



THE RISK MANAGER

A QUARTERLY NEWSLETTER BY LAWYERS MUTUAL INSURANCE COMPANY OF KENTUCKY

Special Edition: SCAMS!

LAWYERS REMAIN LUCRATIVE TARGETS FOR SCAMMERS

IF LAWYERS EVER THOUGHT that Internet scams directed at them were a one-off event, there can be no doubt now that scams are a permanent fact of life for the practice of law. This change introduces a new dimension to lawyer risk management. Now lawyers must stay current on developments by scammers and hackers attempting to infiltrate firm databases and trick lawyers into fraudulent Internet transactions. In this special edition we provide an overview of the current scams that lawyers must recognize, risk management guidelines, and the professional responsibility rules that apply to scam attacks.

RANSOMWARE

Earlier this year CNN reported that “Cyber-criminals collected \$209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers. This is not a new scam, but is so successful that it is expanding rapidly. At a computer security conference in Boston late last year, the FBI advised that some of the ransomware is so effective that in may not be possible to recover data without paying the ransom.

As we have reported in prior newsletters, the most common type of ransomware, Cryptolocker, scrambles all the data files on your computer with virtually unbreakable encryption. You

learn you are infected when a pop-up window tells you that your data has been scrambled and will be deleted unless you pay a ransom within a very short period of time, typically 48 hours or so. The ransom is typically in the range of \$100 to \$300, but can be much higher depending on the scope of files encrypted. Ransom is usually payable only in bitcoins, a type of virtual currency that makes payments untraceable.

Our risk management advice to avoid ransomware scams is:

- ◆ Use computer-security software to block suspicious emails – be sure to update regularly.

CONTINUED ON PAGE 2

TRUST ACCOUNT SCAMS

These scams are not new and we would hope that every Kentucky lawyer who reads this newsletter is well familiar with how “the email from Nigeria” scam works. In our Fall 2015 Newsletter we reported on the Bar of the City of New York Committee on Professional Ethics Formal Opinion 2015-3: *Lawyers Who Fall Victim to Internet Scams* (April 2015). This opinion is an outstanding consideration of trust account scams and is readily available on the Internet. The key risk management advice the opinion offers is:

A lawyer’s suspicion should be aroused by any one or more of these common “red flags” indicating a scam:

- ◆ The email sender is based abroad.
- ◆ The email sender does not provide a referral source. (If the email sender is asked how he found the firm, he may respond that it was through an online search. If prospective clients rarely approach the recipient attorney based on an Internet search, this should be an immediate red flag.)
- ◆ The initial email does not identify the law firm or recipient attorney by name, instead using a salutation such as “Dear barrister/solicitor/counselor.”

CONTINUED ON PAGE 7

INSIDE THIS ISSUE:

Ransomware	1
Trust Account Scams	1
Phishing Scams	2
Bar Association Scam Warnings	3
Scam Professional Responsibility	6
Money Mule Scams *	7
Read Our Nine Other Articles on Scams Targeting Lawyers	8



Lawyers Mutual

www.lmick.com

MEMBER NATIONAL ASSOCIATION OF BAR RELATED INSURANCE COMPANIES

PHISHING SCAMS

DEFINITION:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an email. They take the form of a message, allegedly from your bank or an online retailer you deal with that suggests your account has been compromised or that payment is overdue. Phishing scams are usually bulk emails sent to large numbers of people. Even if only two or three per cent of recipients fall for them, hundreds or even thousands of people can be victimized. (LAWPRO Magazine, Lawyers' Professional Indemnity Company, "Serving Indigenous Clients" (Vol. 15 no. 1).



PHISHING RISK MANAGEMENT:

Don't reply to email, text, or pop-up messages that ask for your personal or financial information. Don't click on links within them either – even if the message seems to be from an organization you trust. It isn't. Legitimate businesses don't ask you to send sensitive information through unsecure channels.

SPEAR PHISHING:

The "spear" in spear phishing alludes to the fact that messages are targeted to specific individuals. Spear phishing messages are more convincing because they are personally addressed, appear to be from someone you already know, and may include other detailed personalized information.

....

