Westlaw Journal
PROFESSIONAL LIABILITY
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 27, ISSUE 10 / MARCH 2018

## WHAT'S INSIDE



## PROFESSIONAL LIABILITY

# Lawyer's error after botched prenup started new clock for claims, Minnesota high court says

**By Thomas Parry**

A divorced Minnesota man with an invalid prenuptial agreement can sue his attorney for malpractice even though the limitations period stemming from the original drafting of the agreement expired, the state's highest court has ruled.

***Frederick v. Wallerich et al., No. A15-2052, 2018 WL 735829 (Minn. Feb. 7, 2018).***

In reversing a lower court decision, the Minnesota Supreme Court ruled 5-2 that attorney Kay Wallerich's alleged subsequent failure to alert her client that the prenuptial was void constituted an independent negligence claim that triggered a new limitations period.

The client adequately alleged a timely legal malpractice claim based on the later alleged negligence, Justice Natalie E. Hudson said in an opinion for the majority.


CONTINUED ON PAGE 10

## EXPERT ANALYSIS

# Insurance coverage for social engineering fraud

Ken Kronstadt of Kelley Drye & Warren surveys recent court rulings on insurance coverage for losses resulting from social engineering fraud and other computer-related scams, and he offers advice for policyholders to increase the likelihood the claim will be paid.

SEE PAGE 3

## EXPERT ANALYSIS

# Cyberclaims and litigation against insurance professionals

Robert A. Stines of Freeborn & Peters analyzes the potential for suits against insurance professionals who do not properly advise their clients about the threat of cyberattacks.

SEE PAGE 7

42089595

THOMSON REUTERS™
Westlaw®

**Westlaw Journal Professional Liability**

Published since September 1991

**Director:** Nadia Abadir

**Editors:** Susan A. Aase, Esq.
Susan.A.Aase@thomsonreuters.com

Aaron A. Rolloff

**Desk Editors:**
Jennifer McCreary, Elena Neuzil, Katie Pasek, Sydney Pendleton, Abbie Sarfo, Maggie Tacheny

**Graphic Designers:**
Nancy A. Dubin, Ramona Hunter

**Westlaw Journal Professional Liability**
(ISSN 2155-6016) is published monthly by Thomson Reuters.

**Thomson Reuters**
175 Strafford Avenue, Suite 140
Wayne, PA 19087
877-595-0449
Fax: 800-220-1640
www.westlaw.com
Customer service: 800-328-4880
For more information, or to subscribe, please call 800-328-9352 or visit legalsolutions.thomsonreuters.com.

**Reproduction Authorization**
Authorization to photocopy items for internal or personal use, or the internal or personal use by specific clients, is granted by Thomson Reuters for libraries or other users registered with the Copyright Clearance Center (CCC) for a fee to be paid directly to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923; 978-750-8400; www.copyright.com.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner.

# TABLE OF CONTENTS




© 2018 Thomson Reuters

# Insurance coverage for social engineering fraud

**By Ken Kronstadt, Esq.**
***Kelley Drye & Warren***

Social engineering fraud occurs when a scammer tricks a company employee into transferring funds, often by sending an email impersonating a vendor, client or executive of the targeted company. In these increasingly common schemes, the email says the vendor or client's banking information has changed or that the company must immediately wire funds "at the executive's direction."

The emails appear to be authentic because they duplicate the targeted company's logo, look and feel. As part of the scammers' effort to escape detection, they also often use an email domain that differs only slightly from the legitimate domain they are attempting to disguise.

Due to these or similar techniques, target companies have sustained millions of dollars in losses when unsuspecting employees unwittingly comply with the instructions.

Companies seeking coverage for social engineering fraud most often look to their crime/fidelity policy. Insurers often take the position that the loss did not result from a "direct" fraud, saying the loss was caused by the company's intervening actions.

While recent court decisions have been mixed, the overall trend has favored insurers. Given this trend and its impact on a company's bottom line, savvy companies should carefully review their traditional crime/fidelity policies and the increasingly prevalent cyber risk/liability policies to ensure coverage for loss from social engineering fraud.

### *Apache Corp. v. Great American Insurance Co.*

In an October 2016 opinion that insurers often cite in lawsuits related to social engineering fraud, the 5th U.S. Circuit Court of Appeals denied coverage to Apache Corp. for $1.5 million in losses sustained after company employees routed vendor payments to a phony bank account.[1]

> Social engineering fraud occurs when a scammer tricks a company employee into transferring funds, often by sending an email impersonating a vendor, client or executive of the targeted company.

A person identifying herself as an employee of Petrofac, an Apache vendor, called and instructed Apache to change its bank account information for payments to Petrofac. An Apache employee stated that the company would need a formal request on Petrofac letterhead.

A week later, Apache's accounts payable department received an email from a petrofacltf.com domain (the real domain was petrofac.com) instructing them to use a new bank account for future payments. A signed letter on Petrofac letterhead with similar instructions was attached to the email.

An Apache employee called the number on the letterhead to verify the request, and a different Apache employee approved and implemented the change.

A week later, Apache transferred funds to the new bank account for payment of Petrofac invoices. Within a month, Petrofac notified Apache that it had not received nearly $7 million that was due.

Apache submitted a claim to Great American, which had issued it a commercial crime policy.

The policy's computer fraud provision stated that Great American "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 ... to a person ... outside those premises" or "to a place outside those premises."

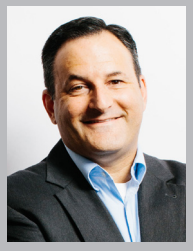
The trial court ruled in Apache's favor, but the 5th Circuit reversed.

Focusing on the fact that the computer fraud provision required that loss result "directly" from the use of a computer to cause a fraudulent transfer, the court stressed that the computer fraud provision was not intended to reach every fraudulent scheme in which an email communication was part of the process.

The court noted that the fraudulent email was merely incidental to the occurrence of the authorized transfer of money, since the fraudulent transfer occurred "only because, after receiving the email, Apache failed to investigate accurately the new, but fraudulent, information provided to it."

### *Medidata Solutions v. Federal Insurance Co.*

Last July a New York federal judge held that Medidata Solutions Inc. was entitled to coverage after company employees were duped into wiring money overseas by an imposter posing as the company's president via email.[2]



**Ken Kronstadt** is a senior associate at **Kelley Drye & Warren** in Los Angeles, where he is a member of the firm's insurance recovery group. He concentrates his practice in the areas of insurance coverage litigation and counseling in the construction and entertainment industries, and he has in-depth knowledge of insurance coverage for emerging cybersecurity and data privacy-related events.

© 2018 Thomson Reuters

An accounts payable employee, Alicia Evans, received an email purportedly sent from Medidata's president, bearing his name, email address and picture. The message said the company was finalizing an acquisition, that an attorney named Michael Meyer would contact Evans, and that she should devote her full attention to his demands.

Later that day, Evans received a phone call from "Meyer," demanding that she process a wire transfer. Evans explained she would need an email from Medidata's president requesting the wire transfer and approval from Medidata's vice president, Ho Chin, and director of revenue, Josh Schwartz.

Chin, Evans and Schwartz then received an email purportedly sent by Medidata's president instructing Evans to complete the wire transfer.

Evans then initiated the transfer, which Schwartz and Chin approved. Nearly $4.8 million was wired to the bank account provided by Meyer and, two days later, Meyer requested a second wire transfer.

Thinking that the email address in the "reply to" field seemed suspicious, Chin spoke to Evans, who sent an email to Medidata's president inquiring about the wire transfers. The president said he had not requested the transfers and the employees then realized the company had been defrauded.

Medidata submitted a claim to Chubb Ltd., which had issued the company a crime policy.

Finding the 5th Circuit's decision in *Apache* unpersuasive, the District Court ruled in favor of Medidata under two separate policy provisions.

First, it deemed the loss covered under the computer fraud coverage provision, which protected against the "direct loss of money, securities or property sustained by an organization resulting from computer fraud committed by a third party."

The court concluded that, while Medidata's computers were not directly hacked by a third party, the requirements of the provision were still met because the thief gained entry into Medidata's email system with spoofed emails.

These emails were also armed with a computer code that masked his true identity and made the emails appear as though they originated from Medidata's president.

The court also deemed the loss covered under the policy's funds transfer fraud coverage provision, which protected against "direct loss of money or securities sustained by an organization resulting from funds transfer fraud committed by a third party."

Chubb had argued that the wire transfer was voluntary and made with Medidata's knowledge and consent.

The court rejected this argument, stating that "the fact that [Evans] willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction" or a voluntary one. "Larceny by trick is still larceny," it said.

The court held that the fraudulent emails did not "directly" or "immediately" cause American Tooling to transfer funds from its bank account.

Rather, the court found that American Tooling took several steps between when it received the fraudster's emails and when it transferred the funds, such as verifying production milestones, authorizing the transfers and initiating the transfers without verifying bank account information. As a result, the court could not find a loss "directly caused" by the use of any computer.

Whether a company is able to obtain coverage for social engineering fraud under a crime/fidelity policy will depend largely on the precise language of the company's policy.

### *American Tooling Center v. Travelers Casualty & Surety Co.*

Relying in part on *Apache*, a Michigan federal court ruled in August 2017 that Travelers Casualty & Surety Co. was not obligated to cover American Tooling Center Inc.'s losses resulting from a fraudulent, email-based scheme.[3]

American Tooling outsourced some of its work to manufacturing companies overseas, one of which was YiFeng Automotive Die Manufacture Co. American Tooling Vice President/Treasurer Gary Gizinski sent an email to his contact at YiFeng, requesting copies of all outstanding emails.

Gizinski received a response from a scammer using the domain "yifeng-rnould," which is easily confused with the correct domain,"yifeng-mould.com." The scammer instructed American Tooling Center to send payment for several invoices to a new bank account.

Without verifying the new banking instructions, American Tooling wired $800,000 to a bank account not controlled by YiFeng. After the fraud was discovered, the money could not be recovered.

American Tooling sought coverage for the loss from Travelers, which issued American Tooling a policy covering "computer crime," in which Travelers would pay American Tooling for its "direct loss of, or direct loss from damage to, money, securities and other property directly caused by computer fraud."

