



LAWPRO

magazine

MARCH 2024

THE CONFIDENCE CLIENT

Their stories are fake
the threat is real

How fraudsters are targeting lawyers

Contents

MARCH 2024

| ON-DEMAND CPD

| COULD IT HAPPEN TO YOU

| WELLNESS



Features

- 4 Survival tips to prevent fraud
- 8 Wire fraud
- 10 Phishing
- 12 5 questions to ask yourself about technology
- 18 Corporate ID fraud
- 20 Bad cheque scams
- 24 Title insurance matters
- 25 Real estate scams

Departments

- 3 On-demand CPD from LAWPRO
- 13 Could it happen to you?
One click and you are out thousands of \$\$\$
- 15 Wellness
How managing your schedule can help you stay well

In practice

- 22 Tech tip
Client portals improve information security and client service

LAWPRO
magazine

President & CEO: Dan Pinnington dan.pinnington@lawpro.ca
Editor: Naomi Dummett naomi.dummett@lawpro.ca
Design & Production: Freeman Communications studio@freemancomm.com

lawpro.ca
Tel: 416-598-5800 or 1-800-410-1013 Fax: 416-599-8341 or 1-800-286-7639



LAWPRO Magazine is published by Lawyers' Professional Indemnity Company (LAWPRO) to update practitioners about LAWPRO's activities and insurance programs, and to provide practical advice on ways lawyers can minimize their exposure to malpractice claims. The material presented does not establish, report, or create the standard of care for lawyers. The material is not a complete analysis of any of the topics covered, and readers should conduct their own appropriate legal research.

The comments in this publication are intended as a general description of the insurance and services available to qualified customers through LAWPRO. Your policy is the contract that specifically and fully describes your coverage and nothing stated here revises or amends the policy.

On-demand CPD from LAWPRO

LAWPRO adapted to the changing times and many of the presentations we did last year are available as on-demand CPD. They are free and you can claim the LAWPRO Risk Management Credit for watching any of our CPD presentations. Many also qualify for Law Society of Ontario professionalism hours.



▶ Client Management and Effective Client Relationships (2023)

Learn from leading advocates about a well-drafted retainer agreement, setting fee expectations, and what to do when the client does not pay; understanding how diversity and culture can impact communication with clients; and managing communication and relationship breakdowns when they occur.

▶ Building Resilience and Maintaining Mental Health in the Legal Profession (2023)

Watch our continuing conversation about managing mental health and building resilience. This session will provide practical advice from those on the frontlines of improving mental health for lawyers.

▶ Top Tips for Advocates (2023)

This program, full of practical advice and tips, is for advocates from all areas of practice. Learn from leading advocates and LAWPRO counsel about recent developments in areas such as limitation periods, ineffective assistance of counsel, and establishing the legal status of clients.

▶ Protecting your firm against fraud (2023)

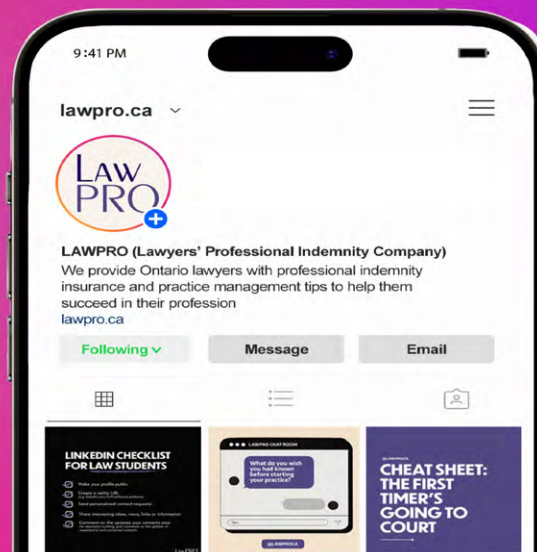
Fraud targeting lawyers continues to be a serious concern for the profession. This program provides up-to-date information on actual fraud attempts, the types of fraud claims LAWPRO counsel are seeing and how best to avoid these scams.

▶ Insurance 101 for lawyers: Tips for insuring your practice (2023)

This panel provides key information for sole practitioners and lawyers managing a practice on understanding and obtaining the different types of insurance available to protect their firm from risk. These experts explain the how-to of putting the insurance puzzle together—from Errors & Omissions coverage to Executor and Trustee coverage to Commercial General Liability.

Join us on Instagram

| @lawpro.ca



Publications Mail Agreement No. 40026252
Return undeliverable Canadian addresses to:
LAWPRO
250 Yonge Street
Suite 3101, P.O. Box 3
Toronto, ON M5B 2L7

LAWPRO* (Lawyers' Professional Indemnity Company)

Trademarks

* LAWPRO, TitlePLUS, practicePRO and their logos are registered trademarks and the Excess logo is a trademark of Lawyers' Professional Indemnity Company; other trademarks are the property of their respective owners.

Copyright

© 2024 Lawyers' Professional Indemnity Company, except certain portions which are copyright in favour of external authors.



THE CONFIDENCE CLIENT: SURVIVAL TIPS to prevent fraud

In the nineteenth century, American journalists and law enforcement coined the term “confidence artist” to describe a form of fraud that preys on the trust and credulity of its target. The form these frauds took was always changing but relied on the good faith of the target and either a promise of profit or a warning of impending losses to encourage co-operation.

Examples are legion: In the early 1920s, Charles Ponzi defrauded investors of millions of dollars by purporting to invest the money of trusting “marks” in a “postal reply coupon” arbitrage scheme that didn’t exist. In 1925, an Austrian con artist by the name of Victor Lustig fraudulently “sold” the Eiffel Tower to a Parisian scrap metal business—the following year, he attempted to do it again.