Educate the lawyers and staff at your firm to make sure they will not fall for a spear phishing scam. Follow firm

processes and procedures for the review and approval of financial transactions – and don't bypass them due to urgent circumstances. Never share confidential client or firm information without being sure it is appropriate to do so by getting confirmation from someone familiar with the file. Be on the lookout for and question any last minute changes on fund transfers or payments. (LAWPRO Magazine, Lawyers' Professional Indemnity Company, "Serving Indigenous Clients" (Vol. 15 no. 1).

WHALING

Phishing attacks directed specifically at senior executives and other high profile targets within businesses appearing to be sensitive business matters. Often come in the form of subpoena, customer complaint, or executive issue. (Wikipedia)

CLONE PHISHING

A legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. (Wikipedia) 

RANSOMWARE

CONTINUED FROM FRONT PAGE

- ◆ Never open attachments from a source you don't recognize.
- ◆ Require all firm members to be especially vigilant before downloading photos or PDF files, even if apparently from known sources, to avoid downloading an executable file that could download malware.
- ◆ Establish off-site data backup systems and procedures for alternate access to the network.
- ◆ Backup and archive all files nightly in an off-line system that is not connected to the vulnerable main office system. Some firms nightly backup all files on tape and lock the tapes in a fireproof safe in the office. They then further backup the files in off-site storage.
- ◆ Include home computers, laptops, iPads, and smart phones in office cyber security programs.
- ◆ Review computer system backup architecture and file-sharing architecture to assure that a single event of a malware download cannot infect both the main system and backup systems. 

“ANY SCAM ARTIST THAT DOESN'T USE THE INTERNET OUGHT TO BE SUED FOR MALPRACTICE.”

*Joseph Borg,
Alabama Securities
Commissioner*

BAR ASSOCIATION SCAM WARNINGS

The following are verbatim state bar alerts to its members concerning scams:

KENTUCKY BAR ASSOCIATION

WARNING: POTENTIAL SCAM TARGETING BAR ASSOCIATIONS' MEMBERS

Other state bar associations are reporting that their members have been targeted by scammers requesting dues payments. The KBA has not received any reports from our members, but we ask that you be careful as the 2016-17 dues invoices will be mailed around July 8, 2016. When you pay your KBA dues online, always check the web address to make sure you are on the correct site: <https://www.kybar.org>. In addition, if you receive any emails from the KBA, all of our emails are sent from the domain: [kybar.org](https://www.kybar.org). **If you are unsure about an email or a website, please contact us at (502) 564-3795.**

NORTH CAROLINA STATE BAR ASSOCIATION

WIRE INSTRUCTION FRAUD CONTINUES TO PLAGUE NORTH CAROLINA LAWYERS

Over the last two weeks, Lawyers Mutual (*North Carolina*) has received multiple reports of North Carolina attorneys who were targeted by scammers attempting to divert seller closing proceeds following real estate transactions. Unfortunately, several of these attacks were successful and hundreds of thousands of dollars were stolen and are very unlikely to be recovered. However, several attacks were foiled by attorneys and staff members who approached transactions with a high degree of skepticism.

While the details of the recent scams are emerging, it appears hackers first became aware of the closing by compromising email accounts of differing [*sic*] parties. Sometimes the attorney account was compromised, sometimes the Seller's account was compromised but the most common scenario was the Realtor's account was being monitored by international criminal organizations. The foreign-based hackers would observe the account, likely for several weeks, and only actively intervene once an understanding of the business practices were obtained and a significant wire was to be produced. In the interim, the unsuspecting Realtor would continue to use the account unaware his or her client and the closing attorney were being set up to be robbed.

Below are some tips that will help your office avoid falling victim to the latest series of scams.

HAVE THE SELLER SIGN THE WIRING INSTRUCTIONS AT THE CLOSING CEREMONY IN THE PRESENCE OF THE ATTORNEY.

WIRE TRANSFER REQUEST



1. EVERY wire request should be verified and the more personal the verification, the better.
 - ◆ The best way to verify wiring instructions is to have the Seller sign the wiring instructions at the closing ceremony in the presence of the attorney. We know of no wire fraud that has taken place when this has occurred, and even if it did, the closing attorney would likely be insulated from liability by the doctrine of contributory negligence. (*Note: N.C. still has the doctrine of contributory negligence*)
 - ◆ If the Seller is unable to attend the ceremony, we recommend the wiring instructions be included in the same package in which the deed is delivered. In these situations, have the Seller sign wiring instructions and have the signature notarized, if possible. Even then, we recommend the Seller verify the closing instructions over the telephone via a call initiated by the law office, using contact information from very early in the file prior to any discussion of proceeds and wires.

