United States alone, prosecutors said, Fin7 has successfully breached the computer networks of businesses in 47 states and the District of Columbia, stealing more than 15 million customer card records from over 6,500 individual point-of-sale terminals at more than 3,600 separate business locations. Additional intrusions occurred abroad, including in the United Kingdom, Australia, and France. Many companies have publicly disclosed hacks attributable to Fin7.

Many other individuals, operating alone or with others, engage in online fraud in an effort to steal from businesses in the United States and elsewhere. Often times, following a loss, a company that has been defrauded will seek to recover from its insurance company. As this article discusses, these claims have received varying treatment by the courts under the computer fraud provisions of the companies' insurance policies.

APACHE CORPORATION

One such decision, *Apache Corp. v. Great American Ins. Co.*,[2] was issued by the U.S. Court of Appeals for the Fifth Circuit in 2016, on appeal from the U.S. District Court for the Southern District of Texas.

The case arose in March 2013 when an employee of Apache Corporation, an oil-production company with its principal place of business in Houston, Texas, that operated internationally, 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 requested change could not be processed without a formal request on Petrofac letterhead.

A week later, Apache's accounts payable department received an email from a petrofacltd.com address. Petrofac's authentic email domain name, however, was slightly different: petrofac.com.

The email advised that Petrofac's "accounts details have now been changed" and that "[t]he new account takes . . . immediate effect and all future payments must now be made into this account." As noted in the email, an attachment to it was a signed letter on Petrofac letterhead, providing both old bank account information and the new bank account number, with instructions to "use the new account with immediate effect."

In response, an Apache employee called the telephone number provided on the letterhead to verify the request and concluded that the call confirmed the authenticity of the change request. Then, a different Apache employee approved and implemented the change.

[2] *Apache Corp. v. Great American Ins. Co.*, 662 Fed. Appx. 252 (5th Cir. 2016).

A week later, Apache was transferring funds for payment of Petrofac's invoices to the new bank account.

Within one month, however, Apache received notification that Petrofac had not received the £4.3 million (approximately $7 million) that Apache had transferred to the new (fraudulent) account. After an investigation determined that the criminals likely were based in Latvia, Apache recouped a substantial portion of the funds. It contended, however, that it suffered a loss, before the $1 million policy deductible, of approximately £1.5 million (approximately $2.4 million).

Apache submitted a claim to its insurance carrier, seeking coverage for its loss under a crime protection insurance policy's computer fraud provision, which stated:

> We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:
>
> a. to a person (other than a messenger) outside those premises; or
>
> b. to a place outside those premises.

The insurer denied Apache's claim, advising in a denial letter that Apache's loss "did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds."

Apache sued the insurer, and the parties moved for summary judgment.

The district court denied the insurer's motion and granted Apache's motion. The district court ruled, among other things, that "the intervening steps of the [post-email] confirmation phone call and supervisory approval do not rise to the level of negating the email as being a 'substantial factor'" that caused Apache's loss. Moreover, the district court reasoned, if the insurer policy only covered losses due to computer hacking, the policy would be rendered "pointless."

The insurer appealed to the Fifth Circuit. It argued that Apache's loss was not covered under the computer fraud provision of its policy because the loss did not, as required by the provision, "result[] directly from the use of any computer to fraudulently cause a transfer." According to the insurer, the transfer of funds to the fraudulent bank account resulted from other events: before the email, the telephone call directing Apache to change the account information; and, after the email, the telephone call by Apache to the criminals to confirm the change request, followed by the Apache supervisor's review and approval of the emailed request, Petrofac's submission of invoices, the review and approval of them by Apache employees, and Apache's authorized and intentional transfer of funds, even though the funds were transferred to the fraudulent bank account.

In response, Apache claimed that its loss was covered based on the "commonly understood meaning" of the computer fraud provision's terms.

THE FIFTH CIRCUIT'S DECISION

The Fifth Circuit, applying Texas law, reversed.

