


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



! If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

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.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on “All Fraud Warnings” for a list of confirmed fraudsters.

© 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 the topics covered, and readers are encouraged to conduct their own appropriate legal research.

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



! If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

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.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on “All Fraud Warnings” for a list of confirmed fraudsters.

© 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 the topics covered, and readers are encouraged to conduct their own appropriate legal research.

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



If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

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.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on “All Fraud Warnings” for a list of confirmed fraudsters.

© 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 the topics covered, and readers are encouraged to conduct their own appropriate legal research.


INTERNAL OFFICE FRAUD

Is the fraudster in your office?

Not all fraudsters are strangers. Even partners, associates, law clerks or other employees can be fraudsters.



FRAUD WATCH

The background of the lower half of the page is a vibrant, futuristic graphic. It features a laptop with a glowing blue screen and keyboard. Overlaid on the laptop and extending into the background are various digital elements: a 3D bar chart with red and blue bars, a line graph with a green trend line, a circular radar chart with concentric rings, and a network diagram with nodes and connecting lines. The overall color palette is dominated by blues, purples, and reds, creating a high-tech, data-driven atmosphere.

If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

SIGNS

- Someone never takes vacation or sick leave, works overly long hours, or refuses to delegate work.
- A firm member undergoes a sudden change in lifestyle or temperament.
- The firm receives mail for a corporation for which no client file is opened or billed, or minute books are kept in the lawyer's office instead of with the corporate law clerk.
- Unusual patterns such as a sudden increase in payments to a person or entity, or complaints about slow payment from suppliers or clients, or an increase in written-off work in progress.
- Handwritten amendments on cheques returned from the bank.
- Double endorsed cheques which pay the fraudster personally. Look for names that are similar but not quite the same as existing clients and parties.

For more information see "Fraud on the Inside: What to do when partners, associates or staff commit fraud" at lawpro.ca/magazine

TIPS

- Conduct regular and random spot audits of lawyers and staff with access to law firm trust accounts.
- Keep an eye on lawyers and staff morale.
- Create a law firm culture which encourages mentorship and collegiality.
- Use unique passwords for anyone with access to law firm trust accounts.
- Create accounting systems where one person does not have full control or access to the money.
- Conduct a proper investigation, including gathering evidence and obtaining legal advice before proceeding on any suspicions of internal fraud.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on "All Fraud Warnings" for a list of confirmed fraudsters.

© 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 the topics covered, and readers are encouraged to conduct their own appropriate legal research.

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

The background of the lower half of the page is a complex digital graphic. It features a grid of binary code (0s and 1s) in various shades of blue and green. Overlaid on this are several glowing digital elements: a large, semi-transparent blue circle with a red vertical line through its center; a smaller, glowing green circle with a red vertical line through its center; a glowing pink rectangular area with a jagged, wave-like pattern inside; and a glowing green circular area with a red vertical line through its center. There are also several glowing blue and green lines and dots scattered throughout the background.

If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

SIGNS that your client may be a fraudster

- Property owned by same person or family for several years
- Property may be mortgage free or may be subject to an institutional first mortgage and may have lots of equity, one or more recently discharged mortgages, or recent transfers. (Always request a PIN printout with full history of deleted instruments)
- Client is in a hurry and may discourage house inspection or appraisal
- Transaction closes, funds are withdrawn quickly and client disappears
- 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
- 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)

- Recent registrations and discharges of private mortgages
- 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
- Small deposit relative to price
- 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?
- Does the same picture appear on two different types of ID issued years apart?
- Is the signature similar to your client's?
- Is the client's name spelled differently in different types of documents/ID?

TIP

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



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on "All Fraud Warnings" for a list of confirmed fraudsters.

© 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 the topics covered, and readers are encouraged to conduct their own appropriate legal research.