CONTINUED ON PAGE 4

“PEOPLE WHO THINK MONEY CAN DO ANYTHING MAY VERY WELL BE SUSPECTED OF DOING ANYTHING FOR MONEY.” *Mary Poole*

BAR ASSOCIATION

CONTINUED FROM PAGE 3

- ◆ Confirming a telephone call verification via email is a good practice and a great way to document the file. However, **an email verification alone is inadequate.**
- 2. Do not accept changes to wiring instructions.
- 3. If wiring instructions are attached to an email from a free email service (gmail, yahoo, aol.com, nc.rr.com, etc.) they should be assumed to be fraudulent and extra diligence should be taken in the verifying their authenticity. Sometimes hackers will set up an alias account with a very similar name (frequently dropping or swapping letters) to send modified instructions so the authentic user is not aware of their presence. Examining the account name in detail is a good idea; however, as the hacker already has access to the original account, he or she may not take this step and will use the same account that all other correspondence used.
- 4. Real Estate attorneys should not be using free email accounts. These accounts have major security concerns and are likely being mined for data by their providers in violation of Rule 1.6 of the Rules of Professional Conduct. In addition, they are very unlikely to be compliant with the ALTA Best Practices.
 - ◆ If you are currently using a free service, immediate action should be taken to find a more secure and professional alternative. In the interim, it is possible to see when and from where the free account was recently accessed. Here is a link explaining how to do it for gmail accounts: <http://www.groovypost.com/howto/check-gmail-login-activity/> Other services should have similar abilities. If you see suspicious activity, please immediately change account passwords and contact your professional liability carrier along with your cyber or crime carrier.
- 5. Be very suspicious of wires going to any account that is not in the name of the Seller. Also, be suspicious of any account with a geographic location different than the Seller. Why is a North Carolina Seller relocating to New York sending a wire to Wisconsin? There are some reasons for the different names and odd locations, but these are red flags, which should be explored in detail (and not via email).
- 6. Do NOT send wires overseas. Once money leaves the United States, it is likely gone forever.

- 7. Regularly change your passwords
- 8. We understand these policies appear harsh and some pushback may occur. However, hacking crimes can be devastating to a law firm's finances and reputation. Explaining the policy up front is a good way to limit negative actions. Below is sample language I recommend to be included in your Seller engagement letter.

Funds Availability Policy

It is our goal to make real estate commission checks and funds available as soon as practical following closing. However, NC State Bar Rules expressly prohibit disbursing any closing funds prior to recording. Should you request funds be wired, our office can accommodate the request for a fee of \$____.00. In order to prevent fraud and protect your proceeds, all wiring instructions will be verified and you will be required to sign the instructions at the closing ceremony. **THIS OFFICE WILL NOT ACCEPT CHANGES TO WIRING INSTRUCTIONS.**

PHONE SCAM SPOOFING LAWYERS' PHONE NUMBERS TARGETS NC CITIZENS

We have recently been made aware of a new phone scam targeting North Carolina citizens. In this new scam, the caller purports to represent a law firm collecting a debt. The caller threatens the citizen with arrest if the debt isn't paid via credit card during the phone call. The phone call has been reported to go like this:

- ◆ "I am with [law firm] calling to collect a debt. If you do not give me a credit card number and pay this immediately, the sheriff is standing by to come to your house and arrest you."

Victims of these scams are chosen at random. The scammers are hoping to scare vulnerable people into thinking they must provide credit card information to avoid going to jail. Unfortunately, there is nothing law firms can do to prevent scammers from spoofing their phone number.

Law firms can help alert the public to this scam. Here are some steps you can take to help:

- 1. Alert your family and friends. Anyone could be a victim. Make your staff aware of the issue so they can address phone calls should your firm receive them.