### *Principle Solutions Group v. Ironshore Indemnity*

Less than a year before *Medidata*, a Georgia federal court found that Ironshore Indemnity Co. was required to cover a $1.7 million loss from a transfer resulting from a fraudulent scheme similar to that in *Medidata*.[4]

In the case, Principle Solutions Group's controller received an email from a person purporting to be Josh Nazarian, one of the company's managing directors. The email referenced a company acquisition and instructed the controller to "treat the matter with the utmost discretion" and to work with an attorney, Mark Leach, to ensure that the wire went out that day.

Later that morning, the controller received an email from a "Mark Leach," who represented himself as a partner at Alston & Bird. The email said "Leach" was reaching out at Nazarian's request, and it included instructions for wiring the funds to a bank in China.

The controller approved the wire transfer after Leach called the controller to stress that they needed to complete the transaction that day. The financial institution's fraud prevention unit called the controller for verification and, after being told that Leach had verbally received the wire instructions from Nazarian, released the transfer.

When the controller spoke with Nazarian the next day, the pair realized the company had been defrauded. Nazarian immediately called the financial institution's fraud


© 2018 Thomson Reuters

department, but the company could not recover the $1.7 million.

Principle sought coverage from Ironshore, which had issued a commercial crime policy providing "computer and funds transfer fraud" coverage for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit your 'transfer account' and transfer, pay or deliver 'money' or 'securities' from that account."

Ironshore argued that the loss did not result "directly" from a fraudulent instruction because Leach conveyed additional information for the wire transfer after the initial email and Principle's employees set up and approved the transfer.

The court found the policy language was ambiguous, either requiring an immediate link between the injury and its cause, as Ironshore contended, or providing coverage even if there were intervening events between the fraud and the loss.

As courts commonly do when deeming policy language ambiguous, the court construed the policy in the light most favorable to the insured and found for Principle.

Notably, in its August 2016 opinion, the *Principle Solutions* court relied on the *Apache* trial court opinion to support its positon. As discussed above, however, the 5th Circuit reversed that trial court opinion in October 2016, less than two months after *Principle Solutions* was decided.

### *Pestmaster Services v. Travelers Casualty & Surety Co.*

In a case involving computer fraud coverage but not social engineering fraud, the 9th U.S. Circuit Court of Appeals held that there was no coverage for a fraudulent scheme resulting in losses that did not flow "immediately" and "directly" from the use of a computer.[5]

In *Pestmaster*, a payroll contractor of the insured, Priority 1 Resource Group, was hired to withhold and submit payments for the insured's payroll taxes. Priority 1 prepared invoices for Pestmaster Services Inc. and was authorized to initiate transfers of funds from Pestmaster's bank account to Priority 1's bank account to pay invoices approved by the insured.

Instead of paying the approved invoices, Priority 1 fraudulently used Pestmaster's funds to pay Priority 1's own expenses, leaving Pestmaster indebted to the IRS for payroll taxes.

After Travelers denied coverage, Pestmaster brought suit against the insurer, which had issued a "crime plus wrap" policy to Pestmaster that included, in pertinent part, a computer crime insuring agreement covering "direct loss of, or your direct loss from damage to, money, securities and other property directly caused by 'computer fraud.'"

The District Court sided with Travelers, finding the "claimed losses did not 'flow immediately' and 'directly' from Priority 1's use of a computer" because they did not occur until after the transfer, when Priority 1 used the funds to pay its own obligations rather than Pestmaster's federal payroll taxes.[6]

The 9th Circuit affirmed, reasoning that the phrase "fraudulently cause a transfer" required an unauthorized transfer of funds, and no such unauthorized transfer occurred because Pestmaster authorized the transfer to Priority 1.

"Because computers are used in almost every business transaction," the court wrote, "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," essentially covering losses from all forms of fraud rather than a specified risk category.

Several other notable cases have similarly denied coverage outside the context of social engineering fraud where a company was victimized through the incidental, rather than direct, use of a computer.

For example, courts have held in the insurers' favor where users exploited a loophole in a prepaid debit card authorization process using a telephone to redeem funds, resulting in a behind-the-scenes interaction with a computer and causing losses of over $10 million.

They have also denied coverage where a company offering health insurance to Medicare-eligible individuals sustained losses of over $18 million for payment of fraudulent claims for medical services that were falsely entered into a computer system as having been performed.[7]

## SECURING COVERAGE

Whether a company is able to obtain coverage for social engineering fraud under a crime/fidelity policy will depend largely on the precise language of the company's policy. Even a slight variance in policy language can have a dramatic impact on coverage.

As the cases discussed above illustrate, even where a crime/fidelity policy requires that loss be caused "directly" by fraud, courts have reached inconsistent conclusions on the coverage question. It is possible, as in *Medidata* and *Principle Solutions,* that a court will afford coverage even when intervening acts separate the fraudulent conduct and the loss sustained.

A company looking to ensure coverage should not assume that a court will rule in its favor on these issues. As of now no cases have relied on *Medidata*'s holding to find coverage, and two cases have declined to follow *Medidata*.[8]

As discussed above, *Principle Solutions* relied in large part on the trial court ruling in *Apache*, which was reversed less than two months after the *Principle Solutions* court issued its opinion.

> Because courts have yet to address coverage for social engineering fraud under cyberliability policies, and given the lack of uniformity in policy language, it is difficult to predict how a court will decide coverage.

More cases have denied than granted coverage for social engineering fraud where the crime/fidelity policy required that the loss be caused "directly" by fraud. These decisions reasoned that intervening actions between the fraud and the loss negated coverage.

Given the increasing demand to insure against social engineering fraud risks, some insurers have begun to offer policy endorsements specifically providing coverage for these claims.

Policyholders should scrutinize the language of these endorsements. They may be subject to a sublimit; they may cover some, but not all social engineering fraud risks; and they may be subject to additional exclusions.

Companies seeking coverage for social engineering fraud claims may also wish to consider a cyberliability insurance policy. Although these policies are often more

© 2018 Thomson Reuters

specifically tailored to cover data breaches and similar events, there is no "standard" cyberliability insurance form, and the types of coverages available often differ drastically from insurer to insurer.

Many cyberliability policies exclude "voluntary parting" or "voluntary payments," that is, losses flowing from the insured's voluntary transfer of money to a third party. Though these exclusions would bar coverage where an employee is tricked into wiring money, savvy companies can specifically request coverage for social engineering fraud for only a nominal additional premium.

## CONCLUSION

Simply obtaining a crime/fidelity or cyberliability policy does not ensure coverage if a company falls prey to social engineering fraud. The specific language used in a company's individual policy will always determine coverage.

As the cases above illustrate, where a crime/fidelity policy requires "direct" causation — as many often do — it appears somewhat more likely that a court will deny coverage for social engineering fraud where there are intervening actions between the fraud and the loss sustained. In light of *Medidata*'s holding, however, policyholders have legitimate grounds to argue for coverage.

Given the significant differences in the policy forms issued across the cyberliability market, even where social engineering fraud fits within the coverage grant under some policies, a "voluntary parting" or "voluntary payments" exclusion may preclude coverage.

Because courts have yet to address coverage for social engineering fraud under cyberliability policies, and given the lack of uniformity in policy language, it is difficult to predict how a court will decide coverage.

In the face of this uncertainty, policyholders should get an endorsement specifically designed to provide social engineering fraud coverage under either a crime/fidelity or cyber risk policy.

Because these types of endorsements are so new however, policyholders need to carefully scrutinize their wording to make sure they cover the types of social engineering fraud risks the company may face. WJ

## NOTES

[1] *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. App'x 252 (5th Cir. 2016).

[2] *Medidata Solutions Inc. v. Fed. Ins. Co.*, No. 15-cv-907, 2017 WL 3268529 (S.D.N.Y. July 21, 2017).

[3] *Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am.*, No. 16-cv-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017).

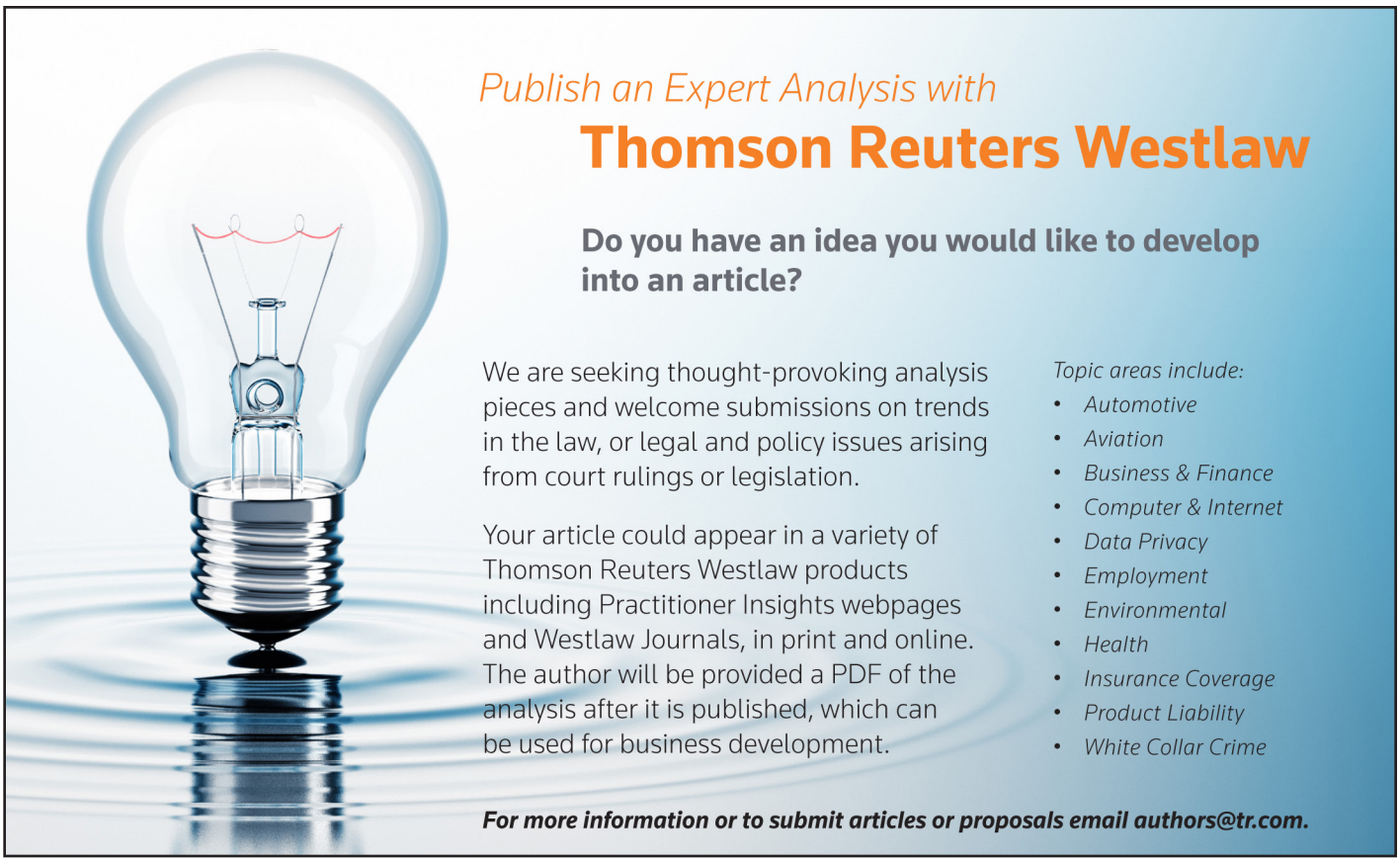
[4] *Principle Solutions Grp. LLC v. Ironshore Indem.*, No. 15-cv-4130, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016).

