Avoiding Financial Fraud and Scams at Your Law Firm

Nota by M&T Bank

The number of scams targeting lawyers, law firms, and their clients is on the rise. With today's sophisticated technology, the severity of these scams is constantly evolving, and more and more firms are falling victim to financial fraud. To protect yourself, your team, and your clients, this article will outline the most effective methods for avoiding financial fraud and scams at your law firm.

How Scams Work

Since most law firms rely on digital communication with clients and prospects today, you must be diligent with all transactions and solicitations. Anytime you are conducting a transaction, it is important to exercise caution and remain skeptical anytime money is leaving your firm.

Arming yourself with knowledge, doing your due diligence, and taking action to protect your firm will help to stop scammers in their tracks so that you can avoid falling victim to their ruse. In this article, we will identify some of the most common red flags to be on the lookout for, and how you can protect your firm from fraudulent activity.

Wire Fraud Scams

During a wire fraud scam, social engineering is used to transfer funds to an unauthorized recipient. Social engineering is a method in which scammers manipulate their victims to gain confidential information that will allow them to complete a fraudulent transaction.

A cybercriminal will impersonate an individual that the victim knows, and will use that person's email address and signature to get the victim to wire money to the criminal's bank account. They may imitate a colleague or client who is requesting that funds in one of your accounts be distributed to them and may even request that any retainer fees be held in escrow to avoid paying for your services.

In many cases, scammers make mistakes that give away their plan. And these are the clues you and your staff should look out for. Their email may be written in broken English, when you know that the client they are impersonating is a native (or excellent) English speaker. They may also provide inconsistent contact information, such as a telephone number from one geographic location, and an address in another.

If you notice multiple inconsistencies, grammatical errors, and otherwise question the authenticity of the "client", chances are that a scammer is behind the inquiry, and you should not send any money to them until or unless you can verify their identity.

Check Scams

Check scams continue to plague law firms across the country. As technology continues to evolve, it has become increasingly difficult to identify phony checks. Here are a few ways to verify whether a check is authentic and valid:

- Ensure that the check was issued by a reputable bank
- Check the microprinting on the signature line
- Be sure that the back of the check reads “original document”
- Check for discoloration or ink smudging that could indicate that the check was tampered with

If you are questioning the validity of a check, it is always best to investigate. If the check was distributed by a reputable bank, you should call the bank to verify that the account in question has available funds to cover the costs. The bank will be happy to assist you to ensure that you are not being scammed.

In addition, it is in your best interest to avoid writing out checks until funds have settled. This will provide plenty of time to verify the validity of the account. Do your due diligence and always trust your instincts. If something feels off, it probably is!

Email Scams

Phishing and social engineering are serious issues for law firms. Since it is rare for frauds to get on the phone with their intended victims, they will attempt to communicate exclusively through the internet to set up their scheme.

Scammers will often spoof an email address to trick you or someone at your firm into believing that they are emailing a client or legitimate contact. Be sure to double check every email to verify that the address is spelled correctly, and to confirm that you are communicating with the intended recipient.

With a phishing scheme, the scammer will typically make contact with a sense of great urgency, requesting information or action on your part immediately. If you notice that a client is reaching out with abnormal or unnecessary urgency, and a request that deviates from the original agreement or plan, that is a sign that you may be dealing with a phishing scheme. Unless proper action is taken, here is how a scheme will usually play out:

1. The “client” will sign your retainer agreement, and then reach out to let you know that your services are no longer needed.
2. You receive a settlement check that is deposited into your trust account.
3. The “client” requests a wire distribution of the settlement funds, typically into a foreign account.
4. Once the funds are distributed and it is determined that this transaction was a scam, you will now be stuck with an overdrawn account, and now owe that balance to the bank.

This situation can cause a great deal of distress, so be sure to do your due diligence during every transaction and verify the authenticity of each contact and payment.

Dishonest Employees

Unfortunately, law firms are at risk for embezzlement at the hands of dishonest employees. While there is no clear-cut answer for why this occurs, a poor job market and unstable economy increase the risk of employees stealing from your firm.

When bringing new team members on board, it is crucial to thoroughly screen each candidate, and be on the lookout for red flags and warning signs, such as:

- History of frequent job changes
- Recent or frequent relocations
- A history of criminal activity
- Substance abuse
- Living outside of their means
- Financial issues
- Significant debt
- Gambling habit

How to Mitigate Risk

With so much potential for fraud, both internal and external, it is up to you to do everything you can to protect your firm. Luckily, there are plenty of safety measures that you can implement to lower your risk.