CONTINUED ON PAGE 5

“BUT WHEN TO MISCHIEF MORTALS **BEND THEIR WILL, HOW SOON THEY FIND FIT INSTRUMENTS OF ILL!**” Alexander Pope

BAR ASSOCIATION

CONTINUED FROM PAGE 4

2. If your firm has been scammed, consider posting a notice on your website. Sample text listed below:
 - ◆ This firm **DOES NOT** collect debt via phone call. If you receive a phone call to collect debt purporting to be from this law firm, **please do not provide personal or financial information to the caller.** If possible, write down the name of the law office that appeared on the caller ID and hang up.

ALERT: NEW PHISHING ATTACK – EXERCISE CAUTION

There is a new phishing scam targeting bar members across the country. The fraudulent email pretends to be a communication from the State Bar or Bar Association.

There are several versions of this scam. The most common are: “[state] Bar Complaint,” “[state] Bar Association Past Due Notice,” and “Lawyers and judges may now communicate through this portal.”

In many instances, scammers pull names from State Bar or Bar Association websites to add legitimacy to their scam.

If you receive one of these fraudulent emails:

1. Do not respond or open any attachments.
2. Delete the email immediately. These emails likely contain malicious software or contain links to phony websites.
3. If you think your account has been compromised, change your password **immediately**.

STATE BAR OF ARIZONA

STATE BAR WARNS ABOUT NEW SCAM DIRECTED AT ATTORNEYS AND THEIR CLIENTS

The State Bar of Arizona is warning its members about a new type of scam directed at both attorneys and their clients. This sophisticated scam exploits the attorney/client relationship and defrauds consumers of their money.

How the scam works:

- ◆ The client receives a phone call.
- ◆ The caller ID shows the number belongs to the attorney.
- ◆ The client is told that they need to pay additional money.

- ◆ The client is then given a toll-free number to call.
- ◆ When the client calls, they are directed as to how to pay the money.

This scam works through a process known as “Caller ID Spoofing”. “Spoofing” allows a caller to change their ID to reflect any desired number, which will then show up on the recipient’s caller ID. Previous “spoofing” scams, for example, have involved callers using a number that belongs to the IRS.

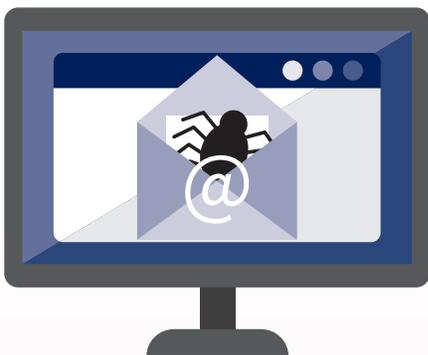


“What makes this most recent case especially troubling is that the scammers have linked the attorney with the client,” said John Phelps, CEO/Executive Director of the State Bar of Arizona. “While this information may be publicly available through court documents, we have not seen it used in this way. This recent case involved bankruptcy court and the client was told they needed to pay more money to a creditor. Fortunately, the scam was caught in time and no money was lost.”

Attorneys should consider advising their clients about the potential for this type of scam. Consumers should confirm with their attorneys before sending money. Both attorneys and consumers should file a report with the FBI’s Internet Crime Complaint Center (IC3) at www.ic3.gov if they are a victim of this scam. 

SCAM PROFESSIONAL RESPONSIBILITY

The Bar of the City of New York Committee on Professional Ethics, Formal Opinion 2015-3: *Lawyers Who Fall Victim to Internet Scams* (April 2015) provides a helpful analysis of the ethics and risk management issues facing lawyers dealing with emails believed to be fraudulent. The following extracts cover the key guidance of the opinion.



May You Ignore an Email that Appears to be Fraudulent?

As the California State Bar Association Committee on Professional Responsibility and Conduct (“COPRAC”) has noted: “The best approach is to ignore such solicitations altogether.” COPRAC Ethics Alert: *Internet Scams Targeting Lawyers* (Jan. 2011). An attorney has no ethical obligation to respond to an unsolicited email inquiry from a prospective client. See NYSBA Ethics Op. 833 (2009) (“An attorney is not ethically required to respond to unsolicited letters from incarcerated individuals requesting legal representation.”). If the attorney responds to the email, however, he should be mindful of certain ethical obligations that arise once he engages in those communications.