[5] *Pestmaster Servs. v. Travelers Cas. & Sur. Co. of Am.*, 656 Fed. App'x 332 (9th Cir. 2016).

[6] *Pestmaster Servs. v. Travelers Cas. & Sur. Co. of Am.*, No. 13-cv-5039, 2014 WL 3844627 (C.D. Cal. July 17, 2014).

[7] *InComm Holdings Inc. v. Great Am. Ins. Co.*, No. 15-cv-2671, 2017 WL 1021749 (N.D. Ga. Mar. 16, 2017); *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 37 N.E.3d 78 (N.Y. 2015).

[8] *See Am. Tooling*, 2017 WL 3263356; *Posco Daewoo Am. Corp. v. Allnex USA Inc.*, No. 17-cv-483, 2017 WL 4922014 (D.N.J. Oct. 31, 2017).




© 2018 Thomson Reuters

# Cyberclaims and litigation against insurance professionals

**By Robert A. Stines, Esq.**
***Freeborn & Peters***

Technology such as cloud computing, machine learning, the "internet of things" and autonomous vehicles are changing society. Along with these rapid societal changes, cyberthreats are evolving more quickly than chief information security officers can deploy systems to anticipate and prevent breaches. While these breaches were once considered threats only for larger corporations, they since have become problems for smaller companies and individuals as well.

This increased risk of cyberevents presents a fertile market for the insurance industry to create new products. Insurance professionals who aim to serve the needs of their corporate clients (whether large or small) must market and provide advice about these new products.

The numerous vectors for cyberattacks — and the uncertainty surrounding how these new insurance products will respond to cyberclaims — has increased the risk of litigation against insurance professionals.

This analysis will briefly discuss uncertainty related to cyberinsurance policies, litigation against insurance agents and brokers, the evolving duty to advise clients about cyberinsurance, and risk management considerations to avoid litigation.

## CYBERINSURANCE POLICIES

Although there are exceptions, courts have generally decided that commercial general liability insurance does not cover cyberevents. To avoid confusion, many insurance carriers now affirmatively exclude cyberclaims from CGL policies.

Carriers are clearly communicating to insureds that they must obtain separate coverage addressing today's cyber risks in the form of cyberinsurance policies.

Unfortunately, the language in these policies is not standardized and is customizable depending on the carrier. Claims filed under them are frequently challenged in court, and each new court decision provides some answers — but also more confusion.

> The Medidata and American Tool cases illustrate the lack of agreement regarding what is and what is not covered under cyber-related policies.

Confusion regarding coverage can easily arise when a social engineering vector causes an insured to wire funds to unintended recipients. A vector is the term used in the cybersecurity industry to describe the method of a cyberattack. Is the attack a cyberevent, criminal fraud, employee error or all of the above?

In *Medidata Solutions v. Federal Insurance Co.*, through a sophisticated scheme of spoofed emails, a Medidata employee was tricked into wiring $4.8 million to an overseas account. Medidata held a $5 million insurance policy with Federal. The policy contained a "crime coverage section" addressing loss caused by various criminal acts, including computer fraud coverage and funds transfer fraud coverage.[1]

Relying on the policy, Federal 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.

In challenging causation, Federal argued that "there is no direct nexus" between the spoofed emails and the fraudulent wire transfer. The insurer also challenged coverage under the funds transfer fraud clause because the bank wire transfer was voluntary and with Medidata's knowledge and consent.

The court explained that "a thief sent spoofed emails armed with a computer code into the email system that Medidata used." To achieve the spoof, the thief's computer code changed data in email addresses. The fraud tricked several high-level employees to consent to the wire transfers out of Medidata's own bank account.

Ultimately, the court found coverage under the computer fraud clause and funds transfer fraud clause.

In a similar case, Travelers prevailed in a computer fraud claim case against its policyholder, American Tooling Center Inc.[2] After receiving emails that appeared to be from one of its vendors, ATC authorized payments to a bank account it believed belonged to the vendor. But the emails were fraudulent, and the fraudsters received the payments.

ATC sought coverage from Travelers under the computer fraud provision of its policy. Travelers argued ATC did not incur a covered loss under the policy. Specifically, it contended "computer fraud" encompasses a digital attack vector that causes loss but

**Robert A. Stines** is a partner at **Freeborn & Peters** in Tampa, Florida. He is a trial lawyer focused on defending professionals against malpractice and errors-and-omissions claims. A part of his practice is concentrated on legal issues created by emerging technologies. He can be reached at rstines@freeborn.com.

© 2018 Thomson Reuters

does not encompass the use of a digital vector to defraud the organization through an employee's behavior.

The court decided that although spoofed emails were used to impersonate a vendor and dupe ATC into transferring funds, they did 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 funds transfer; rather, ATC authorized the transfer based upon the information received in the emails. Hence, the court ruled that Travelers was not liable for losses from an email-based theft scheme.

The Medidata and American Tool cases illustrate the lack of agreement regarding what is and what is not covered under cyberrelated policies. Underwriters and courts are still grappling with what is considered a "cyberclaim." This creates a significant problem for insurance professionals who offer cyberinsurance policies to clients.

## LITIGATION AGAINST INSURANCE PROFESSIONALS

Though it did not involve a sophisticated cyberevent, the fallout from a data breach experienced by Perpetual Storage, a Colorado Casualty Insurance Co. insured, illustrates the exposure insurance professionals may face.

Perpetual Storage stored certain records, including hard copies, microfilm, microfiche and magnetic computer tape on behalf of the University of Utah. Backup tapes containing personal information of 1.7 million patients were stolen from a Perpetual Storage employee's car.

The university said the theft caused it to incur more than $3 million in costs, consisting of one year of credit monitoring expenses for each impacted patient, printing and mailing costs, phone bank costs, and other miscellaneous expenses.

Colorado Casualty filed a declaratory judgment action contending that Perpetual Storage's policy did not cover the university's credit monitoring expenses or notice costs. Perpetual Storage file a third-party claim against its insurance broker alleging, among other things, negligent procurement of insurance, breach of fiduciary duty and failure to advise.[3]

After three years of litigation, the parties stipulated to a dismissal of all claims, counterclaims, cross-claims and third-party claims.

In 2011 an Illinois corporation engaged in electronic commerce sued its insurance broker alleging reduced revenues for a period of seven months due to a cyberattack that destroyed the corporation's electronic commerce capability. The agent procured a policy that included "business income extension for websites" coverage for only the first seven days of lost revenue.

> An exception to the general rule of no duty to advise applies if a "special relationship" exists between the broker and the client.

The corporation filed claims against the insurance broker for negligence and breach of contract.[4] After several years of litigation, this case also ended with a dismissal by stipulation.

In a 2016 case, a Louisiana hotel alleged breach of contract, disputing the coverage limit of a cybersecurity policy issued through underwriters at Lloyd's of London. The hotel also named the insurance agent in the suit.

The hotel alleged that when it sought cyberinsurance coverage, it required a policy that would cover operational fraud and operational reimbursement amounts for fraudulent charges and the cost of replacing payment cards as a result of a cyberattack.

The agent procured a policy with total policy limits of $3 million; however, unbeknownst to the hotel, the policy contained a sub-limit of $200,000 for operational fraud and operational reimbursement amounts.

The retail agent filed a third-party claim against the wholesale broker who claimed to have specialized in cyberpolicies.[5] The parties quickly resolved the dispute and filed a joint motion to dismiss, which the court granted.

These cases are examples of situations in which a policy to cover cyberexposure was warranted based on the client's business operations. But what if the insured does not specifically request a cyberinsurance policy?

If every company, large or small, is theoretically at risk of a cyberbreach, then insurance professionals may have an affirmative duty to advise corporate clients about cyber risks and available coverage.

## DUTY TO ADVISE

Generally, an insurance agent or broker who undertakes to procure insurance for another and fails to do so may be held liable for damages resulting from the failure. As a general proposition, insurance agents and brokers do not have a duty to advise insureds as to the coverage needs.[6]

However, a well-developed body of case law has established an exception to this general rule. The exception applies if a "special relationship" exists between the broker and client, thereby triggering an enhanced duty of care to advise the client about the amount of coverage needed to completely meet its insurance needs.[7]

Case examples supporting a finding of a special relationship include situations in which:

- The agent misrepresented the nature of the coverage being offered or provided, and the insured justifiably relied on that representation in selecting the policy.[8]
- The agent voluntarily assumed the responsibility of selecting the appropriate insurance policy for the insured (by express agreement or promise to the insured).[9]
- The agent professed expertise in a field of insurance being sought by the insured, and the insured relied on that expertise.[10]
- The agent or broker exercised broad discretion to service the insured's needs and received compensation above the customary premium paid for the expert advice provided.[11]
- The agent was intimately involved in the insured's business affairs or regularly gave the insured advice or assistance in maintaining proper coverage.[12]

If an insurance professional has a corporate client and a special relationship exists, then there is arguably a duty to advise the client about the availability of cyberinsurance policies.

