Caution: Internet Scammers Targeting Lawyers

by
Patrick R. Burns, First Assistant Director
Minnesota Office of Lawyers Professional Responsibility

Reprinted from *Minnesota Lawyer* (February 2, 2009)

What would your reaction be if you received an e-mail from a government functionary in Nigeria telling you that he has access to several million dollars of unused oil pipeline funds and requires your assistance, for a generous fee, in transferring the funds out of the country?

Hopefully, most would recognize this for what it is - a variation of a fraud known as a 419 fraud or Nigerian fraud.

What ultimately happens to anyone stumbling into this offer is that he or she is tricked into forwarding considerable "advance fees" in order to free up the nonexistent millions of dollars and, of course, no money is forthcoming to the victim.

A new and more sophisticated variation of this scheme is targeting lawyers. This scheme, often utilizing the cover of what appear to be legitimate Asian businesses, involves e-mails sent to lawyers asking that they assist in the collection of debts owed to them by other businesses.

Typically, the e-mail will appear to originate from a legitimate foreign business and will ask the lawyer to assist in collecting a debt owed from another legitimate business. The scammers will, of course, provide fake contact information to the lawyer and have even been known to direct the lawyer to fake company websites that have been set up to give the air of added legitimacy.

The scammers agree to pay the lawyer a substantial retainer for their collection services and ask that an appropriate retainer agreement be sent to them. Shortly thereafter the lawyer gets word that the debtor company has agreed to make a substantial payment toward the alleged debt. The scammers then instruct the lawyer to deposit that payment into their trust account, pay themselves their retainer and then wire the balance of the funds to the scammer's account. The lawyer subsequently receives what appears to be a legitimate check drawn on the corporate account of a legitimate business or even a money order or certified check. These checks are forgeries.

Unfortunately, it may take as much as two to three months for the fraudulent check to be discovered. In the meantime, the lawyer victim disburses funds from the trust account to themselves for the retainer promised and to the scammer as the proceeds of the collection action. Once the nominal issuer of the check reports it as a fraud, the bank upon which the trust account disbursements were drawn will debit the trust account to recover the funds. Often the result is that the trust account is overdrawn and the lawyer is out the money

sent to the scammers.

Over the last year the OLPR has been notified of at least three lawyer trust accounts that have been overdrawn as a result of the lawyer falling victim to these scams.

In these troubled times lawyers are loathe to turn away any business that comes in the door. Nevertheless, caution must be exercised.

Typically these scams involve funds in the tens or hundreds of thousands of dollars. Utilizing a pooled trust account to process the phony funds places the legitimate client funds in that account at risk and exposes the lawyer to substantial liabilities.

What can you do to protect yourself?

Exercise extreme caution when dealing with a client you have never personally met. Ask the potential client for references and check with third parties. Ask them how it is they found you and decided that you would be the attorney they wish to retain. If the substantial payment from the debtor follows quickly upon the heels of your retention, ask yourself why a lawyer intermediary is even necessary in the transaction. In other words, is that $10,000 retainer in exchange for services no more complicated than running the funds through your trust account too good to be true?

Contact the issuer of the check and/or the bank upon which the check is drawn to inquire whether the check is legitimate. When doing so, do not use the phone numbers printed on the face of the check – scammers have been known to alter these phone numbers so that you will end up speaking with them rather than the actual company involved. Look up the true contact information in the phone book or on the Internet.

Finally, the FBI and others maintain websites detailing various frauds being perpetrated. It is worthwhile checking these out since, in many instances, the scammers are using a particular front company or companies repeatedly and the company that has contacted you for collection services may be listed as one being utilized to perpetrate these scams.