Confidentiality Issues When Reporting a Suspected Fraudulent Email

(Applicable Kentucky Rules of Professional Conduct (KRPC) 1.6, Confidentiality of Information, and 1.18, Duties to Prospective Client)

An attorney who discovers that he is the target of an Internet-based trust account scam does not have a duty of confidentiality towards the individual attempting to defraud him, and is free to report the individual to law enforcement authorities, because that person does not qualify as a prospective or actual client of the attorney.

However, before concluding that an individual is attempting to defraud the attorney and is not owed the duties [of confidentiality] normally owed to a prospective or actual client, the attorney must exercise reasonable diligence to investigate whether the person is engaged in fraud.

What is Reasonable Diligence When Investigating Suspected Email Fraud?

(Applicable KRPC 1.1, Competence)

[A]n attorney who receives an email solicitation from an unknown individual should conduct a reasonable investigation to ascertain that the email sender is a legitimate prospective client. The due diligence may include verifying the accuracy of the information provided by the email sender, such as names, addresses, telephone numbers, website addresses, and referral sources. The attorney should resist the temptation to depart from his customary intake procedures, such as performing conflict checks, verifying the prospective client’s business and financial status, executing a retainer agreement, and obtaining an advance retainer.

Client Trust Account Violations

(Applicable KRPC 1.15, Safekeeping Property, and 1.4, Communication)

[B]ecause Internet-based trust account scams may harm other firm clients, a lawyer who receives a request for representation via the Internet has a duty to conduct a reasonable investigation to ascertain whether the person is a legitimate prospective client before accepting the representation. A lawyer who discovers he has been defrauded in a manner that results in harm to other clients of the law firm, such as the loss of client funds due to an escrow account scam, must promptly notify the harmed clients. 

THE RISK MANAGER
PUBLISHED BY LAWYERS MUTUAL INSURANCE COMPANY OF KENTUCKY

DEL O’ROARK
Newsletter Editor

This newsletter is a periodic publication of Lawyers Mutual Insurance Co. of Kentucky. The contents are intended for general information purposes only and should not be construed as legal advice or legal opinion on any specific facts or circumstances. It is not the intent of this newsletter to establish an attorney’s standard of due care for a particular situation. Rather, it is our intent to advise our insureds to act in a manner which may be well above the standard of due care in order to avoid claims having merit as well as those without merit.

FOR MORE INFORMATION ABOUT LAWYERS MUTUAL,
CALL (502) 568-6100 OR KY WATS 1-800-800-6101 OR
VISIT OUR WEBSITE AT LMICK.COM.

“BELIEVE NOTHING AND BE ON YOUR GUARD AGAINST EVERYTHING.” *Latin Proverb*

MONEY MULE SCAMS *

The PenFed Credit Union in an alert it issued about money laundering described a Money Mule “as someone who transfers and launders money acquired illegally in the following manner: in person, through a courier service, or electronically (for example, by using your account with PenFed or another financial institution to transfer the funds) on behalf of others. Money Mules are often recruited online in what they believe is a legitimate reason – unaware that the money is the product of a crime. The money is transferred from the Mule’s account to the scammer, typically in another country.”

The alert identified these risk of becoming a Money Mule:

- ◆ Potential criminal prosecution.
- ◆ Financial Loss: Mules are often found personally liable for repaying the losses.
- ◆ Loss of personal information and identity theft.
- ◆ Having financial accounts frozen by law enforcement during the investigation.

Warning signs are listed as:

- ◆ The proposition involves transferring money or merchandise.
- ◆ The offer originates from (or the recipient of the funds is in) another country.
- ◆ All communication and transactions are online; you have not personally met with anyone.
- ◆ The email address connected to the offer or solicitation is ‘unofficial.’ For example, the solicitor is using a generic Gmail, Hotmail, or Yahoo account.
- ◆ You are asked to wire money from your account to strangers.

Lawyers are ripe targets for money laundering scams because fraudsters know from Client Trust Account scams that lawyers are well situated to facilitate money transfers. The twist for lawyers in this scam is that the certified check they receive, unlike the one in trust account scams, is not a forgery. The third party receives real money and the lawyer gets a real fee. When the money laundering crime is discovered, the lawyer-Money Mule should expect no mercy from prosecutors. 