## WHAT IS AT STAKE?

Cyberevents in which thousands of people have their personally identifiable information stolen (including events involving Equifax,


© 2018 Thomson Reuters

Home Depot, Target and Yahoo) garner extensive media coverage. Less attention is paid to attacks carried out using other vectors, like ransomware, which prevents a company from accessing information unless a ransom is paid.

In 2017, the WannaCry and Petya ransomware attacks impacted thousands of computers and blocked user access to data systems unless and until users made ransom payments. And ransomware attacks have already been reported in 2018.

In January Hancock Regional Hospital was hit with a ransom demand for bitcoin from hackers who encrypted data files associated with the hospital's most critical information systems.[13] After notifying the FBI, its attorneys, cybersecurity specialists and the cybersecurity insurance company, the hospital made the decision to pay the hackers for decryption keys to access the data files and restore its information technology network.

Another troublesome vector is a denial-of-service attack that disrupts customers' access to an organization's system, such as an attack that affected Twitter, Netflix and Sony's PlayStation network.[14] There is also the social engineering vector in which an employee is tricked into transferring funds or confidential information.

These types of cyberattacks cause business interruptions that could lead to losses amounting to hundreds of thousands of dollars. While larger corporations may survive such an attack, smaller uninsured companies may be forced to shutter.

And companies may pursue litigation against the insurance professional who failed to procure adequate insurance. If found liable, an insurance professional may have to pay the difference between the coverage that should have been in force, but for the error, and the actual net insurance recovery, if any.

## ISSUES TO CONSIDER

With all this in mind, insurance professionals should appreciate the demand and need for cyberinsurance policies for every company that relies on computers and the internet — essentially every company. Although cyberinsurance is still relatively new, there are many insurance professionals who have in-depth experience and knowledge in this area.

But beware: The risk of litigation is extremely high if an insurance professional claims expertise in cybersecurity and the client suffers a breach that results in a denied claim.

Likewise, when an insurance professional is intimately involved in the insured's business affairs (for example, handles all the insurance needs for the client or regularly provides advice in maintaining proper coverage), then the agent should advise about cyber risks, in writing, and engage a broker with far more knowledge.

In addition, when offering a cyberpolicy, insurance professionals should take great pains to review the language of the policy with the client. The client should understand what is, and what is not, covered. Because courts are still grappling with the language in some policies, there are no guarantees. At the very least, the insurance professional and the client should review the policy's exclusions and definitions.

The definitions of "confidential information" and "personally identifiable information" are the most fundamental in a cyberinsurance policy.

Some policies define confidential information broadly as any information from which an individual may be uniquely and reliably identified or contacted. This may include an individual's name, address, telephone number, Social Security number, account relationships, account numbers, account balances, account histories or passwords. Under such a definition, an individual's name, on its own, could be considered PII.

In contrast, other policies may identify very specific items that are considered confidential information that may mirror state-specific definitions of PII. For example, Florida defines personal information as an "individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: a Social Security number; a driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account," etc.

Beware of exclusions for contractual liability; criminal conduct; terrorism, hostilities and claims arising from "acts of foreign enemies"; and unauthorized collection of customer data. These exclusions could have unintended consequences.

A criminal conduct exclusion would bar any claims that resulted from a social engineering scheme. An exclusion for terrorism could bar cyberbreaches that resulted from foreign actors or governments.

Similarly, an exclusion for unauthorized collection of consumer data could affect any company engaged in online activities, especially activities in which consumer financial data is collected.

Although not a bulletproof defense in litigation, an insurance professional could attempt to limit the scope of services, in writing, to exclude any advice regarding cyberinsurance. From a business perspective, an agent or broker may not want to refer clients to competitors to evaluate cyber risks.

## EMBRACE THE FUTURE

Like many industries, insurance will change and evolve as society embraces new internet-reliant technologies. Insurance professionals will have to understand how new technology and the advent of cyberspace will affect their clients.[15] Failing to embrace, evolve and implement strategies to offer insurance products for the cyberage will expose insurance professionals to litigation. WJ

## NOTES

[1] *Medidata Sols. Inc. v. Fed. Ins. Co.*, 268 F. Supp. 3d 471, 472 (S.D.N.Y. 2017).

[2] *Am. Tooling Ctr. Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017).

[3] Perpetual Storage Inc.'s Answer, Counterclaim and Third-Party Complaint, *Colo. Cas. Ins. Co. v. Perpetual Storage Inc.*, No. 10-cv-316 (D. Utah July 8, 2010), 2010 WL 1141910.

[4] Complaint, *Learning Enhancement Corp. v. Haywood & Fleming Assocs.*, No. 2011-L-013210 (Ill. Cir. Ct. Dec. 11, 2011), 2011 WL 6440349.

[5] Third-Party Complaint, *New Hotel Monteleone LLC v. Certain Underwriters at Lloyd's of London*, No. 16-cv-61 (E.D. La. Mar. 28, 2016), 2016 WL 1221443.

[6] Gary Knapp, Annotation, Liability of Insurer or Agent of Insurer for Failure to Advise Insured as to Coverage Needs, 88 A.L.R. 4th 249, § 3, 1991 WL 741640 (1991); *Emerson Elec. Co. v. Marsh & McLennan Cos.*, 362 S.W.3d 7 (Mo. 2012).

© 2018 Thomson Reuters

[7] *See* generally *Peter v. Schumacher Enters. Inc.*, 22 P.3d 481 (Alaska 2001), and *Fitzpatrick v. Hayes*, 67 Cal. Rptr. 2d 445 (Cal. Ct. App., 1st Dist. 1997).

[8] See, e.g., Fitzpatrick at 452.

[9] *See, e.g., Harts v. Farmers Ins. Exchange*, 597 N.W.2d 47, 51-52 (Mich. 1999).

[10] *See, e.g., Meridian Title Corp. v. Gainer*, 946 N.E.2d 634 (Ind. Ct. App. 2011); *Warehouse Foods Inc. v. Corporate Risk Mgmt. Serv.*, 530 So. 2d 422 (Fla. 1st Dist. Ct. App. 1988).

[11] *See e.g., Sintros v. Hamon*, 810 A.2d 553 (N.H. 2002).

[12] *Buelow v. Madlock*, 206 S.W.3d 890 (Ark. Ct. App. 2005).

[13] Grace Johansson, Cyber-attack shuts down US Regional Hospital's online system, SC Media, Jan. 16, 2018, 2018 WLNR 1733059.

[14] Raphael Satter, Internet attack disrupts service, web-traffic manager Dyn Inc. struck twice, Associated Press, Oct. 22, 2016, 2016 WLNR 32536680.

[15] This article is not intended to provide an exhaustive risk analysis for insurance professionals; it is only the tip of the iceberg. The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

## Botched prenup

CONTINUED FROM PAGE 1

Chief Justice Lorie S. Gildea, joined by Justice G. Barry Anderson, dissented from the majority, finding that Wallerich made one error — failing to be aware of prenuptial requirements — and that Minnesota's six-year clock for legal malpractice claims had run.

### WITNESSES LACKING

In September 2006 Wallerich prepared a prenuptial agreement for Joseph Frederick based on his intent that his then-fiancée, Cynthia Gatliff, would not gain any of his assets should they divorce, the majority opinion said.

Frederick and Gatliff signed the agreement the same month and married the following day, but because the agreement did not include the statutorily required witness signatures, it was unenforceable, the opinion said.

About a year later, on Sept. 12, 2007, Frederick had Wallerich draw up a will that incorporated the prenuptial agreement and included a provision stating, "I have intentionally omitted my spouse from taking under this will as we have provided for bequests at our death by separate written instrument dated Sept. 28, 2006," according to the opinion.

Gatliff filed for divorce in January 2013 and in the proceedings obtained a share of Frederick's assets, in part due to a ruling by the divorce court that the prenuptial agreement was unenforceable, Justice Hudson's opinion said.

Frederick filed his malpractice suit against Wallerich on Sept. 10, 2013, alleging that the attorney was negligent by failing to alert him in 2007, when she drew up his will, that the prenuptial agreement was invalid, the opinion said.

The trial court dismissed the suit as untimely.

Citing *Antone v. Mirviss*, 720 N.W.2d 331 (Minn. 2006), the court found that the six-year limitations period for a legal malpractice claim started running on the date of marriage because that was when "some damage" to Frederick from the alleged malpractice occurred.

The state Court of Appeals affirmed.

Frederick again appealed, and the state's high court agreed to review the case, saying the issue whether multiple acts by an attorney can give rise to independent legal malpractice claims was one of first impression.

### INDEPENDENT ACT OF NEGLIGENCE

The Supreme Court reversed the Court of Appeals' ruling and remanded to the trial court.

Although Frederick was too late to sue over the prenuptial agreement, his claim that Wallerich failed to advise him a year later that the agreement would not protect him alleged an independent act of negligence, the high court majority said.

That act started its own six-year clock Sept. 28, 2007, when Frederick executed the will, the majority said.

Frederick's suit against Wallerich was therefore timely, the majority said.

The majority explained that the alleged 2007 error did not necessarily flow from the alleged 2006 error and that it significantly worsened Frederick's standing in the divorce proceedings.

The faulty advice allegedly given in 2007 deprived Frederick of the opportunity to immediately initiate divorce proceedings or seek a new agreement, actions that would have saved him $1 million in asset appreciation that went to Gatliff, the majority said.

### THE DISSENT

In her dissent, Justice Gildea said Frederick's suit alleged that Wallerich made just one error — the failure to be aware of witness requirements for prenuptial agreements — but made it multiple times.