Train Employees to Recognize Scams

All of your employees should be kept up to date on the latest scams. Training your employees to recognize scams will ensure that your firm is protected from all angles. Assistants, attorneys, administrators, and paralegals should all be kept in the loop, and have a firm grasp on the most appropriate protocols to implement in every situation.

Make sure employees feel comfortable reporting the small mistake of clicking on a spam link, do not let the fear of getting in trouble supersede the importance of reporting and mitigating the damage.

Utilize Security Measures

There are a number of security measures that you can utilize to protect your firm and your money.

Activate Two-Factor Authentication

You should activate two-factor authentication (2FA) before transferring any funds. Better, be sure to implement 2FA for everyone in your firm for any service that offers it. It is important to call the phone number provided by the client or point of contact to verify their identity. If you notice that there are any sudden requests for changes to a transaction or request, that is a red flag that should put you on high alert.

No money should ever leave your firm without direct communication with the receiving party. This is a quick and easy way to confirm whether the intended recipient is who they claim to be over email. Authentic clients should have no problem with your request to speak with them over the phone to verify their identity. If the person gives you a hard time, or is hesitant to get on the phone, that is another red flag that you may be dealing with a fraud.

Email

Whenever possible, you should use security measures such as encrypted emails or secure communication portals to reduce risk. If you receive any questionable, unsolicited emails, do not open them! It is especially important to refrain from opening any links or attachments within a suspicious email.

Internet

Did you know that up to 64% of lawyers use the cloud in their practice? While the cloud has proven to be a valuable asset and is used by law firms every day, be sure that you are selecting a reputable provider, and ask them questions about their security measures, and their privacy practices. If they cannot guarantee that your data will be protected, steer clear and speak with other providers. If you are unsure of their “tech speak”, consult with a neutral technology consultant or advisor. Many Bar associations offer technology and practice management guidance.

Desktops, Laptops & Mobile Devices

All devices used in your firm for business purposes should be fully equipped with the latest antivirus software. Both Windows and MacOS come outfitted with robust antivirus, antimalware, and antispyware services. They both have built in firewalls as well. You should prioritize keeping security software updated every day. Both Windows and MacOS will do this automatically by default.

Be sure you and everyone in your firm are following the best password protocols to protect your data from breaches.

A strong password includes between 8 and 20 total characters, at least one special character, and a combination of numbers and both uppercase and lowercase letters.

If you need assistance setting up a thorough security protocol for your devices, you may want to consult with a third-party IT professional to ensure that all of your software and equipment is protected and up to date.

Secure Client Communications Through Portals

Rather than utilizing email, text, and phone calls, consider implementing a cloud-based client portal to improve security and user experience. This will provide your firm with the tools you need to safely collect and store client data no matter where you are.

Some additional benefits of setting up secure client communications through portals include the following points.

Enhanced Security

Since attorney-client relationships include substantial amounts of information sharing, it is crucial that all of the information within these communications - including bank statements, legal documents, and contracts - be protected from unauthorized access. Client portals provide enhanced security by eliminating the threat of unsecured

emails and access to sensitive information.

Improved Response Time

When clients have 24/7 access to the portal, you will see an improved response time since clients will be able to interact with your firm outside of business hours if necessary. They will have access to documents, project plans, and even calendar items when they need them. Clients can access information to help with common questions that may reduce the need for additional emails or phone calls. These features help to ensure a more seamless process for both parties.

Seamless Payment Transactions

Client portals provide a secure space for both you and your clients to view bills and send or receive payments.

Consider Insurance Coverage

Sometimes, despite your best-efforts cybersecurity breaches can still happen. In addition to taking action to reduce your risk of an attack, it is a good idea to consider fraud insurance coverage. Coverage for fraud is generally not included in many insurance policies or endorsements, including:

- General liability
- Professional liability
- Fidelity
- Privacy breach
- Cyber practices
- Employment practices

While there is a chance that you may be partially covered, the chances are slim that you are fully protected from the entire scope of cyberattacks and other fraudulent activities. It is best to speak with a well-informed, professional insurance agent to discuss all the policies that are available to guarantee your protection.

To find out more about digital banking or how technology can make managing your law practice easier and more efficient, visit the Nota by M&T website at www.trustnota.com.