Modern examples are often less metallurgical, more technological. Online scams such as “Nigerian Prince” emails may be easy to spot, but sophisticated variations and alternatives can be surprisingly convincing to even the most careful victim.

Today in Ontario, lawyers are often targets of these frauds, sometimes taking the form of sophisticated variations on classic “confidence artist” techniques. Fraudster clients take advantage of their lawyer’s trust by involving them in a fraudulent mortgage scheme. Alternatively, the “confidence client” may provide their lawyer with a cheque pertaining to a supposed transaction, have the lawyer hold the funds in trust for a very short period, then, explaining that the deal has fallen apart in some way, ask for the funds to be returned—less legal fees. All of this will happen quickly before the lawyer realizes the client’s original cheque bounced, and the lawyer has now erroneously transferred money out of trust. Or fraudsters may target the confidence of a law firm’s staff member by using spoofed email addresses of a managing partner, requesting the employee’s assistance to immediately purchase and email “gift cards” to the fraudster for seemingly legitimate business purposes.

SURVIVAL TIPS

to prevent fraud

To help lawyers better understand these growing threats and how to avoid them, LAWPRO hosted a virtual CPD event along with the Toronto Lawyers Association focused on cyber and homeowner impersonation fraud targeting lawyers. Juda Strawczynski (JS), and LAWPRO's Vice-President Public Affairs, Ray Leclair (RL), were joined by Mouna Hanna (MH), Partner at Whitelaw Twining, to talk about recent fraud efforts targeting lawyers and provide "survival tips" to prevent successful frauds from occurring.

The following are edited highlights from that conversation.

What are the common forms of cyber fraud targeting lawyers?

MH: In the last year alone, LAWPRO has seen firm losses from fraud ranging anywhere from \$200,000 to \$4 million. In a typical claim involving wire fraud, what we see is a hacker who gains access to legitimate email conversations between a lawyer and their client, or between two lawyers discussing a transaction, and the fraudster will linger within the system and watch the conversations. Eventually they will insert themselves into the conversation and begin impersonating one or both sides of the conversation. They may use your email application's rules or settings to automatically filter legitimate responses from clients or opposing counsel into hidden folders, so the lawyer only sees spoofed emails or communications created by the fraudster themselves. Once the fraudster controls the conversation, they will reroute funds in a transaction to a bank account they control. This may be by altering documents within the computer system itself, or by emailing "new" wire instructions. Often these hackers will continue the façade even after a wire has occurred to give them enough time to get the money out of the receiving account.

Typically, someone within your firm will have received a fraudulent or phishing email, clicked a link or attachment, and inadvertently provided access to their computer. From

there, the hacker can obtain the employee's passwords and gain access to secure internal systems. If firms aren't using Two Factor Authentication (2FA), they not only leave themselves open to fraudsters impersonating their clients this way, but also the threat of ransomware. Ransomware and wire fraud is a big problem from a cost perspective and is not typically covered under a firm's professional insurance policy.

My top tip for firms is always to use 2FA, which is the process whereby you're authenticating your login to your computer or online account using two systems. One may be a password, and the other may be an application on your phone, so that only someone who both knows the password and has access to that specific phone will be able to log in.

The good news here is that banks have been on top of wire fraud recently. If you catch it early enough, the bank may be able to trace back the funds. But what we're finding is that banks are requiring you to issue an application or claim against the bank for a tracing order to retrieve the funds. So, it's still complicated and expensive, even if the fraud can be unwound. LAWPRO recently provided an article on "What to do if money is diverted to a fraudster's account."

JS: If a wire instruction comes in by email, calling the person on the other side, using contact information that is stored *outside* of the email chain itself because the fraudster may have altered that info, is key to avoiding these sorts of fraud attempts. We've recently seen some close calls where

lawyers receive a last-minute wire redirection, and because they've made note about our recent warnings about these sorts of frauds, they've contacted the bank, or the other side of the transaction, and discovered that the wire redirection was fraudulent. These close calls can save a lawyer hundreds of thousands of dollars that they could be on the hook for if the money leaves their trust account.

What is happening with homeowner impersonation fraud in the real estate market?

JS: Many people in the real estate realm are seeing significant increases in property owner impersonation fraud. Private mortgage fraud especially seems to be the "flavour of the day." This is a situation where fraudsters are securing private mortgages against properties that they don't own, or even selling the property to unsuspecting buyers, by pretending to be the owner. Once the proceeds of the mortgage or sale get directed to them, they disappear with the funds. It's a complex and costly matter trying to undo these transactions.

RL: With institutional mortgages, there are often a number of safeguards and procedures in place to prevent fraud. Private mortgage lenders are a common target because fraudsters are always looking for the low-hanging fruit. While many private mortgage lenders have sophisticated systems in place to screen files for red flags, many others don't. Some lenders jump at the opportunity to lend money and make a supposed great return and are then susceptible to this type of fraud where you have someone purporting to be the owner but is running a complex impersonation scheme.

How do they convince people they own these properties? They use Google or the Multiple Listing System (MLS) to obtain pictures of the property. They often target Airbnb properties so that they can rent the property and take personal photos inside, or bring an appraiser, banker, or lawyer to the property to assuage any ownership concerns.

Some years back, the police arrested an individual with 13 cell phones on him. On the back of each cell phone was the name of a "character" so he could pretend to be the mortgage broker, the banker, the borrower, and so on, depending on which phone rang. It can be quite sophisticated.

JS: LAWPRO is also seeing situations where the homeowner impersonation has been used on a sale. Usually in these cases, the true owner of the targeted property is not living in the residence at the time. These may be snowbirds or people who split their time between different locations. By the time the lawyer is involved, the fraudster may already have a sale in progress, and the lawyer is merely asked to paper what appears to be a legitimate transaction.

What red flags are of concern for homeowner impersonation frauds?