"That is, Wallerich failed to advise Frederick, at a later time, of Wallerich's original error," the justice wrote.

That error began to accrue on the date of Frederick and Gatliff's marriage, the dissent said, agreeing with the trial court that *Antone* governed the case. WJ

**Attorneys:**
*Plaintiff:* Patrick H. O'Neill Jr., Larson King LLP, Saint Paul, MN

*Defendant:* Kay Nord Hunt, Lommen Abdo, Minneapolis, MN

***See Document Section A (P. 23) for the opinion.***


© 2018 Thomson Reuters

# Panel revives $20 million malpractice claim against Heller Ehrman

**By Lisa Uhlman**

A California bankruptcy court wrongly found a client's $20 million malpractice claim against defunct law firm Heller Ehrman LLP was time-barred, a federal appeals panel has ruled, saying fact issues remained as to when the parties' attorney-client relationship ended.

***In re Heller Ehrman LLP; Paravue Corp. v. Heller Ehrman LLP, No. 16-15385, 2018 WL 1148408 (9th Cir. March 5, 2018).***

The bankruptcy court misapplied summary judgment standards when it found an email thread between a Heller attorney and a director of the client conclusively terminated the relationship, triggering California's statute of limitations on legal malpractice claims, the 9th U.S. Circuit Court of Appeals panel said.

## CORPORATE SHUFFLE

Lauren Barghout founded vision software startup Paravue Corp. in 2002 and served as its chief science officer, according to a previous order by the U.S. District Court for the Northern District of California. Paravue hired international law firm Heller Ehrman as corporate counsel.

Paravue subsequently obtained financing from venture capital firm Acuity Ventures II LLC, the order said. After a corporate governance dispute arose, Paravue's board appointed Acuity partner Laurence Hootnick as CEO in late 2006.

Acuity ultimately sued Paravue and Barghout in state court, seeking to convert Paravue's debt into preferred stock. In June 2007 it demanded Paravue prepare its assets for a public sale, according to the 9th Circuit panel's opinion.

## EMAILS, WITHDRAWAL, ASSET SALE

In a series of emails beginning July 3, 2007, Barghout and her personal counsel, Jack Russo, repeatedly demanded Heller take action to prevent the sale, the opinion said. A Heller attorney responded that the firm would not act on Barghout's direction and that Barghout lacked authority to speak for Paravue.

On July 10, 2007, Heller told Russo it was withdrawing as Paravue's counsel, and July 11 it filed an application with the state court seeking to withdraw, the opinion said. The state court granted the application July 17, 2017.

Meanwhile, Barghout learned Hootnick had resigned July 9, so she stepped in as CEO. Paravue's board confirmed the appointment July 13, 2007, but the parties disagree about when her new role became effective and what authority she had before being confirmed, the opinion said.

Acuity held the public sale and purchased Paravue's assets Oct. 31, 2007. On July 14, 2008, Heller and Paravue agreed to toll the statute of limitations as to any of Paravue's potential claims against the firm that were not already time-barred, according to the District Court's order.

## SUMMARY JUDGMENT

Heller filed a Chapter 11 petition in the U.S. Bankruptcy Court for the Northern District of California in December 2008. Paravue asserted a $20 million malpractice claim against the debtor April 27, 2009, and Heller moved for summary judgment, saying the claim was time-barred.

The Bankruptcy Court agreed with the debtor, finding the claim barred under California's one-year limitations period for legal malpractice actions, Cal. Civ. Proc. Code § 340.6. Paravue appealed, and the District Court affirmed in its Oct. 7, 2015, order.

Paravue then turned to the 9th Circuit, arguing that the Bankruptcy Court erred by conflating Barghout, a board member and director, with Paravue, the corporation and Heller's actual client, in deciding the claim was time-barred.

## CONTINUOUS-REPRESENTATION RULE

Under Cal. Civ. Proc. Code § 340.6(a)(2), the limitations period is tolled while an attorney continuously represents the plaintiff on the "specific subject matter in which the alleged wrongful act or omission occurred."

In *Gonzalez v. Kalu*, 43 Cal. Rptr. 3d 866 (Ct. App. 2006), the California Court of Appeal held that, when an attorney unilaterally withdraws, the representation is deemed to end "when the client actually has or reasonably should have no expectation that the attorney will provide further legal services."

A determination of continuous representation under Section 340.6(a)(2) should be made "objectively from the client's perspective" and is "predominantly a question of fact," the *Gonzalez* court said.

## GENUINE FACT ISSUES

Here, the Bankruptcy Court found the July 2007 email thread conclusively ended Heller's representation of Paravue, causing the limitations period to begin running no later than July 11, 2007. Thus, it said, the malpractice claim was untimely because it expired prior to the July 14, 2008, tolling agreement.

Rejecting that finding, the 9th Circuit panel said the Bankruptcy Court misapplied summary judgment standards, which require courts to view the facts in the light most favorable to the nonmoving party, that is, Paravue.

The July 2007 emails "do not irrefutably terminate the attorney-client relationship" because there are genuine issues of fact as to whether Heller's representation of Paravue continued, the panel said, adding that a "reasonable factfinder could conclude" that it did.

© 2018 Thomson Reuters

The Bankruptcy Court seems to have viewed the facts in the light most favorable to Heller, the party seeking summary judgment, and to treat Barghout, rather than Paravue, as Heller's client, the panel said.

Moreover, the evidence does not show Paravue "actually and reasonably believed" Heller's representation had ended based on the email thread, the panel said.

It noted that the emails from the Heller attorney were sent not to Hootnick, Paravue's then-CEO, but to Barghout, then only chief science officer, and her personal attorney. Heller's attorney also explicitly said in the emails that the firm believed Barghout had no authority to direct its actions.

The Bankruptcy Court thus "improperly weighed the evidence and implicitly made credibility determinations to conclude that no genuine issue of material fact existed as to the meaning and effect of the emails," the panel said.

It therefore reversed the Bankruptcy Court's ruling on summary judgment that Paravue's claim was time-barred, and remanded the case. WJ

**Attorneys:**
*Plaintiff-appellant:* Jack Russo and Christopher J. Sargent, ComputerLaw Group LLP, Palo Alto, CA

*Defendant-appellee:* Thomas A. Willoughby and Jason E. Rios, Felderstein Fitzgerald Willoughby & Pascuzzi, Sacramento, CA; John D. Fiero, Pachulski Stang Ziehl & Jones, San Francisco, CA; Jonathan W. Hughes, Arnold & Porter Kaye Scholer, San Francisco, CA; Marjorie E. Manning, Bolling & Gawthrop, Sacramento, CA; Pamela Phillips, Howard Rice Nemerovski Canady Falk & Rabkin, San Francisco, CA; Christopher Daniel Sullivan, Diamond McCarthy LLP, San Francisco, CA

**Related Filings:**
Opinion: 2018 WL 1148408
Appellant's opening brief: 2016 WL 4491413
Appellee's answering brief: 2016 WL 6091139
Appellant's reply brief: 2016 WL 6935611
District Court's opinion: 2015 WL 5834134

## SANCTIONS

# Bankruptcy lawyer sanctioned for 'abandoning' clients upon retirement

**By Thomas Parry**

A New Orleans bankruptcy attorney who abruptly retired without notifying his clients or the court must pay $3,500 in fines and return the fees he collected after abandoning his job duties, a Louisiana bankruptcy judge has ruled.

***In re Galloway et al., No. 15-12646, 2018 WL 1065124 (Bankr. E.D. La. Feb. 23, 2018).***

U.S Bankruptcy Judge Elizabeth W. Magner for the Eastern District of Louisiana found that attorney Nelson Rivers violated standards of professional conduct and made misrepresentations to the court in a series of actions following his sudden decision to move to Oregon.

### '2,000 MILES AWAY'

After decades as a bankruptcy attorney in New Orleans, Rivers informed his secretary Sherry Swanson in early July 2017 that he was retiring and moving "2,000 miles away" to Oregon by the end of the month, Judge Magner explained in her opinion.

Rivers had 50 bankruptcy cases pending in New Orleans federal court, but failed to formally notify any of his clients and mentioned his retirement plans only to those who happened by his office, the opinion said.

By July 31, 2017, Rivers sold the building that housed his practice to attorney Wayne Aufrecht and moved out, leaving all of his files behind, it said.

Just prior to his departure, Rivers filed five new cases, and then filed two more after leaving New Orleans, according to the opinion.

In Rivers' absence, Swanson attempted to arrange new representation for clients who had upcoming hearings and meetings, the opinion said.

On Aug. 22, 2017, Rivers failed to appear in court to represent his clients Larry and Robin Galloway at a hearing on a motion by the Chapter 13 trustee to dismiss their case for failure to make plan payments, according to the opinion. At a subsequent hearing on the motion, Rivers appeared via a faulty phone connection and was "wholly unprepared," the opinion said.

During the phone hearing, Rivers insisted to the court that Aufrecht had assumed responsibility for his clients, the opinion said.

The court ordered Rivers and Aufrecht to show cause why they should not be held in civil contempt and then conducted hearings on the matter.

### 'DERELICTION OF DUTIES'

Judge Magner found that Aufrecht had agreed only to buy Rivers' building, not to take over his cases, and that Rivers' statements to the contrary were misrepresentations.

"[Rivers] intentionally led the court to believe that the gap in representation was as a result of Mr. Aufrecht's failure to substitute, rather than state the truth," the judge said.

She further found that Rivers improperly relied on Swanson to wind down his law practice, essentially leaving her to practice law without a license.

Judge Magner also found that Rivers had had failed in his duties to the Galloways by not monitoring the progress of the critical motion to dismiss their case, and had blown meetings and hearings for his other cases and "completely abdicated his responsibility to his clients" thereby violating multiple professional conduct rules.

"There can be no clearer example of a failure of professional responsibility or dereliction of duties owed under contract" and various


© 2018 Thomson Reuters

professional conduct requirements, the judge said.

For these violations, the judge ordered Rivers to disgorge $350 for each missed hearing or creditors meeting, for a total of $6,300.