In its decision, the Fifth Circuit explained that the "computer use" involved in this case was an email with instructions to change a vendor's payment information and make "all future payments" to it; the email, with the letter on Petrofac letterhead as an attachment, followed the initial telephone call from the criminals and was sent in response to Apache's directive to send the request on the vendor's letterhead.

Once the email was received, the Fifth Circuit added, an Apache employee called the telephone number provided on the fraudulent letterhead in the attachment to the email, instead of, for example, calling an independently-provided telephone contact for the vendor, such as the pre-existing contact information Apache would have used in past communications. In the circuit court's opinion, had the confirmation call "been properly directed, or had Apache performed a more thorough investigation," it never would have changed the vendor's payment account information. Moreover, the Fifth Circuit continued, Apache changed the account information, and the transfers of money to the fraudulent account were initiated by Apache to pay legitimate invoices.

The email "was part of the scheme," but, the Fifth Circuit decided, the email "was merely incidental to the occurrence of the authorized transfer of money." It then stated that to interpret the computer fraud provision of the insurance policy as reaching "any fraudulent scheme in which an email communication was part of the process" would "convert the computer fraud provision to one for general fraud."

The circuit court took 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, the Fifth Circuit declared, "few – if any – fraudulent schemes would not involve some form of computer-facilitated communication."

The circuit court decided that Apache's transfers "were made not because of fraudulent information, but because Apache elected to pay legitimate invoices." The invoices, not the email, were the reason for the funds transfers, according to the Fifth Circuit. Accordingly, it concluded that Apache's loss was not a covered occurrence under the computer fraud provision of the insurance policy.

OTHER DECISIONS REJECTING COVERAGE

Numerous other court decisions have rejected coverage for similar claims under different insurance policies.

For example, the U.S. Court of Appeals for the Ninth Circuit, in *Pestmaster Services, Inc. v. Travelers Casualty and Surety Co. of America*,[3] affirmed a decision by the U.S. District Court for the Central District of California denying coverage under a computer fraud provision in a crime policy. It defined "computer fraud" as "[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property. . . ."

As the district court explained in its decision, the underlying fraud was committed by a payroll contractor against the insured. The contractor had been hired to withhold and submit payments for the insured's payroll taxes. To that end, the contractor prepared invoices for the insured and was authorized to initiate transfers of funds from the insured to the contractor's bank account to pay invoices approved by the insured.

Instead of paying the approved invoices, the contractor wrongfully used the insured's funds to pay its own obligations, ultimately leaving the insured indebted to the Internal Revenue Service for payroll taxes.

The insured sued its insurer after being denied coverage for its claim, but the district court rejected coverage under the crime policy's computer fraud provision because the "claimed losses did not 'flow immediately' and 'directly' from [the contractor's] use of a computer." According to the district court, there was "no loss when funds were initially transferred to [the contractor] because the transfers were authorized by [the insured]."

In affirming, the Ninth Circuit interpreted the phrase "fraudulently cause a transfer" in the policy's definition of computer fraud to require an "unauthorized transfer of funds." It added that, because computers are used "in almost every business transaction," reading this provision to cover all transfers that involved both a computer and fraud at some point in the transaction would convert the policy into a "General Fraud" policy.

In *Interactive Communications Int'l, Inc. v. Great American Ins. Co.*,[4] the U.S. Court of Appeals for the Eleventh Circuit analyzed whether, under Georgia law, the insured's loss had "resulted directly" from computer fraud. In that case, there was a multi-step, multi-actor process that had caused the loss.

First, the bad actors manipulated the insured's computer system essentially allowing for a double redemption of pre-paid, reloadable debit cards – this was the computer fraud.

Second, this fraud induced the insured to transfer the money to its account held by an innocent third-party intermediary.

Third, the bad actors made a purchase using the debit cards.

---

[3] *Pestmaster Services, Inc. v. Travelers Casualty and Surety Co. of America*, 656 Fed. Appx. 332 (9th Cir. 2016), *aff'g Pestmaster Services, Inc. v. Travelers Casualty and Surety Co. of America*, No. CV 13-5039-JFW (C.D. Cal. July 17, 2014).