RL: If you get a large number of referrals from a new source, such as a broker or agent, it can be tempting to jump into a supply of new business. But a series of similar transactions over a small timeframe can be a sign of danger.

Rushed transactions should be of concern. They may be legitimate, but you need to know the reason for the rush. You should be asking your client to explain why they are proceeding with the transaction and why they are insisting on a short timeframe. If the client doesn't want title insurance, it may be because they don't want the scrutiny that comes with a title insurance policy. If their photo identification doesn't look quite right, you need to dig deeper. In any situation where the client is dictating to you how you do your legal work, you should be asking questions.

JS: Which brings us to our next tip: Know your client. Ask your client lots of questions. If you're acting for a purported vendor, a good question is "Why are you coming to me? Why are you not using the lawyer you used when

you bought the property? What changed?” But don’t stop there, ask them how they found you, why they chose you. Recently we’ve been seeing things that should give lawyers pause. For example, if the client claims to own a property in downtown Toronto, but they retain a lawyer in Barrie, that needs explanation. We sometimes see people retaining counsel where there is no rational connection between the property’s location and the lawyer. The client may have an answer for that, perhaps they spoke to a former client, or they liked your website online, but there needs to be some sort of explanation and lawyers shouldn’t be afraid to press their clients for it.

You should also inquire with the client as to why they are selling the property at this time. How did they determine the price? How does the price compare to neighbouring properties on MLS? A client should be able to happily and trustingly tell their lawyer why they came there, what their intention is, and the history of the transaction.

How should lawyers confirm their clients’ identities?

JS: Sometimes real ID is being used for fraud. We’ve seen cases where the actual homeowner has lost their ID or it’s been stolen, and that makes its way to fraudsters who pose as clients. More often, though, it’s fake IDs that are being used.

For starters, you can always check a driver’s licence on the Ministry of Transportation’s website. You can enter the licence number online to see if it matches what is on the licence itself. Sometimes fraudsters use a legitimate licence number but swap out the phone number or the name. We’ve seen cases where a fraudster uses the same photo on multiple pieces of identification. That is an obvious red flag because each piece of ID should have a different photo—probably taken at different times or even in different years.

RL: You need to take the time to look at the ID. Photocopying it and putting it in a file is not good enough. You need to take the time to compare images on different IDs, compare the information on the ID with other available sources. Think about the information on the ID: Does the provided date of birth make sense? Meet with the client in-person, if possible, to confirm their appearance.

MH: We often use the words “identify” and “authenticate” interchangeably, but they are different. You can identify yourself with a statement such as “I am Mona Hanna.” Authentication takes it further and involves verification of the claim of identity.

There are also a number of third-party platforms that can be used to independently verify client IDs. Examples include Verified.Me, Vaultie, Treefort, or TransUnion. Generally, you can expect these programs to provide you with a digital process to identify and authenticate a client before you meet with them.

RL: One other thing to note: Unfortunately, individuals are not the only ones having their identity stolen. Corporations continue to have their ID stolen under the new Interior Business Registry. We still see situations where fraudsters file false documentation with the registry changing the directors and officers of a corporation as well as the location of corporate headquarters. They can then falsely act on behalf of the corporation to buy or sell property, as they are now the officer or director of record.

To watch the full CPD discussion which is eligible for 1.5 hours of LSO professionalism and LAWPRO’s Risk Management Credit visit the practicepro.ca/CPD. ■

At the time of the writing of this article Juda Strawczynski was the Director, practice-PRO at LAWPRO. He is currently the CEO and Registrar, CPATA (College of Patent Agents & Trademark Agents)



Virtual Identity Verification (IDV) Service Provider Chart

As of January 1st, 2024, the Law Society of Ontario requires lawyers who only meet with clients virtually to verify their clients’ identity online by authenticating their identification documents, or using an alternate, approved verification method.

The virtual authentication of identity is done via technology that does multiple searches/verifications of the client’s identity. The Law Society of Ontario refers lawyers to a directory maintained

by the Digital Identification and Authentication Council of Canada (DIACC).

LAWPRO invited companies listed on the DIACC directory, along with other known vendors, to provide information about the service they provide including costs, onboarding time, turnaround time, process, and privacy. The vendors completed a survey and provided self-asserted information. You will find the responses received in the Identity Verification (IDV) service Provider Chart.



VIRTUAL IDENTITY VERIFICATION (IDV) SERVICE PROVIDER CHART

from practicepro.ca/idvvendors

WIRE FRAUD

Fraudsters are actively trying to direct lawyers and law firms to wire money to them – often through spoofed emails of people you know or hacking into emails.

Fraudsters have pretended to be:

- A lawyer in the firm directing staff to wire funds to a client or to complete a transaction
- A lawyer or staff acting for a seller in a transaction directing the other side to wire funds
- A financial institution directing wire payment to itself
- A client seeking payment of funds by wire



FRAUD WATCH



It starts with a hacked email system or impersonation using a lookalike fake email address. In the hacked email situation, the fraudster hacks into a lawyer or law firm email system, the client's email, or the email of others related to the transaction (or those copied in the email thread) and monitors the emails. The fraudster then sends wire transfer instructions from legitimate email addresses directing the wiring of funds to a particular account that the fraudster has set up or can access. When using a lookalike fake email address, the fraudster sends instructions that appear to be legitimate. In some cases, corporate records may be altered to add credibility to the scheme.

In recent cases reported to LAWPRO, a fraudster infiltrated a law firm email system, intercepted correspondence regarding a transaction, and then sent wiring instructions from a law clerk's email address. Since the wire instructions were being sent from a legitimate law firm email address, there was nothing to suggest anything suspicious from the email itself. Given that the fraudster could see incoming emails, only a separate means of verifying the instructions could stop the fraud.

TIPS

Verify instructions independently: Anytime you receive instructions to wire money to a bank account, contact the payee directly by an independent method (not replying to the email sending the instructions) to verify the instructions received and the accuracy of the bank routing information.