Additionally, Rivers owed $3,500 for the misrepresentations he made to the court regarding Aufrecht, the judge said.

Finally, Rivers had to forgo any stipends forthcoming from his cases and return to his clients $10,065 in unearned fees, including $8,500 in unearned Chapter 13 "no look" fees, she said. WJ

**Related Filings:**
Opinion: 2018 WL 1065124

BANKRUPTCY/MISAPPROPRIATION

# Injury lawyer can't dodge ill-gotten settlement-related debts in Chapter 7

**By Thomas Parry**

A now-disbarred personal injury attorney cannot discharge through his bankruptcy case $200,000 in debts owed to a loan provider that funded his clients' living expenses, an Illinois bankruptcy judge has ruled.

***In re Santilli et al., Nos. 16-14713, 16-23020; Preferred Capital Funding of Illinois LLC v. Santilli, Adv. No. 16-707, 2018 WL 1305057 (Bankr. N.D. Ill. Mar. 12, 2018).***

U.S. Bankruptcy Judge Jacqueline P. Cox of the Northern District of Illinois found that attorney Frank Santilli deposited settlement checks from his personal injury cases into his firm's escrow account but failed to abide by his obligation to repay money owed to Preferred Capital Funding of Illinois Inc.

In granting Preferred Capital's motion to except the debts from Santilli's bankruptcy case, Judge Cox found that Santilli avoided making payments through years of intentional deception that amounted to appropriation of the loan provider's funds.

## SETTLEMENTS DIVERTED

According to Judge Cox's opinion, Preferred Capital made living-expense loans to about 100 of Santilli's clients over the last 10 years of his personal injury and workers' compensation practice.

When Santilli won settlements for his client's injury claims, he was required under the terms of the loans the company made to his clients to direct the settlement proceeds to repay the loans, the opinion said.

However, Santilli's law career ended in September 2016 when the Illinois Supreme Court disbarred him for knowingly misappropriating $500,000 of a client's settlement funds, according to Judge Cox's opinion.

Meanwhile, in April 2016, while the disciplinary case was pending, Santilli and his wife filed a joint Chapter 7 bankruptcy petition, and three months later he filed a Chapter 7 petition on behalf of his law firm, the Santilli Law Group. The court later consolidated the cases.

Preferred Capital filed an adversary complaint seeking to prevent Santilli from discharging the more than $200,000 it claimed he owed the company over loans made to 10 of his clients.

According to the lender, Santilli had told it that those 10 cases were still in litigation, or that there had been a delay in the settlement payments, when in fact he had received settlement funds in those cases and had kept the money instead of directing it to Preferred Capital to repay the loans.

Santilli disputed Preferred Capital's version of facts and the court held a trial in January 2018 to hear evidence.

## DECEPTION AND THE VEIL

Judge Cox determined that the debts Santilli owed to Preferred Capital were nondischargeable under Sections 523(a)(2)(A) and (a)(4) of the Bankruptcy Code, 11 U.S.C.A. §§ 523(a)(2)(A) and (a)(4), finding that Santilli obtained the debts through intentional deception.

Santilli made false statements and crucial omissions of fact in communications over whether settlement funds had arrived, thereby abusing the lender's "justifiable reliance" on him as required by Section 523(a)(2)(A), the judge said.

Furthermore, Santilli carried out these deceptions with regard to 10 cases over several years, evincing an intent to mislead Preferred Capital in what amounted to a misappropriation of the loan, constituting "embezzlement" for purposes of Section 523(a)(4), the judge said.

The judge also found the debts nondischargeable under Section 523(a)(6) of the code, 11 U.S.C.A. § 523(a)(6), saying Santilli's refusal to pay Preferred Capital, resulting in a loss of its investment, caused a "willful and malicious" injury.

Finally, Judge Cox found that Santilli, as the "sole owner and check writer" of his firm, was personally liable for these debts, thus warranting a grant of the lender's bid to "pierce" the Santilli Law Group's "corporate veil."

"Injustice would be promoted if the veil does not get pierced; we would condone Mr. Santilli's conduct that misled [Preferred Capital] regarding the status of his clients' cases," the judge said. WJ

**Related Filings:**
Opinion: 2018 WL 1305057

© 2018 Thomson Reuters

# Illinois judge convicted in $1.4 million mortgage fraud plot

A federal jury in Chicago has convicted an Illinois judge of defrauding banks of $1.4 million by using fraudulent documents to obtain loans for a number of property transactions before she was elected to the bench.

***United States v. O'Brien et al., No. 17-cr-239, verdict returned (N.D. Ill. Feb. 15, 2018).***

Judge Jessica Arong O'Brien of the Cook County Circuit Court, 50, a licensed loan originator and real estate broker, was found guilty Feb. 15 on one count each of bank and mail fraud, U.S. Attorney John R. Lausch Jr. of the Northern District of Illinois said in a statement.

O'Brien and co-defendant loan officer Maria Bartko made false representations on loan applications and supporting documents to induce multiple lenders, including Citibank and JPMorgan Chase Bank, to issue $1.4 million in mortgage and commercial loans between 2004 and 2007, prosecutors said. She became a judge in 2012.

## STATE WORKER

At the time of the fraud, O'Brien held Illinois licenses to practice law, sell real estate and act as a loan originator, according to the April 2017 indictment against her. She owned real estate firm O'Brien Realty LLC, the charges said.

In addition, she worked full time as a special assistant attorney general for the Illinois Department of Revenue in Chicago and part time as a loan officer with Lincolnwood, Illinois-based Amronbanc Mortgage Corp., prosecutors said.

Bartko was O'Brien's co-worker at Amronbanc, according to the indictment.

## FALSIFIED LOAN APPLICATIONS

O'Brien submitted a mortgage loan application to an unidentified lender in August 2004, seeking funds to buy a property on 46th Street in Chicago, according to the charges. The documents falsely listed her monthly income from the Revenue Department as $6,800 and did not disclose that she owed more than $260,000 on another mortgage for a property she owned with an unidentified person.

After obtaining the mortgage and buying the 46th Street property, O'Brien bought a property on 54th Street a month later. She sought to refinance the mortgages on both parcels in September 2005, the charges said.

Working with Bartko as a loan originator for the transactions, O'Brien submitted falsified applications to a lender and misrepresented her income and employment. She caused the lender to refinance the loans by indicating on the documents that O'Brien Realty was her only employer and that she earned $20,000 a month, prosecutors said.

O'Brien also gave JPMorgan Chase false information to obtain a commercial line of credit in November 2006 so she could obtain funding purportedly on O'Brien Realty's behalf, telling the bank that the company's annual revenue was $150,000 and the annual profit $100,000, the charges said.

After the bank issued the loan, O'Brien used the money to cover expenses on the 46th Street and 54th Street properties, prosecutors said.

## PROPERTY SALES

In March 2007 O'Brien and Bartko engineered the fraudulent sale of both properties, the indictment said.

They planned for Bartko to buy the parcels, but since she could not qualify for a loan, she agreed to find a person who would act as a straw buyer for both sales transactions, according to the charges.

O'Brien paid Bartko and the straw buyer to participate in the scheme, the indictment said. She also prepared falsified documents to make it appear the straw buyer had income sufficient to qualify for the loans and would occupy the properties.

The false representations caused Citibank to extend a $73,000 mortgage loan for the straw buyer's purported purchase of the 46th Street property, the charges said. Prosecutors did not disclose whether any lender funded a loan for the 54th Street property.

## POSSIBLE 60-YEAR SENTENCE

U.S. District Judge Thomas M. Durkin will sentence O'Brien on July 6. She faces up to 30 years in prison on each count of bank and mail fraud, prosecutors said.

Bartko pleaded guilty to one count of mail fraud affecting a financial institution. Judge Durkin has not yet set her sentencing date. WJ

**Related Filings:**
Indictment: 2017 WL 7051461


© 2018 Thomson Reuters

# Florida eye doctor gets 17 years for billing fraud after avoiding bribery retrial

**By Jodine Mayberry**

South Florida ophthalmologist Salomon Melgen has been sentenced to 17 years in prison and ordered to pay $42.5 million in restitution for health care fraud, just weeks after federal prosecutors dropped unrelated bribery charges against him and New Jersey U.S. Sen. Robert Menendez.

***United States v. Melgen, No. 15-cr-80049, defendant sentenced (S.D. Fla. Feb. 22, 2018).***

After a 28-day trial last April, a jury in the U.S. District Court for the Southern District of Florida convicted the West Palm Beach eye doctor of 76 counts of health care fraud that may have cost taxpayers as much as $73 million. *U.S. v. Melgen*, No. 15-cr-80049, *verdict returned,* 2017 WL 1547310 (S.D. Fla. Apr. 28, 2017).

Sentencing on those charges had been postponed pending the outcome of a joint trial in the U.S. District Court for the District of New Jersey with Melgen's longtime friend Menendez. The two were tried on 18 counts of bribery and influence peddling.

That trial resulted in a hung jury last year. U.S. District Judge William H. Walls then acquitted the defendants on seven of the bribery counts, and prosecutors dropped the remaining charges Jan. 31. *U.S. v. Menendez*, No. 15-cr-155, *order issued* (D.N.J. Jan. 31, 2018).

***Ophthalmologist Salomon Melgen*** REUTERS/Eduardo Munoz

## MEDICARE FRAUD SENTENCE

In addition to the prison term and restitution order, U.S. District Judge Kenneth A. Marra imposed a $6,700 fine and sentenced Melgen, 63, to three years of supervised release.

The judge noted that the $42.5 million restitution order was preliminary and subject to modification at a to-be-determined hearing date. Judge Marra also said the "intended loss" from the false billings was $73.4 million.

Melgen, who has been incarcerated since his conviction, indicated he would appeal and submit a written motion for bond seeking his release pending the appeal's outcome, according to the minutes.

The Medicare fraud indictment filed in April 2015 said Melgen falsely billed the government for thousands of unnecessary and useless medical tests and treatments for age-related macular degeneration and retinal injuries.