[4] *Interactive Communications Int'l, Inc. v. Great American Ins. Co.*, No. 17-11712, 731 Fed. Appx. 929 (11th Cir. May 10, 2018).

Fourth, the third party deducted the amount of the purchase from the insured's account.

The Eleventh Circuit reasoned that even though the insured had transferred the money at step two, it had retained control over the money until after the fourth step. Thus, the circuit court ruled, the computer fraud occurred at step one; but "the point of no return" after which the money had left the control of the insured occurred not at step two – when it transferred the money to the third-party intermediary – but after step four.

The Eleventh Circuit concluded that "[t]he lack of [temporal] immediacy" and "the presence of intermediate steps, acts, and actors" meant "that the loss did not 'result[] directly'" from the computer fraud.

In *Brightpoint, Inc. v. Zurich American Ins. Co.*,[5] the U.S. District Court for the Southern District of Indiana ruled that similar policy language did not cover a loss claimed by an insured distributor of prepaid mobile telephone cards.

In that case, a distributor received a facsimile transmission of purchase orders, post-dated checks, and bank guarantees from a purported customer, and then delivered the inventory in exchange for the original documents. The transaction was a fraud, with the distributor never receiving payment.

The district court assumed, without deciding, that the facsimile transmission constituted "use of a computer." In concluding that the loss was not covered, the district court stated:

> We do not view the faxed [documents] to have "fraudulently cause[d] a transfer" of the phone cards, as required under the policy definition of "Computer Fraud." . . . [T]he facsimile simply alerted the [insured] to the fact that [the insured's customer], or perhaps in this case some other person mimicking his methods, wished to place an order. Only after [the insured] received the physical documents would [it] release the phone cards and, based on established practices of [the insured], the cards would not have been turned over simply on the basis of the facsimile.

Another case was decided by the U.S. District Court for the Northern District of Texas. In *Great American Ins. Co. v. AFS/IBEX Financial Services, Inc.*,[6] an employee of the insured, an insurance premium finance company, used a computer to submit more than 100 false loan applications to induce the insured to issue checks that the employee deposited for personal use. The insured's claim with its insurer sought coverage under the computer fraud provision of a crime protection insurance policy that covered a loss

---

[5] *Brightpoint, Inc. v. Zurich American Ins. Co.*, No. 1:04-CV-2085-SEB-JPG, 2006 U.S. Dist. LEXIS 26018 (S.D. Ind. March 10, 2006).

[6] *Great American Ins. Co. v. AFS/IBEX Financial Services, Inc.*, No. 3:07-CV-924-O, 2008 U.S. Dist. LEXIS 55532 (N.D. Tex. July 21, 2008).

"resulting directly from the use of any computer to fraudulently cause a transfer of . . . property."

The insurer denied the claim and the court determined that the loss was not covered under this provision. It interpreted the policy language as being "designed to cover losses *directly* stemming from fraud perpetrated by use of a computer."

AMERICAN TOOLING

Two circuit courts in recent months have *found* coverage under insurance policies at issue, under similar circumstances.

American Tooling Center, Inc. v. Travelers Casualty and Surety Co. of America[7] involved American Tooling Center, Inc. ("ATC"), a tool and die manufacturer in Michigan that subcontracted some of its manufacturing work to Shanghai YiFeng Automotive Die Manufacture Co., Ltd. ("YiFeng"), a vendor in China.

According to the decision by the U.S. Court of Appeals for the Sixth Circuit, to be paid for its work, YiFeng emailed invoices to ATC. After receiving an invoice from YiFeng, ATC employees verified that YiFeng had completed the necessary steps required for payment. Each week, ATC's treasurer reviewed a physical spreadsheet of the outstanding accounts payable and determined the bills that needed to be paid that week. ATC paid YiFeng and its other international vendors via wire transfer. To initiate a wire transfer, ATC's treasurer signed into a banking portal using software on his computer. He manually entered the payee's name, banking information, and the amount to be wired. After the treasurer submitted the wire transfer request, ATC's assistant comptroller had to log into the banking portal using his computer to approve it. The court noted the following pertinent facts:

- On March 18, 2015, the ATC treasurer emailed a YiFeng employee requesting that YiFeng provide ATC all outstanding invoices. An unidentified third party intercepted this email. This third party, impersonating the YiFeng employee, then began a correspondence with the ATC treasurer about the outstanding invoices.
- On March 27, 2015, the impersonator emailed the ATC treasurer and claimed that, due to an audit, ATC should wire its payments to a different account from usual. ATC wired the money to the new account.
- On April 3, the impersonator emailed the ATC treasurer and informed him that "due to some new bank rules in the province," the previous wire transfer had not been credited to its account and it would return the payment. The impersonator requested that ATC instead wire the money to a different bank account. ATC's treasurer wired the money to this new account on April 8, 2015.

[7] *American Tooling Center, Inc. v. Travelers Casualty and Surety Co. of America*, 895 F.3d 455 (6th Cir. 2018).

The impersonator ran the scam two more times and ATC wired additional payments of $1,575 and $482,640.41 on April 9, 2015 and May 8, 2015.

According to the court, when the real YiFeng demanded payment, ATC realized it had wired the money to an imposter. ATC paid YiFeng approximately 50 percent of the outstanding debt and agreed that the remaining 50 percent would be contingent on ATC's ability to recover from its insurer.

ATC submitted a claim for its loss to its insurer, arguing that it fell within the computer fraud provision of a business insurance policy, but its insurer denied the claim. ATC subsequently sued its insurer for breach of contract.

The U.S. District Court for the Eastern District of Michigan granted summary judgment to the insurer, holding that ATC's loss was not covered under the policy.

ATC appealed to the Sixth Circuit, arguing that its loss was a result of computer fraud, a type of computer crime covered by its insurer's policy.

The Sixth Circuit's Decision

The Sixth Circuit reversed, finding that ATC's loss was covered by the insurer's policy.

In its decision, the circuit court noted that the policy stated:

> 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**.

It then found that ATC had suffered a "direct loss" within the meaning of the policy's computer fraud provision. The circuit court opined that ATC "immediately" lost its money when it transferred the approximately $834,000 to the impersonator; and that "there was no intervening event."

The circuit court also opined that whether ATC had contractually owed that money to YiFeng and the two parties later agreed to spread the loss between them had "no bearing on whether this loss was directly suffered by ATC."

The Sixth Circuit then ruled that the impersonator's conduct constituted computer fraud, defined by the policy to mean:

> 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**.

The Sixth Circuit opined that *Pestmaster* was distinguishable, principally on its facts. It stated that the fraud in *Pestmaster* occurred when the company Pestmaster hired to

handle its payroll tax services, and to which it had granted electronic access to its bank account, failed to pay the taxes and kept the money instead.

By contrast, the Sixth Circuit determined, an impersonator sent ATC fraudulent emails using a computer "and these emails fraudulently caused ATC to transfer the money to the impersonator." The policy did not require that the fraud "cause any computer to do anything."

The Sixth Circuit ruled that ATC's "direct loss" was caused by computer fraud which "was an immediate cause of its loss."

MEDIDATA

The U.S. Court of Appeals for the Second Circuit reached a similar conclusion in *Medidata Solutions Inc. v. Federal Ins. Co.*,[8] affirming a decision by the U.S. District Court for the Southern District of New York.[9]

The case involved Medidata Solutions Inc., a provider of cloud-based services to scientists conducting research in clinical trials. In September 2014, a Medidata employee in the company's accounts payable department responsible for processing all of Medidata's travel and entertainment expenses received an email purportedly sent from Medidata's president. The email message contained the president's name, email address, and picture in the "From" field and stated that Medidata was close to finalizing an acquisition and that an attorney named Michael Meyer would contact her. The email advised the Medidata employee that the acquisition was strictly confidential and instructed her to devote her full attention to Meyer's demands.

On that same day, the Medidata employee received a phone call from a man who held himself out to be Meyer. Meyer demanded that the Medidata employee process a wire transfer for him. She told Meyer that she needed an email from Medidata's president requesting the wire transfer and approval from Medidata's vice president and director of revenue.