Double check email addresses to see if they are fake: Fraudsters will spoof an email address by creating a very similar looking address by adding an extra letter/number or changing a character(s). Having hacked into one account, they may spoof other email addresses that were in the email thread to increase your confidence that it is a proper message. It is important to carefully look at all the email addresses in the message. And remember, if the client's email account is compromised, it could be the fraudster sending you emails that look like they are coming from your client.

Implement two-factor authentication on your email systems: Two-factor authentication is an extra layer of security to make sure that people trying to gain access to your email are who they say they are. First, a user will enter their username and password. Then, instead of immediately gaining access, they will be required to provide another piece of information such as a code. Outlook and Gmail both offer two-factor authentication.

Regular training: Train staff in what to look out for and have regular discussions to reinforce the cyber security message. Someone from the office may see information or indications of fraud that others may not.

Educate your clients: Advise your clients of wire transfer risks. If you do not accept wire payments from them, tell them so that if they are approached to send funds by wire, they know it will be a fraud. If you do accept wire payments, explain your process and insist that they call you before they send you payments.

Examples of independent verification in action

Internal verification: The law firm partner purportedly emails from the firm address or a personal email address instructing you to wire money out of trust. Walk down the hall to the partner's office to ask if the partner sent the instructions. If the partner is out of the office, rather than replying to the email to confirm the direction (which will not help if the lawyer's email account has been compromised), call or text the lawyer.

Before wiring funds to another firm: If a lawyer at one firm emails wire instructions to a lawyer at another firm, that lawyer should call them to confirm the wire instructions. The same process can apply on receiving wire instructions from a financial institution or any other request for payment by wire transfer.

Before wiring funds to a client: A client may email you to instruct you to wire payments to an account. You can call the client to verify that the client's instructions are valid and that the client's account has not been hacked.

Firms that have implemented independent verification protocols have successfully blocked fraud attempts. A quick call to verify written wire payments might save you from being a victim of fraud.

PHISHING

Personal information and identity theft and/or payment scams are the motives behind most phishing scams. Phishing is an email, text message or phone call that appears to come from a trusted source, institution, vendor or company, but is actually from a third-party impostor. Phishing emails, texts or phone messages are intended to trick you into giving fraudsters your information by asking you to update or confirm personal or online account information.



FRAUD WATCH



A “spear” phishing attempt is a phishing message that is personally addressed to you, will appear to be from someone you already know (such as a senior partner at the same firm), and may include other detailed personalized information.

Fraudsters do their best to make phishing messages look official and legitimate. They will mimic real communications from the company or entity they are supposedly from by using the same layout, fonts, wording, message footers and copyright notices. They will often include corporate logos and even one or more links to the alleged sender’s real website.

Many phishing messages will include a link or attachment that you are asked to click so you can update your information. After doing so, the webpage or attachment you will see (which will also have text and logos to make it look official) will prompt you to enter your name, account number, password and other personal information – thereby giving it to fraudsters.

SIGNS

- The link you are asked to visit is different from the company’s usual website URL (place your mouse over the link and look at the taskbar in your window to see if the link matches. It should take you to the proper website)
- The main part of the sender’s email address is not the same as the company’s usual email address
- Spelling and grammar mistakes
- A sense of urgency – money has to be transferred quickly without the usual checks and balances
- The caller purports to be from the fraud prevention department of your bank, credit card company or other institution and needs you to provide them with key personal information over the phone
- Anyone asking for money – even if you know them
- The promise of receiving money or another big prize

Examples of phishing

- An irregular salutation from someone you are familiar with, such as “Hello Mr. Smith,” instead of “Hi Johnny.”
- An alert to reset your password or login to your account to review invoice or payment.
- “...your account has been hacked”: A request to update your information and go to a website or attachment, then prompting you to enter your account number, password and personal information.

- “...won a big prize,” “...refund to you”: A request to go to a website or open an attachment to claim monies.
- “...document I promised”: Posing as someone you know who may send you documents, a request to open an attachment.
- A call from a fraudster claiming to be from a legitimate corporate or government entity saying that you owe money or face civil/criminal charges.
- Requesting payment in Bitcoin, other cryptocurrencies or with gift cards.

TIPS

Never respond to requests for personal information in the mail, over the phone or online – just delete them. Never reply to unsolicited or suspicious emails, instant messages or web pages asking for your personal information (e.g., usernames, passwords, SIN number, bank account numbers, PINs, credit card numbers, mother’s birth name or birthday), even if they appear to be from a known or trusted person or business since this is probably the most common way that personal information is stolen.

Legitimate businesses should never send you an email asking to send your username, password or other information to them in an email message. If in doubt, call the company yourself using a phone number from a trusted source. Don’t use the number in the email – it could be fake too!

Share this information with 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.

Source: *Author's calculations based on data from the 2007 Survey of Consumer Expenditures, Bureau of Economic Analysis, U.S. Department of Commerce.*

-

lawpro.ca

One click

and you are out thousands of \$\$\$

Could it happen to you? If you have a trust account, then you're at risk.

We are seeing a sharp increase in social engineering fraud against law firms and their clients, where the goal is to divert funds to fraudsters' accounts. When money gets diverted, the lawyer and/or the client is out of funds. For the lawyer and staff involved, an errant funds transfer is one of the most stressful situations to be in.

Picture this situation: Your firm acts for a couple selling their home and buying a new one. They need to discharge the mortgage on their first house to complete the same. You log into your account and see an email from the current mortgage company with payment instructions, including the wire transfer account number.

Several days later, the mortgage company sends you a further email, asking that you send the funds to a different wire account. The email appears to be from your regular contact at the company. The mortgage company apologizes for the earlier email and advises that the funds transfer direction was sent in error. The email provides new wire transfer instructions.