He directed his staff to enter an ARMD diagnosis into nearly every patient chart and would diagnose most of his Medicare patients with the disease either before he even saw them or immediately afterward, the indictment said.

Many of his patients did not suffer from ARMD at all or had a variant of the disease called "dry ARMD" but were diagnosed with "wet ARMD" instead, prosecutors said.

Dry ARMD cannot be treated, but wet ARMD can be stabilized with certain expensive drugs, such as Lucentis.

Melgen allegedly made "exorbitant and improper profits" from Lucentis by splitting single-use vials of the drug into as many as four doses. He then administered the doses to multiple patients and billed Medicare and other health care providers at the full reimbursement rate for a single dose, prosecutors said in a statement after his indictment in 2015.

## BRIBERY INDICTMENT

The New Jersey indictment alleged that Melgen had bribed Menendez with private jet travel, luxury vacations and hundreds of thousands of dollars in campaign contributions in exchange for the Democratic senator's intercession with federal agencies on his behalf.

At least some of Melgen's payoffs to Menendez were made to seek the senator's help in resolving an $8.9 million Medicare billing dispute over his practice of splitting the Lucentis vials, the indictment said.

Menendez is alleged to have met with the acting director of the Centers for Medicare and Medicaid Services and the secretary of the Health and Human Services Department on Melgen's behalf, but both refused help, saying they would not pay for the same vial of Lucentis twice, according to the indictment. WJ

**Attorneys:**
*Plaintiff:* Alexandra Chase, Roger H. Stefin and Carolyn Bell, U.S. Attorney's Office, West Palm Beach, FL

*Defendant:* Kirk Ogrosky and Murad Hussain, Arnold & Porter, Washington, DC

**Related Filings:**
Sentencing order: 2018 WL 1027149
Fraud indictment: 2015 WL 1874554
Bribery indictment: 2015 WL 1457957

© 2018 Thomson Reuters

# Georgia high court reverses $22 million verdict for deadly procedure, citing faulty jury instruction

**By Thomas Parry**

A Georgia doctor and the estate of a patient who died following a procedure at the doctor's ambulatory surgery center will have to undergo a retrial, the state's highest court has ruled, concluding the trial court's instructions failed to separate ordinary negligence from malpractice.

***Southeastern Pain Specialists PC v. Brown et al., Nos. S17G0732, S17G0733 and S17G0737, 2018 WL 1143818 (Ga. Mar. 5, 2018).***

In reversing a $22 million verdict against Dr. Dennis Doherty and the surgery center, an eight-member panel of the Georgia Supreme Court unanimously found the trial court improperly instructed the jury that Doherty's response to medical equipment data could be construed as "ordinary negligence."

"The plaintiffs' case of medical malpractice was very strong," Justice Nels S.D. Peterson wrote in an opinion for the high court.

"But a very strong case of medical malpractice does not become a case of ordinary negligence simply due to the egregiousness of the medical malpractice," he added.

"The ordinary negligence instruction invited jurors to decide the doctor's liability of the defendants without consideration of the strictures on claims for professional malpractice, such as the need for expert testimony to overcome the presumption of due care," the judge said.

Doherty, his surgery center and the estate of his now-deceased patient Gwendolyn Lynette Brown will have to go through a full retrial to resolve the matter, the high court said.

## LOW OXYGEN

On Sept. 16, 2008, Brown went to Doherty's practice to undergo an epidural steroid procedure to treat her chronic back pain, the opinion said.

Shortly after Doherty put Brown under anesthesia, the oximeter — a device that measures a patient's blood oxygen level — sounded an alarm, the opinion said.

Brown's oxygen level registered zero on the oximeter, and her blood pressure monitor ceased to register any readings, the opinion said.

According to the opinion, Doherty rejected the attending nurse's suggestion that they call for more help, and at the close of the 18-minute procedure, Doherty refused to call 911.

Almost two hours later, when a nonresponsive Brown was admitted to emergency care, Doherty failed to advise the hospital that his medical equipment had registered a dangerous drop in Brown's oxygen levels, the opinion said.

The hospital determined Brown had suffered acute respiratory failure, it said.

Following the procedure, Brown remained cognitively impaired and wheelchair-bound, and her husband filed a medical malpractice suit against Doherty, according to the opinion.

When Brown died in 2014, her husband amended the suit to include a wrongful-death claim, the opinion said.

At trial, the court instructed the jury that Doherty could be liable under "ordinary negligence" in addition to professional medical negligence because a layperson would understand the meaning of the data from the oximeter and would know how best to respond, according to the opinion.

The jury returned a $22 million general verdict in favor of Brown's estate, and a divided appellate panel affirmed the judgment.

Doherty successfully petitioned the Georgia Supreme Court to consider whether the trial court had erred in its instructions to the jury.

## MIXED THEORIES

The high court reversed the verdict after determining the trial court had erred in its jury instructions.

The evidence supported liability under a theory of professional malpractice, the high court said, noting that Doherty responded inadequately to medical data from medical instruments.

To prove medical malpractice, "a plaintiff generally must present testimony from an expert witness to overcome the presumption that the provider acted with due care and establish the provider's negligence," the court said.

Brown's estate argued that the data from the oximeter was within the range of a layperson's knowledge because the devices were readily available from pharmacies.

The high court rejected that argument.

"The ability of the public to purchase a medical device is not evidence of general lay knowledge regarding how to interpret and act upon readings provided by that device, much less in the middle of a medical procedure," Justice Peterson said.

He noted that Doherty's failure to inform the emergency service of what had happened during the procedure could fall within the realm of ordinary negligence.

However, the jury had delivered a "general verdict," making it impossible to tease out which theory of liability it had applied, he said.

## RETRIAL REQUIRED

In determining the case would have to undergo a full retrial, Justice Peterson rejected the defendants' request to affirm the damages award, which included zero punitive damages.


© 2018 Thomson Reuters

"The jury's decisions on punitive damages are too related to the questions of liability and compensatory damages," he said.

On retrial, Brown's estate could argue for a higher assessment of damages, the justice said.

"Moreover, the jury on retrial may well hear a different body of evidence or rely on a different theory of liability and thus may make a different judgment as to the reprehensibility of Dr. Doherty's conduct," Justice Peterson wrote. WJ

**Attorneys:**
*Plaintiff:* James N. Sadd, Daniel M. Epstein and Edward M. Wynn III, Slappey & Sadd, Atlanta, GA

*Defendant:* John E. Hall Jr., Nichole Lee Hair and Steven Maher Harkins, Hall Booth Smith PC, Atlanta, GA

**Related Filings:**
Opinion: 2018 WL 1143818

***See Document Section B (P. 39) for the opinion.***

## BREACH OF DUTY

# Equifax directors are liable for data hack, investors say

**By Nicole Banas**

Equifax Inc. directors and executives are facing a new shareholder derivative lawsuit claiming they failed to protect the consumer credit reporting firm from a massive cybersecurity breach impacting 145 million Americans.

***Teamsters Local 443 Health Services & Insurance Plan v. Gamble et al., No. 18-cv-577, complaint filed, 2018 WL 795090 (N.D. Ga. Feb. 6, 2018).***

The suit, filed Feb. 6 in the U.S. District Court for the Northern District of Georgia, says former Equifax Chairman and CEO Richard Smith and other insiders breached their fiduciary duties by falsely stating that the Atlanta-based company had adequate data security measures in place.

In a derivative suit, any money recovered goes to the company, not directly to shareholders.

Shareholder Teamsters Local 443 Health Services and Insurance Plan filed the complaint about three months after it voluntarily dismissed a similar action against various Equifax insiders. *Teamsters Local 443 Health Serv. & Ins. Plan v. Gamble*, No. 17-cv-4402, *notice of voluntary dismissal filed* (N.D. Ga. Nov. 8, 2017).

The new complaint adds allegations that a special committee of purportedly independent Equifax directors failed to take action against three executives for insider selling.

Chief Financial Officer John W. Gamble Jr., President of U.S. Information Solutions Joseph Loughran III and President of Workforce Solutions Rodolfo Ploder reaped a combined $1.8 million from stock sales before Equifax disclosed the security breach Sept. 7, the suit says.

REUTERS/Kevin Lamarque

***The suit says former Equifax Chairman and CEO Richard Smith, shown here in 2017, and other insiders breached their fiduciary duties by falsely stating that the company had adequate data security measures in place.***

The suit also names several directors, including special committee members Robert Daleo, G. Thomas Hough and Elaine Stock, as defendants.

### DATA BREACH

The complaint says Equifax's security team discovered and blocked suspicious online activity July 29 but waited until Sept. 7 to disclose the incident.

In a statement that day, the company said hackers accessed a U.S. website application from mid-May through July that contained personal information of about 143 million Americans.

The company announced Smith's retirement later that month and disclosed Oct. 2 that the data breach potentially affected more than 145 million consumers.

Smith testified at an Oct. 3 hearing before the U.S. House of Representatives that "human error and technology failures" caused the breach, the suit says.

### 'AMAZINGLY LAX SECURITY'

The defendants allegedly caused Equifax to make false and misleading statements to investors about the strength of its risk management procedures.

© 2018 Thomson Reuters

The company's website stated that information security was a "top priority," but it had "amazingly lax security" in its Workforce Solutions division and failed to prevent another hacking in October, the suit says.

Equifax said in a Nov. 3 statement that a special committee of its board conducted an independent investigation of insider selling allegations and concluded Gamble, Loughran and Ploder were unaware of the security breach when they sold company shares in early August.

Teamsters' suit says it is "simply not believable" that high-level executives did not know about such a "cataclysmic" event days after it was discovered.

The special committee was not sufficiently independent because two of its members, Daleo and Hough, received substantial compensation from the company, the suit says.

## COMPANY 'DEVASTATED'

The defendants' misconduct has "devastated" Equifax's credibility and led to ongoing investigations by the Securities and Exchange Commission, the Justice Department and other government agencies, the suit says.

The company has lost more than 28 percent of its market value since the breach was revealed and faces numerous lawsuits, including a recently consolidated securities fraud class action, the complaint says. *In re Equifax Inc. Sec. Litig.*, No. 17-cv-3463, *order issued* (N.D. Ga. Jan. 10, 2018).