After receiving an email purportedly sent from Medidata's president, the Medidata employee logged on to the company's online bank account to initiate a wire transfer. She entered the banking information provided by Meyer and submitted the wire transfer for approval. Medidata's vice president and director of revenue logged on to the company's online banking system and approved the wire transfer. Thereafter, $4,770,226.00 was wired to the bank account provided by Meyer.

[8] *Medidata Solutions Inc. v. Federal Ins. Co.*, 729 Fed. Appx. 117 (2d Cir. 2018).
[9] *Medidata Solutions, Inc. v. Federal Ins. Co.*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017).

Medidata subsequently realized that it had been defrauded. Medidata contacted the FBI and hired outside counsel to conduct an investigation, which revealed that an unknown actor had altered the emails to appear as if they had been sent from Medidata's president.

Medidata sought coverage for its loss from its insurer under the computer fraud provision of its insurance policy, which covered the "direct loss of Money, Securities or Property" sustained by Medidata "resulting from Computer Fraud committed by a Third Party." The policy defined "Computer Fraud" as "the unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation," which was defined to include 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 [Medidata]."

The insurer denied Medidata's claim under the computer fraud provision of its policy, reasoning that there had been no "fraudulent entry of Data into Medidata's computer system."

Medidata sued, arguing that the policy's computer fraud clause covered its loss because a thief fraudulently entered and changed data in Medidata's computer system. Specifically, Medidata asserted that the address in the "From" field of the spoofed emails constituted data that was entered by the thief posing as Medidata's president. Also, a thief entered a computer code that caused the hacker's email address to "change" to the Medidata president's email address.

The insurer argued that Medidata's loss was not covered by the computer fraud clause because the emails did not require access to Medidata's computer system, a manipulation of those computers, or input of fraudulent information.

The district court concluded that, as a matter of law, the "unambiguous language" of the computer fraud clause provided coverage for the theft from Medidata.

The district court opined that the theft had occurred "by way of email spoofing," and it rejected the insurer's contention that there was "no direct nexus" between the spoofed emails and the fraudulent wire transfer. Instead, the district court found that Medidata employees "only initiated the transfer as a direct cause of the thief sending spoof emails posing as Medidata's president."

Accordingly, it concluded, Medidata demonstrated that its losses were a direct cause of a computer violation, and it granted summary judgment in favor of Medidata.

The Second Circuit's Decision

In a summary order, the Second Circuit affirmed, agreeing with the district court that the "plain and unambiguous language" of the policy covered Medidata's losses.

The circuit court reasoned that fraudsters had crafted a computer-based attack that manipulated Medidata's email system, which constituted a "computer system" within the meaning of the policy. The circuit court added that the spoofing code enabled the fraudsters to send messages that inaccurately appeared, in all respects, to come from a high-ranking member of Medidata's organization. Thus, it found, the attack represented a fraudulent entry of data into the computer system, as the spoofing code was introduced into the email system. The attack also made a change to a data element, as the email system's appearance was altered by the spoofing code to misleadingly indicate the sender.

The Second Circuit also decided that Medidata had sustained a "direct loss" as a result of the spoofing attack, within the meaning of the policy. According to the circuit court, the spoofed emails directed Medidata employees to transfer funds, and the employees made the transfer that same day. The Second Circuit acknowledged that Medidata employees had to take action to effectuate the transfer, but said that their actions were not sufficient "to sever the causal relationship between the spoofing attack and the losses incurred."

Accordingly, it ruled, Medidata's losses were covered by the terms of the computer fraud provision in the policy.

CONCLUSION

As the decisions discussed in this article suggest, courts across the country have reached different conclusions when asked to decide whether different insurance policies cover losses suffered by insureds under a variety of different, albeit similar, factual circumstances. Courts are likely to continue to struggle with insurance coverage issues in these cases, but one thing is clear. More and more criminals in the United States and around the world undoubtedly will continue to try to defraud U.S. businesses using methods such as email spoofing and hacking for quite some time to come.