What do you do? Do you wire the payment to the first account, the second account or not at all? Unfortunately, sometimes, we have seen lawyers send the funds without taking further steps to independently verify the instructions. Hundreds of thousands of dollars have gone missing; sometimes several million dollars diverted.

Preventing loss from social engineering fraud

Claims related to or arising out of social engineering are covered to a sublimit of \$250,000. However, lawyers can extend this "social engineering coverage" to the standard \$1 million limit by taking the following steps:

What should I do to avoid social engineering claims and prevent the associated sublimit?

1. Include written instructions in a retainer or other agreement for the receipt, release, and transfer of any funds or assets.
2. Advise in the written retainer or other agreement that the client or another party to which you owe a duty of care should not ordinarily expect to receive any revised instructions from you or your firm for the transfer of funds or assets.
3. Advise in the written retainer or agreement that, should the client or another party to which you owe a duty of care receive revised instructions for the transfer of funds or assets, they should immediately contact you by way of a telephone number specified in the written retainer or other agreement.
4. If you or your staff receive any changes to the contact information of a client or other party to which you owe a duty of care, or any changes to established instructions for the transfer of funds or assets, you confirm those changes by either calling the client or other party to which you owe a duty of care using contact information previously confirmed to be that of the client or other party, or by meeting with the client or other party.
5. Maintain in writing any updated contact information for a client or other party to which you owe a duty of care, and any updated instructions for the transfer of funds or assets.

For a full description of your obligations under the policy, please see Exclusion (k) of Part III, which applies to losses arising out of or connected to Social Engineering. Nothing in this summary should be taken as limiting or altering that exclusion.

To learn more about social engineering fraud and steps to take to protect yourself and your client see: Social Engineering Toolkit www.practicepro.ca/socialengineering ■

On the next page, you will find example retainer language.

Social Engineering Fraud EXAMPLE RETAINER LANGUAGE

Fraud Prevention

To prevent fraud and ensure the safe and accurate receipt, release, and transfer of any funds or assets, the following steps will always be taken to safeguard such assets:

1. We will only accept funds [or assets] from you [or additional party] by way of:
 - ☐ Electronic funds transfer to our trust account numbered _____
 - ☐ Wire transfer to our trust account numbered _____
 - ☐ Certified cheque delivered to us at _____
 - ☐ Additional method of funds or asset transfer _____
2. We will only transfer funds [or assets] to you [or additional party] by way of:
 - ☐ Electronic funds transfer to your account numbered _____
 - ☐ Wire transfer to your account numbered _____
 - ☐ Certified cheque delivered to you at _____
 - ☐ Additional method of funds or asset transfer _____
3. We will only release funds or assets to a third party upon receiving verbal confirmation of the transfer from you and any other party necessary to confirm the veracity of the transfer details.
4. You [or another party] should not expect to receive any revised instructions for the transfer of funds or assets from us. If you [or another party] receive any written communication advising of such a change that appears to come from us, immediately contact us at [insert telephone number] to verbally confirm these changes.
5. If we receive any changes to your [or another party's] contact information, or any changes to the instructions for the transfer of funds or assets as set out above, we will not act on these changes until we have verbally confirmed the new instructions in-person or by calling you [or another party] at the following phone number: [insert phone number]

Find this form and other social engineering fraud prevention
information at practicepro.ca/socialengineering

©2023 Lawyers' Professional Indemnity Company. LAWPRO is a registered trademark of Lawyers' Professional Indemnity Company. All rights reserved. The material presented does not establish, report, or create the standard of care for lawyers. The material is not a complete analysis of any of the topics covered, and readers should conduct their own appropriate legal research. The comments in this publication are intended as a general description of the insurance and services available to qualified customers through LAWPRO. Your policy is the contract that specifically and fully describes your coverage and nothing stated here revises or amends the policy.

December 2023

How managing your schedule can help you stay well



Decision fatigue is the decline in energy and focus you experience after making decisions or engaging in mundane tasks. This mental drain can cause you to seek immediate rewards, which can lead to poor decision making and inefficient or irrational behavior.

z z

Here are five ways you can manage your daily schedule to stay focused and positive throughout the day.



1

Tackle draining tasks earlier in the day

We all have tasks we dread on our to-do list. Maybe it's mind-numbing administrative work, or some unpleasant emails we've been putting off. When our ego-strength and glucose levels start to run low, these tasks can become extremely frustrating and exhausting. Scheduling some of these tasks for earlier in the day can increase productivity, decrease frustration, and ensure unpleasant tasks aren't weighing on our mind.

2

Eat healthy meals or snacks to replenish glucose throughout the day

Caffeine, adrenaline, or exercise may keep our physical energy up throughout the day, but they can still leave our willpower and mental energy depleted, leading to procrastination and a lack of focus. The brain, like the rest of the body, derives its energy from glucose, the simple sugars your body extracts from most food.

Eating fruits and healthy cereals (those without hidden, added or processed sugars) for breakfast, lunch, or a midday snack can help replenish glucose levels while avoiding "sugar crashes" and other negative consequences from refined sweets.

3

Eliminate unnecessary decisions from your daily activities

We may not notice it through the day, but each small, inconsequential decision we make can drain us of our ability to make large, important decisions. Things as simple as what to eat for breakfast, or what to wear in the morning, can limit our ability to exert self-control or focus on important matters at work. Removing these decision-points from our daily schedule can often lead us to work more effectively and efficiently.

If you crave variety and don't relish the idea of eating or wearing the same thing every day, make weekly wardrobe and meal choices on a Sunday evening, and then put them out of your mind.

4

Take breaks between willpower-draining tasks

Being cognizant of the type of work we're doing can help us more effectively schedule our tasks. Creative work, such as brainstorming potential legal strategies, or drafting legal memos or arguments, uses different mental faculties than administrative or repetitive tasks. When we reach our limit on mundane tasks, we can help recover by turning to more creative endeavors.

