NORTH CAROLINA
LAWYERS WEEKLY

Feb. 22, 2010 www.nclawyersweekly.com

Law firms targeted in overseas e-mail scam

By GUY LORANGER, Staff Writer
guy.loranger@nc.lawyersweekly.com

The e-mail could have come from an overseas cyber café or a laptop right around the corner. All Steven Carr knows for sure is that it didn't come from a legitimate client.

It landed in his inbox on a late September day — a request from a Taiwanese company for assistance in collecting a debt — and it nearly led to Carr's firm suffering a six-figure theft from its trust account.

Months later, the Raleigh lawyer can look back at it with relief, knowing his firm escaped being the victim of an Internet scam that is targeting lawyers across the country.

"I imagine they're looking for small firms in a down economy who might see this as a good opportunity to establish new client relationships," Carr said. "But the truth is they're preying on people."

Sophisticated scam

What Carr and his firm encountered was an Internet-based counterfeit-check scam that has drawn the attention of the Federal Bureau of Investigation.

Unfortunately, some lawyers have discovered that it was a scam after it was too late. According to news reports, a Houston attorney was robbed of $182,500 last year, while an Atlanta lawyer lost $200,000.

"Because lawyers have trust accounts and are used to having large sums of money coming through their offices, I think they're being targeted," said Warren Savage, claims counsel for N.C. Lawyers Mutual.

"And these are much more sophisticated. It's not like they're sending out millions of e-mails and hoping they get a couple of bites. Some of these are more targeted and personal. There's so much information about lawyers that's out there today. They seem to know something about the lawyer and can tailor it."

According to Carr, the unsolicited e-mail he received came from a person

■ See **SCAM** on next page

SCAM

■ Continued from previous page

who claimed to be a representative of Silktex, a company located in Tainan, Taiwan. The "client" said he had learned about Carr through an online legal directory.

That wasn't so unusual. Carr said he has received e-mails from prospective clients from different parts of the country who learned about him or his firm, Ellinger & Carr, through directories such as Martindale-Hubbell.

What did strike Carr as odd: His firm focuses on areas such as affordable housing and community development, banking and finance, business law and employment law — not debt-collection or creditor's rights.

This client claimed that it needed local counsel to collect a delinquent account from a customer based in Morrisville.

A little skeptical, Carr did some research. He found an impressive-looking Web site for Silktex, and he learned that the Morrisville company was real.

He decided to send an engagement letter, which the fraudulent client signed and returned.

But later on, the client became evasive when asked about the terms of engagement and for details about the delinquent customer and account. It raised questions, Carr said.

"Anytime we start a relationship with a client, we set out the terms and scope of the engagement in a letter, as the State Bar encourages you to do," he said.

"But I couldn't get him to tell me exactly what he was engaging us for. I couldn't get a straight answer."

Within two weeks after being contacted by the client, the firm received what appeared to be a genuine invoice from Silktex along with an "official check" for $360,000 drawn on a Citibank account in New York. The Morrisville customer was listed as "remitter." According to the client, the customer had agreed to pay the account.

The client instructed the firm to deposit the check in its trust account and to wire the funds — minus retainer fees — to the client's Japanese associates at an overseas account.

According to Susan Ellinger, Carr's law partner, that package was one of several red flags that had begun piling up.

In particular, the package came from an address in Hamilton, Ontario, not from Morrisville, and with a phone number that appeared to be a residential listing.

When the firm called the number, the person who answered the phone claimed to have no knowledge of the package that had been sent to the firm.

Susan Ellinger and Steven Carr review the file they compiled after receiving an e-mail they believed was part of an Internet counterfeit-check scam. *Photo by Guy Loranger*

Instead of depositing the check, the firm asked the bank to verify that it was real. Within a week, Citibank reported to the firm's bank that the check was counterfeit.

Fortunately, the firm made no disbursements from its trust account.

"We're a small enough firm that we touch every check here. But a big firm might have a system where the check comes in and goes to an accounting department in another city. … This is really a cautionary tale for big or small law firms," Ellinger said.

Ethical duty?

After discovering that it was a scam, Carr and Ellinger figured their duty would be to report the situation to law enforcement.

But would that conflict with their ethical duty, under Rule of Professional Conduct 1.6(a), to not disclose any confidential client information?

According to to Alice Mine, the State Bar's ethics counsel, the situation would actually fall under an exception to that general duty.

Under Rule 1.6(b)(2), a lawyer may reveal information protected from disclosure to the extent the lawyer "reasonably believes necessary" to prevent the commission of a crime by the client, which would include situations where the lawyer is the target of the crime.

"That's an exception that's clearly on point," Mine said. "The standard in the rule is that you can reveal the protected information to the extent the lawyer reasonably believes necessary.

"So, if you have a reasonable belief that this client is attempting to defraud you, then you can make the disclosure. If it turns out that you were wrong, but your belief was reasonable under the circumstances, then you have not violated the rule."

Because they avoided being victims, Carr and Ellinger decided not to report the scam to law enforcement. However, Carr did file a complaint with an FBI-operated Web site, www.IC3.gov, which compiles reports of counterfeit-check scams.

According to Noelle Talley, a spokesperson for the attorney general's office, the state's consumer-protection division received a phone call about a similar scam six months ago. However, because the caller did not file a written complaint, there were no details.

Savage said his office at N.C. Lawyers Mutual has received calls from attorneys in recent months about the scam, which he said could trigger professional liability in certain circumstances or a firm's business-loss policy.

Whenever a firm has been targeted by such a scam, Savage suggests calling the bank immediately and alerting them to the possible fraud.

However, Savage said there have been reports of some scammers going so far as to provide lawyers with a toll-free "bank" hotline in which an operator, purporting to be a bank employee, tells callers that the counterfeit check is legitimate.

That sophistication is chilling, Savage said.

Carr said he at least feels more savvy about it now.

The other day, he received an e-mail from Qin Lee Wang of the Dalian Leong Yang Trading Co. Ltd.

"The name is different," Carr said, "but the pattern's the same."