Equifax has not yet responded to the allegations in the fraud suit.

## DEMAND FUTILITY

Teamsters says it did not bring a litigation demand to Equifax's board of directors before filing suit.

A demand would have been futile because all 11 directors face a "substantial likelihood of liability" for their actions, the complaint says.

The suit alleges breach of fiduciary duty, unjust enrichment and violation of proxy statement requirements of Section 14(a) of the Securities Exchange Act of 1934, 15 U.S.C.A. § 78n(a). WJ

**Attorneys:**
*Plaintiff:* Steven J. Estep and Jefferson M. Allen, Cohen Cooper Estep & Allen, Atlanta, GA; Frank R. Schirripa and Daniel B. Rehns, Hach Rose Schirripa & Cheverie, New York, NY

**Related Filings:**
Complaint: 2018 WL 795090


WESTLAW JOURNAL **PRODUCT LIABILITY**

It's a dangerous world out there, for both the manufacturers and marketers of hundreds of thousands of products and for the individuals who buy and use those products trusting that they will be safe. If your clients include manufacturers, distributors, retailers and users of the many consumer products in the news today because of unexpected deaths, injuries, or performance failures, you will find this reporter useful. You will find ongoing, detail coverage of cases involving statutes of limitations, product liability insurance, the duty to warn, punitive damages, market share liability, alternative design theories, and new items.

**Call your West representative for more information about our print and online subscription packages, or call 800.328.9352 to subscribe.**



© 2018 Thomson Reuters

# Wells Fargo let hacker steal $500,000 in wire-transferred funds, suit says

Wells Fargo Bank failed to prevent a hacker from stealing more than $500,000 that a law firm intended to transfer to a lawyer as part of a business deal, according to a Florida federal lawsuit.

***Peter E. Shapiro PA v. Wells Fargo Bank, No. 18-cv-60250, complaint filed, 2018 WL 992585 (S.D. Fla. Feb. 5, 2018).***

Peter E. Shapiro PA, a law firm in Broward County, Florida, says a Wells Fargo branch knew the name of the designated recipient did not match the name on the hacker-controlled account where the institution deposited the funds. The firm filed its complaint Feb. 5 in the U.S. District Court for the Southern District of Florida.

The law firm also says that in the days following the fraudulent deposit, the bank allowed the hacker to make additional wire transfers to accounts in Nigeria.

## EMAILS HACKED

The Shapiro law firm says it wired $504,611 to Wells Fargo from its legal trust account at Citibank on Nov. 21, 2017.

A hacker or group of hackers, however, had infiltrated the email accounts of the law firm and James H. Messenger Jr., the attorney involved in the business deal, the suit says.

The hacker provided the firm with fraudulent instructions for the wire transfer to Messenger, stating that the funds were to be deposited into an account ending in 0445 at a Wells Fargo branch in Cedar Park, Texas, according to the complaint.

This account did not belong to Messenger but was in the name of Chris Achebe, the plaintiff says. An unknown person or persons opened the account as part of the scheme, the suit claims.

When Wells Fargo received the plaintiff's wire transfer, which noted Messenger as the beneficiary, it placed the money into the Achebe account despite the "apparent discrepancy" between the two names, the complaint says.


REUTERS/Mike Blake

The bank notified Achebe at the end of the business day Nov. 22 that the money was in the account, according to the complaint.

## KNOWLEDGE OF FRAUD

Despite knowing the Achebe account holder was not the correct recipient and that fraud was likely, the bank took no action to restrict the account, protect the law firm or comply with federal banking regulations concerning suspicious transactions and client identification requirements, the suit alleges.

Under the USA Patriot Act, all banks must have an official program to ensure customers' true identity with reasonable certainty. The program must include account opening procedures that specify the identifying information required of each customer.

The Bank Secrecy Act, 31 U.S.C.A. § 5311, requires financial institutions to maintain programs to detect suspicious financial activity and to report it to regulators.

## MONEY MOVES OVERSEAS

The person controlling the Achebe account made a number of wire transfers from the account to recipients in Nigeria between Nov. 24 and Nov. 27, 2017, the suit says.

The law firm and Messenger learned a few weeks later that the funds never arrived in Messenger's bank account and that they had been the victims of a hacking scheme, the complaint alleges.

After the firm contacted law enforcement, Citibank and Wells Fargo about the fraud, a Wells Fargo employee admitted the beneficiary name and the deposit account name did not match in the bank's records, according to the suit.

The law firm unsuccessfully demanded that the bank return the stolen funds before it filed the suit, the plaintiff alleges.

## BREACH OF DUTY

Wells Fargo breached its duty under Fla. Stat. Ann. § 670.302, which governs a bank's obligations when receiving a payment order, by not following the sender's instructions as to the identity of the recipient, the complaint says.

> Under the USA Patriot Act, all banks must have an official program to ensure customers' true identity with reasonable certainty.

The bank also breached its regulatory obligations and the common law duties it owed to the plaintiff.

By letting Achebe have access to the money Wells Fargo knew belonged to Messenger, the bank's actions were "tantamount to intentional assistance to the knowing misappropriation of funds as part of a fraudulent scheme," the suit says.

The plaintiff is seeking an award of unspecified compensatory damages, interest and costs. WJ

**Attorneys:**
*Plaintiff:* Jeffrey B. Crockett, Coffey Burlington PL, Miami, FL

**Related Filings:**
Complaint: 2018 WL 992585

© 2018 Thomson Reuters

# ABA warns lawyer bloggers and tweeters about client confidentiality, publicity

**By Alison Frankel**

(Reuters) – In a newly issued formal opinion, the American Bar Association's Standing Committee on Ethics and Professional Responsibility cautioned lawyers not to disregard their client confidentiality obligations in professional blogs and tweets.

When it comes to client business, the ABA opinion said, lawyers are prohibited from commenting publicly without express consent from their clients — regardless of the medium.

That prohibition, under Model Rule 1.6, includes exposing a client's identity or even disclosing public-record documents like a court order, according to the ABA opinion.

"The duty of confidentiality extends generally to information related to a representation whatever its source and without regard to the fact that others may be aware of or have access to such knowledge," the opinion said. "The salient point is that when a lawyer participates in public commentary that includes client information, if the lawyer has not secured the client's informed consent or the disclosure is not otherwise impliedly authorized to carry out the representation, then the lawyer violates Rule 1.6."

The opinion also reminded lawyers about Model Rule 3.5, which bars them from seeking to influence a judge, juror, prospective juror or other official.

Even if lawyers have obtained permission from their clients to disclose information about a case in a blog or tweet, the opinion said, they have to take care that their blog posts and tweets don't create "a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter."

I emailed ABA Ethics Committee chair Barbara Gillers, a law professor at New York University, and left phone messages for committee members John Barkett of Shook Hardy & Bacon and Wendy Wen Yun Chang of Hinshaw & Culbertson. I wanted to know what sparked the ABA to issue a formal opinion and whether everyone on the committee agreed with the opinion's directives. None of the ethics lawyers immediately got back to me.

Many lawyers who use Twitter did, however, tweet their reactions when I posted a tweet with a link to the new ABA opinion. A group including #AppellateTwitter stalwart Sean Marotta of Hogan Lovells said the ABA is simply reminding lawyers that Model Rule 1.6 applies online.

"The opinion doesn't say you have to be silent," tweeted ethics lawyer Trisha Rich of Holland & Knight. "It says you can't disclose confidential information without consent and, even with consent, you can't disclose information that would be materially prejudicial. That's not new."

Three legal bloggers — Sullivan & Worcester international litigator Nicholas O'Donnell, M&A counsel Stephen Quinlivan of Stinson Leonard Street and insurance defense lawyer Jeremy Richter told me on Twitter that the opinion won't put a crimp in their commentary.

"It just affirms what should be common sense to anyone using blogging, writing articles or any other public forum," said Richter, who added that he often uses anecdotes from his practice in blog posts but is careful to change or omit identifying details in order to preserve client confidences.

O'Donnell said the opinion should have emphasized the Ethics Committee's discussion of Model Rule 3.5 in the age of blogs and Twitter.

"I wish the section on publicity had been more prominent," he told me via Twitter. "It is easier to bump into prohibited contact than it might seem and lawyers are often not anticipating ways they could be communicating with potential jurors or represented parties."

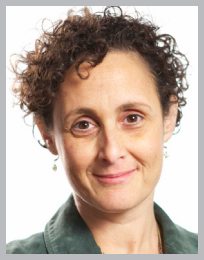
Not everyone is sanguine about the impact of the ABA opinion, though. Three lawyers told me the client confidentiality strictures could scare off attorneys worried about inadvertently breaking Model Rule 1.6.

Joshua Prentice, GC at Four Rivers Nuclear Partnership, said lawyers sometimes take advantage of anonymous Twitter handles to get snarky about clients, but that social media can be an important way to connect with colleagues.

IP lawyer Brian Lynch, who is also a volunteer moderator at a Reddit forum, said solo and small firm practitioners, in particular, can benefit from talking to other lawyers on social media. The ABA opinion could have a chilling effect on lawyers looking for help via a blog or other online medium. Ultimately, Lynch said, that's not good for clients.

"More than anything, this opinion scares away lawyers who were on the fence about tweeting/blogging/etc. because most lawyers are so risk adverse when it comes to online activity," said Keith Lee, who runs Lawyersmack.com.

For what it's worth, I agree that Twitter and blogs are a great way for lawyers to connect. It would be a shame if the ABA opinion stops folks from talking publicly about litigation or from posting public documents from their cases. It doesn't have to, though. Just be careful. WJ



**Alison Frankel** updates her blog, "On the Case," multiple times throughout each day on Thomson Reuters Westlaw's Practitioner Insights. A founding editor of Litigation Daily, she has covered big-ticket litigation for more than 20 years. Frankel's work has appeared in The New York Times, Newsday, The American Lawyer and several other national publications. She is also the author of "Double Eagle: The Epic Story of the World's Most Valuable Coin."


© 2018 Thomson Reuters

# CASE AND DOCUMENT INDEX



© 2018 Thomson Reuters