Spacing out challenging tasks throughout the day can help us maintain energy. Similarly, taking a short walk and stepping away from the desk can help rejuvenate our ability to focus on the task at hand.

5


Identify and distinguish "routine" activities from "creative" ones

While this article has focused on the downsides of "routine" work, there are ways to take advantage of these tasks as distinct from a lawyer's more "creative" responsibilities.

For example, it is often easier to achieve "flow," when engaging in routine or mundane tasks. "Flow" is a mental state where you are fully immersed in a feeling of energized focus and enjoyment of the current activity. "Flow" is more likely to occur when there are clear goals (such as a series of known tasks to be completed) and where you can receive immediate feedback and assess progress. In some legal matters, it's possible to convert "creative" tasks (where flow is difficult because the goals and progress are vague) with "routine" tasks by using checklists. PracticePRO provides an online repository of checklists that can assist practitioners in more efficiently working through files.

Additionally, time-management approaches such as the "pomodoro" technique (where you do constant work for 25 minutes and then take a 5-minute break) are designed to help focus on menial and non-creative tasks. They are less effective at increasing productivity when the tasks are highly creative or ill-defined. The use of checklists, however, can convert a "creative" task, into a "routine" one that is more appropriate for these techniques.

Being aware of the ways creative versus routine tasks can slow us down or limit our productivity can allow us to schedule our days in efficient ways that take advantage of the ways our minds work and when we are best able to tackle certain tasks. Avoiding procrastination and burnout can help keep both our minds and our bodies healthy. ■

A top-down photograph of a white ceramic coffee cup filled with dark coffee. A large, irregular brown spill of coffee has spread across a white document with black text, which appears to be a legal or financial form. The spill is most prominent around the cup and extends towards the bottom right. In the top right corner, a small green succulent in a dark pot is visible. A yellow pen with silver accents lies horizontally at the bottom right of the frame. The background is a solid dark blue.

Spilled coffee
is your biggest
worry when your
firm has Excess
insurance to handle
the rest.

Everyone makes mistakes, don't let a lack of excess insurance be yours.

LAWPRO Excess insurance is optional coverage of up to \$9 million for firms that may need higher limits than the primary Law Society insurance program provides.

In certain circumstances, you could be at risk of exceeding the primary program's \$1 million professional indemnity limit and even threatening your firm's existence. Consider the following to determine if you should consider excess coverage:

- Real estate practice: Average home prices in Toronto are now in the \$1 million range
- Wills and Estates practice: Demographics show that the biggest wealth transfer in history is here
- Corporate Commercial practice: Land values drive up costs in every area of the economy

The LAWPRO Excess program is designed to protect small and medium firms and gives you the comfort you need to handle large trust accounts, a real estate or wills practice, or tax law with ease.

Grow your firm and keep your peace of mind.

To find out if your firm is eligible for Excess coverage, call LAWPRO at 416-598-5899 or 1-800-410-1013.

LAWPRO
excess[™]
Insurance

CORPORATE ID FRAUD

Changing or stealing the identity of corporate property owners is commonly accomplished by filing a notice naming imposter directors and officers, using fake ID for the real directors and officers or changing the address of the registered office. The fraudsters then retain a lawyer to help sell or mortgage the corporation's property.



FRAUD WATCH



SIGNS

- Notice of Change is filed after a long period without a change in control of the corporation – even where real owners or their agents regularly make corporate filings
- Corporation has owned vacant land, disused or run-down property for a long time, without activity on title or visible use of land
- Property may be in highly marketable or developing areas but subject to restrictive zoning, is environmentally sensitive, or lacking road access
- Real directors/officers/shareholders are elderly, remote or otherwise vulnerable
- Current officers and directors were appointed very recently (see “Date Began” in Corporate Profile Report). This may not be a concern by itself, but merits a query about the circumstances of the recent changes and any notes taken (especially if there are other red flags)
- Corporation’s head office changed to non-existent or problematic address (such as a hotel – Street View on Google Maps may help determine this)
- Corporate resolutions or minute book with obvious errors or typos, or simply not available
- One lawyer retained to discharge an existing mortgage or file a Change Notice, but a different lawyer retained for borrower in the new mortgage transaction, or for corporation as vendor in a sale
- Mortgage statement for discharge purposes shows much less than registered amount of mortgage

- Small encumbrance, such as a construction lien, recently registered and discharged from title (to give credibility to the fraudster’s claim to be legitimate owner of the corporation)
- Client is new to you and documents show a different lawyer has acted for a corporation for years
- Clients say that title insurance for new mortgage is not required
- Client pushes for fast closing

TIPS

Check the Document Last Filed in the Corporate Profile Report. It will likely be an Annual Return, but could be a Form 1 – a possible red flag. A Corporate Document List search will disclose a history of the documents filed for the corporation. Ask for details of the change in control of the corporation, or permission to contact the corporation’s previous lawyer, agent, directors or officers.

Share this information with clerks and other law firm staff as they may be involved in parts of the transaction that you may not see.

BAD CHEQUE SCAMS

Fraudsters retain the firm on a contrived legal matter so they can run a counterfeit cheque or bank draft through the firm trust account and walk away with real money. The fraudster will provide real looking ID and documents. When the bad cheque or draft bounces, there will be a shortfall in the trust account.



