



[State Bar Home](#)

CALIFORNIA BAR JOURNAL

OFFICIAL PUBLICATION OF THE STATE BAR OF CALIFORNIA

July 2009

Top Headlines

Opinion

MCLE Self-Study

Attorney Discipline

You Need to Know

Trials Digest

Public Comment

Contact CBJ

Archived Issues

Search CBJ

Go

E-mail scams continue to successfully target lawyers

By Diane Curtis
Staff Writer

Carmichael attorney Jana Aagaard got an unplanned lesson in Internet scams when she learned that someone was using her name to solicit business for a bogus legal client. Her persistent electronic sleuthing resulted in what looks like a happy ending: the culprit was found and the URL that contained her name was suspended. But domain names and access to them are vast, so Aagaard hopes her experience may serve as a cautionary tale to others.

Internet scams are on the rise, and California banks, legal groups and the State Bar report receiving growing numbers of complaints from lawyers about the electronic solicitations. The State Bar also issued an alert to lawyers about the proliferation of lawyer-aimed scams. California lawyers who answered the scammers have lost from \$75,000 up to \$2 million, bank officers say.



[\(Click to Enlarge\)](#)

Often, the scammers use the name of a real attorney to make a phony referral to another attorney with the idea of ultimately collecting a hefty sum from the attorney's own bank account. Typically, an attorney is asked to collect a debt, receives an authentic-looking check and is asked to deposit it, subtract his or her retainer and then send the rest to the "client." Too late, the attorney finds out that the check is no good. Aagaard wasn't specifically targeted for her money, but her good name was used to try to lure in other attorneys.

"Know who you're doing business with," advises State Bar President Holly Fujie. "If you deposit a check for \$500,000, you had better have a clear idea where that money is coming from. Attorneys should be the last people to fall for these scams," she adds. "Be careful."

For Aagaard, it all began the day after Memorial Day. She got a call from a New York lawyer who asked if his name meant anything to her. It didn't. "Well, I just got an e-mail from you," he said. Over the next couple of days, another half dozen lawyers called from several different states, asking basically the same question and informing her that her e-mail had said she was referring one of her clients, a South Korean company, to them.

"I knew right away it was fraud. It was theft. I was horrified," Aagaard said. Still, she Googled the URL with her name on it to make sure that, by some "weird, weird coincidence," there wasn't another lawyer with her name. The e-mail, it was clear, was meant to refer to her.

Thus began the search for the thief and a way to put an end to the misuse of Aagaard's good name. She called the State Bar — first the complaint hotline and then member services — and her membership page now notes that she may be an identity theft victim. She got in touch with her malpractice insurance carrier, who "didn't think there would be any problems" for her. She made a police report. She called the FBI, who told her to file a complaint with the Federal Trade Commission. She did.

But the help that actually made a difference, she said, came from a Utah lawyer who suggested looking up the domain owner's name on Whois.net and getting help from a company called ScamWarners.com. (ScamWarners is made up of volunteers who research complaints and won't reveal their identities for fear they'd be helping the scammers.) In the meantime, the calls from lawyers had stopped.

"I thought everything was good, but a week later, a whole slew of new e-mails went out" and she

started getting the lawyer calls again, this time more than two dozen. At the same time, ScamWarners said if Aagaard provided the "header" — with sender, recipient and time stamp information — they would see what they could uncover. They soon reported the registry had suspended the domain name.

Aagaard said the whole process was very frustrating because it took so much of her time, she didn't know how long it would take to resolve and she worried that someone might have fallen for a scam that had her name attached to it. "It seems to be [over] at this point," Aagaard says. "It's scary that it's so easy for scammers to do this."

Banks will immediately make funds available when a check is deposited by a customer, but if the check is bad and there's no way to recover the money, the loss is the customer's, not the bank's.

While the State Bar cannot provide legal advice on scams, the Ethics Hotline (1-800-238-4427) can direct lawyers to relevant authorities. "Generally, the same rules apply to Internet contacts as in-person contacts," says State Bar Deputy Executive Director Robert Hawley. "Don't be too quick to take on a new client unknown to you. As hard as it may be in this economy, prudence and due diligence still pay high rewards. Ask questions. Be up front about needing confirmation that the contact is who and what is claimed. Be cautious of the need for breakneck speed in processing money."