WIRE FRAUD

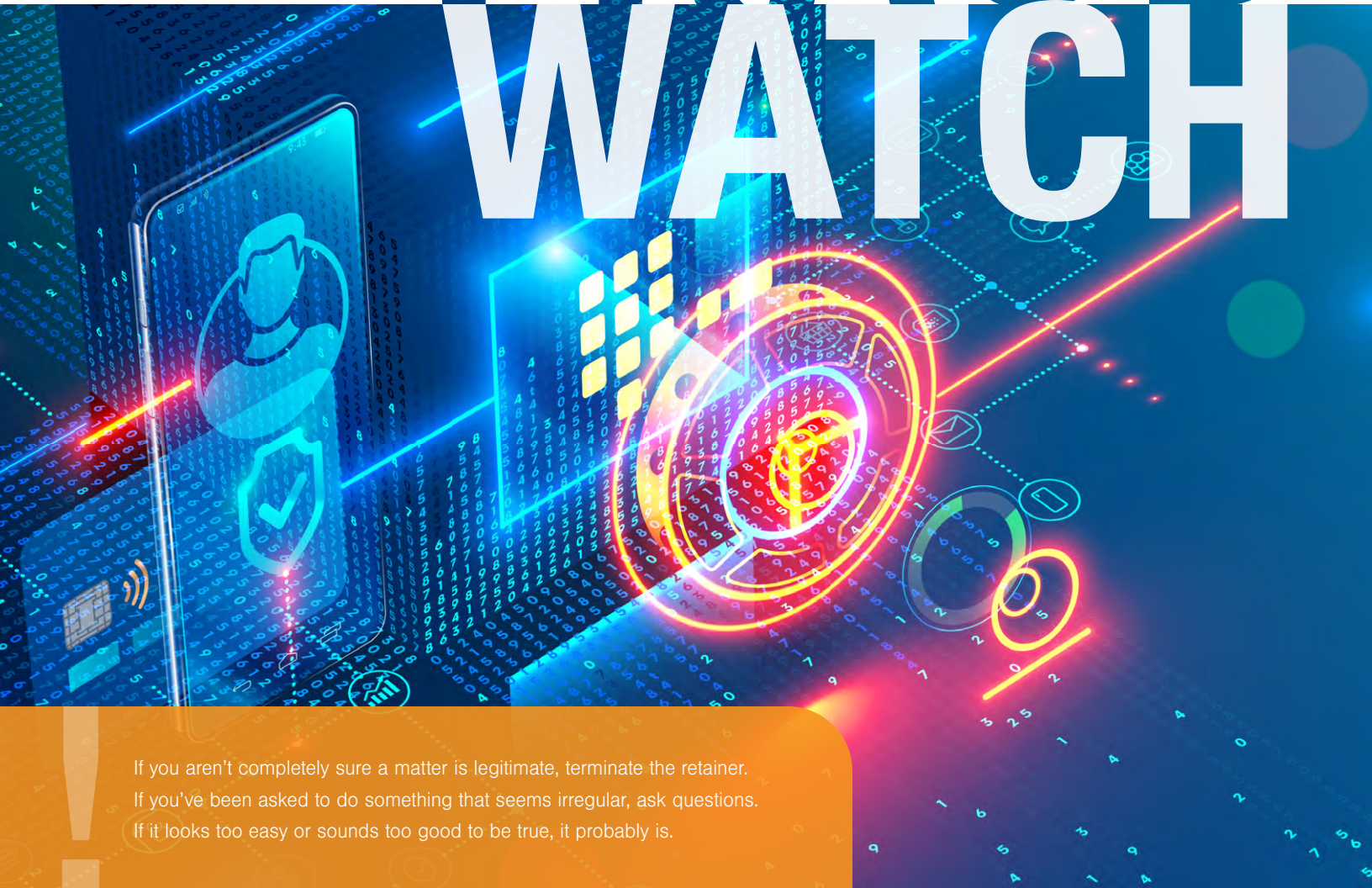
Fraudsters are actively trying to direct lawyers and law firms to wire money to them – often through spoofed emails of people you know or hacking into emails.

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



If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

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 authorization 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.

Use this wire checklist: Funds Transfer Instructions Verification Checklist.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on "All Fraud Warnings" for a list of confirmed fraudsters.

© 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 the topics covered, and readers are encouraged to conduct their own appropriate legal research.