FRAUD WATCH



SIGNS

- Initial contact email is generically addressed (e.g., “Dear attorney”) and/or BCC’d to many people
- Client uses one or more email addresses from a free email service (e.g., Gmail, Yahoo!), even when the matter is on behalf of a business entity
- Domain name used in email address or website was recently registered (check at Whois.com or a similar service provider)
- Email header indicates sender is not where they claim to be
- Client is new to the firm
- Client says they prefer email communication due to time zone differences
- Client may sign retainer but never actually makes the payment
- Client is in a rush and pressures you to “do the deal” quickly, before the cheque clears
- Client is willing to pay higher-than-usual fees on a contingent basis from (bogus) funds you are to receive.
- Despite the client stating a lawyer is needed to help push for payment, the debtor pays without any hassle.
- Cheque is drawn from the account of an entity that appears to be unrelated (e.g., a spousal arrears payment from a business entity)
- Payment amounts are different than expected or change without explanation
- Client instructs you to quickly wire the funds to another bank account based on changed or urgent circumstances

TIPS

Cross-check and verify information provided to you by the client:

- Google names, addresses, and phone numbers of the client and other people/entities involved in the matter.
- Look up addresses using Street View in Google Maps.
- Search AvoidAClaim.com’s database of bad cheque fraud names.
- Ask your bank or the issuing bank to confirm the branch transit number and cheque are legitimate.
- Call the entity making the payment or loan and ask if they are aware of the transaction.
- Hold the funds until all banks confirm funds are clear and can be withdrawn.

Client portals

improve information security
and client service

What is a client portal?

Wikipedia defines the term client portal as “an electronic gateway to a collection of digital files, services, and information, accessible over the Internet through a web browser. The term is most often applied to a sharing mechanism between an organization and its clients.”

Why is it important for lawyers to provide client portals? The legal process generates documents containing sensitive information, and those documents should be shared frequently with clients. The delay of postal delivery is generally not adequate for today's expectations. Email has become the default digital business communication tool. But email is not secure. It travels across the internet as plain text and is relatively easy for a knowledgeable transgressor to intercept. Encrypting email provides security but it is still email, which can be caught by spam filters or lost in an inbox.

While there are business tools appropriate to securely store and share documents, programs designed with lawyers in mind require less customization and are generally the best choice. This is especially true for solo and small firm lawyers without a dedicated in-house IT department. My view is that paying for a practice management software subscription is one of the best investments one can make regarding client file management. That cloud-based practice management tools also provide secure client portals just makes them an even better bargain.

Portals provide superior client service

Many of today's clients have experience with secure portals. Banks, phone and internet providers, hospitals, physicians, physiotherapists and other health care providers have turned to client portals to engage with clients and patients. Clients are increasingly comfortable with and expect secure portals when working with professionals.

The organization of client documents and information within a portal can be a valuable client service, especially when a client needs to review matters while traveling or for consumer clients who are not used to retaining and organizing important paperwork. Portals help clients see their documents and the status of their matter in a way that can help build client confidence and trust.

Portals Can Enhance Security And Reduce Risks

Client portals are simply the best and most secure method to share documents in many cases. While most information related to a client should be treated as confidential, we must also appreciate that bad actors seek personally identifiable information such as financial account numbers, credit card numbers, birth dates associated with the names and the like. So, you cannot assume you won't be a target.

It is simply unworkable to make individual determinations about which documents are too sensitive to email and which can be emailed on a case-by-case basis. It is far better to build a secure system for sharing digital information and then use it for all client communications and document sharing (except the few that have requested traditional mailing). Client portals are that system. Portals also provide confirmation that a client has received and reviewed a particular document. Email can still be used for non-sensitive matters such as scheduling.

Portal options:

Practice management software and standalone services

Most smaller law firms without full-time IT staff should consider cloud-based practice management software solutions that include client portals. These online practice management solutions can provide both the organizational structure for law firms to manage their client file documents and portals for the firm to securely share information with clients. Your client portal should make it easy for clients to upload documents to you securely. For a list of practice management providers, see LAWPRO's Technology Products for Lawyers and Law Firms resource.

Standalone file sharing services can similarly provide many client portal functions. Some examples include Microsoft 365, Dropbox Business, Sharefile and Google Drive. There are many others. Generally, these file sharing services enable the client to securely upload documents to the lawyer, including larger files.

In either case, when considering a portal, lawyers and firms should make sure that the portal meets key security requirements. You and your clients should be maintaining strong passwords, and two-step verification can help secure the portal. Another consideration is where the data is stored. Some portals store all Canadian client documents on Canadian Data centers. This should be confirmed with the provider.

The future of portals

Ambitious law firms may develop different types of client portals. If you represent clients in a particular industry, it might be full of news and information related to that industry. A law firm catering to individual consumer clients may build a portal with a wealth of basic information that may lead to other engagements.

Closing the portal

If the client portal is used for only sharing documents related to a matter, then the portal should be closed at approximately the same time that the client file is closed. You do not do clients any favors by leaving a portal open for many months after a client's matter has been concluded. The idea is not to exclude the clients from their information. Rather, it is to assist them in saving their information before the portal is closed.

Conclusion

Sharing of digital documents will increase and lawyers have an obligation to securely handle that information. Most law firms will use portals because it is the simplest and most efficient way to share a series of documents as the representation progresses. Thinking of the firm portal as your online entrance for clients may lead to many creative ideas. ■

Jim Calloway is Director of the Oklahoma Bar Association's Management Assistance Program

A decorative background featuring several 3D-rendered spheres in red, purple, blue, yellow, and light blue, along with a bright green 3D cube. They are arranged on a light pink surface, casting soft shadows.

Title insurance matters: One of these things is not like the other

You may recall the title as a lyric from a song in a popular kids show many years ago, reinforcing the benefits of being aware and noticing differences.

This same lesson applies when comparing the legal protection coverages offered by other title insurers that compete with the Legal Service Coverage that's included in TitlePLUS policies. The differences are not always obvious and often discovered after a claim, where coverage is not what was expected.

Unfortunately, the lawyer could then be facing a lawsuit from their client, professional reputation damage, and a paid claim under their errors and omissions coverage that may trigger payment of a deductible and claims levy surcharges, often resulting in additional costs of \$17,000 or more over the next five years.