If a lawyer suspects an e-mail is a scam before establishing a relationship with a client, in most cases it can be reported to the authorities, adds Hawley. "That someone has contacted you in and of itself is not confidential except in rare cases. It gets more complex if you have begun the relationship and then suspect that you are being scammed. At this stage, the duty of loyalty and confidentiality kick in. But again, the standards are not different for Internet relationships and personal relationships. If you think a client is scamming you, you would normally confront the client, evaluate the response and continue the relationship or withdraw from it. If you suffered losses from being scammed, after withdrawal, you would write them off or pursue your civil or criminal remedies, respecting the duty to preserve confidentiality as appropriate."

San Francisco attorney Jacqueline Phillips received a scam e-mail sent directly to her by a man representing himself as the CEO of a Hong Kong electronics company. The letter included the Internet address of a real Hong Kong company. The return e-mail address used the CEO's name at a gmail address. Phillips began investigating, and, at the same time, she responded. "I was curious to find out if it was legitimate because it was written so well," she says.

She stopped the correspondence after she got a follow-up e-mail asking where the retainer agreement was, but in the meantime, she hit the books and the Internet to try to sort out what to do when a lawyer gets what might be a scam e-mail. "There may be ways to flush out" scammers, she said, such as getting tax ID numbers and making representation contingent on their agreement that a separate, segregated attorney-client account be established for deposit of only their funds.

Phillips, who is licensed in California, Florida and Hawaii, says since that initial e-mail, she has received several others. A particular problem in California, she notes, is the issue of when an e-mail correspondent becomes a client for purposes of assuming a client-attorney relationship. Phillips said it would be helpful for the California Supreme Court to issue a comment to the Rules of Professional Conduct to clarify when someone is or is not a client, so "that we attorneys are not afraid to report this type of scam to the FBI."

In the end, she reached some general conclusions: "There's a lot of fraud going on out there ... When it's too good to be true, you know it's a scam."

According to cyber experts, Internet scams are not going to stop anytime soon, especially in a bad economy. Not only do the scammers need the money more, they know that their targets are more vulnerable to earn-money-now solicitations.

"People become more desperate," said Craig Butterworth, spokesman for the National White Collar Crime Center, which works with the FBI to thwart and prosecute Internet scams and other crimes. "They're not as cautious as they might be otherwise."

Butterworth said that in the first three months of this year, online crime increased by more than 40 percent over the same period last year.

So what should lawyers do if they think they might be the target of a scam? The FBI's Patti Hansen recommends making a report immediately to the Internet Crime Complaint Center on the ic3.org Web site. If money has been lost, notify local police or the FBI, as well as the Internet

Crime Complaint Center.

The FBI and the Internet Crime Complaint Center ask:

Are you a safe Internet user? You may be at risk if you answer "yes" to any of the following questions:

- Do you visit Web sites by clicking on links within an e-mail?
- Do you reply to e-mails from companies or persons you are not familiar with?
- Have you received packages to hold or ship to someone you met on the Internet?
- Have you been asked to cash checks and wire funds to an employer you met online?
- Would you cash checks or money orders received through an online transaction without first confirming their legitimacy?
- Would you provide your personal banking information as a result of an e-mail notification?

For more information and to test your online practices, visit: www.LooksTooGoodToBeTrue.com.

To report an online crime visit: www.ic3.gov

If a relationship between an Internet client and an attorney has reached the point where the attorney has received what looks like a bona fide cashier's check, the Internet Crime Complaint Center recommends taking these steps to determine whether the check is counterfeit:

- Inspect the cashier's check.
- Ensure the amount of the check matches in figures and words.
- Check to see that the account number is not shiny in appearance.
- Be watchful that the drawer's signature is not traced.
- Official checks are generally perforated on at least one side.
- Inspect the check for additions, deletions or other alterations.
- Contact the financial institution on which the check was drawn to ensure legitimacy.
- Obtain the bank's telephone number from a reliable source, not from the check itself.
- Be cautious when dealing with individuals outside of your own country.

Other sources for information on preventing or reporting Internet scams are: www.fbi.gov; www.ic3.gov; www.ftc.gov; www.fcc.gov.

[Contact Us](#)

[Site Map](#)

[Notices](#)

[Privacy Policy](#)

© 2009 The State Bar of California