* Source: PenFed Credit Union, “Money Mule scams are on the rise.”

TRUST ACCOUNT SCAMS

CONTINUED FROM FRONT PAGE

- ◆ The email uses awkward phrasing or poor grammar, suggesting that it was written by someone with poor English or was converted into English via a translation tool.
- ◆ The email is sent to “undisclosed recipients,” suggesting that it is directed to multiple recipients. (Alternatively, the attorney recipient may be blind copied on the email.)
- ◆ The email requests assistance on a legal matter in an area of law the recipient attorney does not practice.
- ◆ The email is vague in other respects, such as stating that the sender has a matter in the attorney’s “jurisdiction,” rather than specifying the jurisdiction itself.
- ◆ The email sender suggests that for this particular matter the attorney accept a contingency fee arrangement, even though that might not be customary for the attorney’s practice.
- ◆ The email sender is quick to sign a retainer agreement, without negotiating over the attorney’s fee (since the fee is illusory anyway).
- ◆ The email sender assures the attorney that the matter will resolve quickly.
- ◆ The counterparty, if there is one, will also likely respond quickly, settling the dispute or closing the deal with little or no negotiation.
- ◆ The email sender insists that his funds must be wired to a foreign bank account as soon as the check has cleared. (The sender often claims that there is an emergency requiring the immediate release of the funds.)
- ◆ The email sender or counterparty sends a supposed closing payment or settlement check within a few days. The check is typically a forged certified check or a cashier’s check, often from a bank located outside of the attorney’s jurisdiction. 

“GET NERVOUS IF A PLANNER OR ADVISOR SPENDS TIME BRAGGING ABOUT THE INVESTMENT RETURNS OF HIS OR HER CLIENTS.” Steven T. Goldberg



Lawyers Mutual

www.lmick.com

PRESORTED STANDARD
U.S. POSTAGE
PAID
LOUISVILLE, KY
PERMIT NO. 879



Waterfront Plaza
323 West Main Street, Suite 600
Louisville, KY 40202



FOR MORE INFORMATION ABOUT
LAWYERS MUTUAL, CALL (502) 568-6100
OR KY WATS 1-800-800-6101 OR
VISIT OUR WEBSITE AT LMICK.COM.

LAWYERS MUTUAL INSURANCE
COMPANY OF KENTUCKY
BOARD OF DIRECTORS

- RUTH H. BAXTER
Carrollton
- GLENN D. DENTON
Paducah
- CHARLES E. "BUZZ" ENGLISH, JR.
Bowling Green
- DOUG FARNSELY
Louisville
- WILLIAM R. GARMER
Lexington
- ANNE MILTON MCMILLIN
Louisville
- JOHN G. MCNEILL
Lexington
- DUSTIN E. MEEK
Louisville
- ESCU L. MOORE, III
Lexington
- RALPH C. PICKARD, JR.
Paducah
- JOHN G. PRATHER, JR.
Somerset
- CHRISTOPHER L. RHOADS
Owensboro
- MARCIA MILBY RIDINGS
London
- BEVERLY R. STORM
Covington
- DANIEL P. STRATTON
Pikeville
- R. MICHAEL SULLIVAN
Owensboro
- J. TANNER WATKINS
Louisville
- MARCIA L. WIREMAN
Jackson

READ OUR NINE OTHER ARTICLES ON SCAMS TARGETING LAWYERS

Go to www.lmick.com, click on **Resources**, click on **Subject Index**, go to **Scams**, select an article.

1. Are You Ready For The Next Scam Targeting Lawyers?
2. Do You Know What a "Typosquatter" Is?
3. Keeping Up with Lawyer Scams - Cryptolocker and Ransomware
4. Lawyer Scams Continue to Plague Kentucky Lawyers
5. Lawyer Scams I: Fictitious Foreign Company Seeks Representation In Collection Matter
6. Lawyer Scams II: Business Loan Fraud; Debt Collection Fraud
7. Lawyer Scams III: Panel Discussion of the Problem
8. Lawyer Scams: Nigeria Strikes Again
9. The Latest Scam of Special Interest to Lawyers: Client Deposits Lawyer's Trust Account Check By Phone Then Returns Check and Gets Wire Transfer From Lawyer