Real Estate remains one of the highest in claims by area of practice, with LAWPRO reporting that 27% of new claims in 2021 were real estate related. As such, it is important to protect yourself and your clients by understanding the differences in the various legal protection coverages offered by title insurers.

Did you know that many legal service endorsements are subject to the same exclusions, limitations, and exceptions contained in the title insurance policy? Be aware, as circumstances may arise where the lawyer is exposed to liability and could be sued.

Scenario- A lawyer closes a purchase of vacant land but misses adding one of the PIN's on a transfer due to an administrative error. When their client attempts to later sell the property, the missing PIN is discovered to be in the prior owner's name. The client submits a claim under the title insurance policy. However, since coverage is limited to the land as legally described in Schedule A, the claim is denied. Further, although the policy included a legal protection endorsement, it is subject to the same exclusions, conditions, and exceptions of the title insurance policy and unfortunately, there is no coverage.

This claim scenario would have been covered if the lawyer had the Legal Services Coverage included in a TitlePLUS policy, as the policy explicitly states there is coverage if the lawyer:

“Commits an error or omission in providing legal services for the Transaction for which liability is imposed by law.”

Other common policies offered by other insurers are those that cover smaller error and omissions claims but have monetary claim payout limits. Limits on the amount of the claim are always a cause for concern, particularly because the average cost of a real estate claim is \$34,000. A TitlePLUS policy has no limitations on payouts other than the policy amount, and the industry standard inflation protection limit on the original policy amount.

Lastly, some legal service options require you to purchase the coverage each time you order a policy. This additional step can be easily missed, especially in a time of competing priorities and busy days. With a TitlePLUS policy, there are no extra steps. Legal Services Coverage is automatically included in most policies - no missed coverage, no extra input, and no extra charge.

TitlePLUS Legal Services Coverage stands on its own and is the coverage many legal professionals rely upon and trust. Visit titleplus.ca to learn more about the many new changes at TitlePLUS including TitlePLUS Legal Counsel Fees.

To learn about the many scenarios where TitlePLUS Legal Services Coverage would respond, watch this video <https://www.youtube.com/watch?v=nOAzv5U044U> ■

Lisa Burdan is Sales Manager, TitlePLUS at LAWPRO

REAL ESTATE SCAMS

Real estate frauds often occur in situations where the true owner's identity is stolen (ID theft) for sale or mortgage purposes, or the value of a property is exaggerated (flips).

Identity theft

When a client uses fake ID to assume the identity of existing property owners or uses a Notice of Change to become a director or officer or corporate owner for the purpose of committing fraud, this is identity theft. Once identity has been stolen, the fraudster sells or mortgages the property, or discharges a mortgage from title, then gets a new mortgage from another lender.



FRAUD WATCH



SIGNS that your client may be a fraudster

- Client is in a hurry and may discourage house inspection or appraisal
- New client for you and/or new referral source if any, or no referral source
- Funds directed to parties with no apparent connection to borrower, property or transaction
- Client changes instructions regarding amounts or payees just before closing, or fails to bring in funds as promised
- Client does not care about property, price, mortgage interest rate, legal and/or brokerage fees
- Client does not appear familiar with property
- Client won't permit contact with prior lawyer or have a valid explanation why they are not using them
- Other party appears to control the client
- Client advises funds were paid privately. No funds pass through a lawyer's trust account
- One spouse or business partner mortgaging equity in property owned by both
- Client contact is only by email or text
- Client says title insurance for new mortgage is not required
- Client pushes for fast closing

SIGNS that the transaction is fraudulent

- Repeat, recent transfers, mortgages, or discharges on a single property or for a single client (Always request a PIN printout with full history of deleted instruments)
- New referral source sending lots of business
- Use of Power of Attorney and/or funds directed to the Attorney instead of borrower
- Power of Attorney is not executed correctly
- Rental, Airbnb, and vacant properties are especially vulnerable
- Property listing expired without sale (i.e., sale may be unregistered)
- Property has been mortgage free, or subject only to an institutional first mortgage, but owner now registering a large mortgage in favour of private lender
- Property area and/or client residence is distant from your office

- Deposit not held by agent or lawyer
- Deposit is higher than normal and is paid directly to the vendor
- May target long time owners or deceased, ill, or elderly who may be less alert to signs their identity is being stolen
- Rush deals, sometimes with promise of more
- Amendment to Agreement of Purchase and Sale reducing price, deposit, or adding creditors
- Sale is presented as a "private agreement" – no agent involved, or named agent has no knowledge of transaction
- Municipality or utility companies have no knowledge of client's ownership
- Client paying little or nothing from own funds
- Unusual adjustments in favour of vendor, or large vendor take-back mortgage
- Use of counter cheques

TIPS to help verify ID

- Is the person smiling in their ID photo? Smiling isn't allowed in government ID.
- Compare the images on the different pieces of ID – they shouldn't be the exact same image.
- Verify the date on the IDs. Does the person look like they've aged if the ID was from some time ago? If two pieces of ID are many years apart but the image doesn't reflect whether the person has aged, ask questions.
- Does the minister on the ID match who was in office at the time the ID was issued?
- Is the signature similar to your client's?
- Is the client's name spelled differently in different types of documents/ID?
- Does the driver's license number follow the proper sequence?
 - starts with 1st letter of last name
 - ends with person's date of birth
 - women's month date (0 replaced with 5 and 1 by a 6)

TIP

Advise lenders of recent activity on title, amendments to purchase price and significant changes in value in advance of closing.



Risk management
practicepro.ca



Additional professional
liability insurance
lawpro.ca/excess



Title insurance
titleplus.ca



AvoidAClaim.com



LAWPRO



LAWPRO insurance
TitlePLUS Home Buying Guide – Canada



LAWPRO
TitlePLUS



LAWPRO