

When the unthinkable happens:



Internal fraud very costly for LAWPRO

Internal fraud has been very costly for LAWPRO. We have recently seen two major multiple frauds by long-serving and trusted law clerks. The losses on these totalled \$6 million. In one case the lawyer was simply duped by a staff person. In the other case the lawyer totally abdicated responsibility to monitor files and the trust account to a clerk. In both cases it was a long-standing and most trusted employee who committed the frauds.



David Debenham, LLB, C.M.A, D.I.FA., C.FE, C.FI.

Finally, partners and associates often set up shell companies for a number of purposes, so it is an easy matter for them to do so as an instrument to divert monies into their own hands. Partners usually commit frauds by diverting proceeds in transaction forms that they are most familiar with – litigation lawyers will divert settlement funds, commercial and real estate lawyers will divert sale and mortgage proceeds.

Staff fraudsters, on the other hand, will take advantage of flaws in your accounting and internal control systems. They rarely use dummy corporations or divert payments to clients of the firm. They will divert payments to spouses or other family members, family businesses, or fictitious clients or suppliers.

Assistants get so good at “forging” their lawyers’ signatures as a matter of practice that these signatures no longer arouse suspicion when forgeries are used for personal purposes. Although most firms may have formal checks and balances in place, there are often informal procedures – such as assistants forging their lawyers’ signatures – that override the normal checks and balances for the “emergency” claim for lien, mortgage, real estate or commercial transaction. It’s these “exceptions” that allow the person of interest (POI) to “backdoor” the normal process for his own ends. This includes anyone with the ability to rush into a lawyer from another branch of the firm and ask for a “rush” approval signature for an “urgent” transaction, because partners who sign cheques in this way are no controls at all. The formal practice of separate cheque issuance, and cheque requisition approval, and other division of duties are often honored in the breach, making detecting the irregular transaction much harder.

Character

The POI, by definition, has to be in a position of trust – normally a long-term member of the firm. Usually it is the person whom you are least likely to suspect on the surface because your most trusted employees have the greatest opportunity to circumvent office procedures without exciting suspicion. They rationalize wrongdoing to save their family, or to save their self-image. The stress of leading a double life as a respected member of your firm while covertly stealing from you leads most fraudsters to tell you that they they were going to pay back the “loan” if given enough time.

How to spot a fraud

Where then do you start your investigation? The usual suspects are dealing with wills and estates, plaintiff’s personal injury, and large commercial practices (particularly commercial real estate) where one can “borrow” large amounts of cash flow through the firm’s trust accounts. Within these practices, files involving vulnerable or institutional clients where bills are less likely to be scrutinized or questioned are most vulnerable.

How do you catch the lawyers and staff who prey on these practices? Make them the focus of ‘surprise audits’, or rotate staff routinely, or enforce separation of duties. Have the accounting department check that clients and suppliers are receiving the payments issued by the firm. Then review all firm cheques for handwritten amendments to the payee or for double endorsements of the cheques when they come back from the bank.

As lawyers like to use shell companies to divert payments, the corporate law clerk should be questioned about any corporations for which a lawyer is the signing officer, or who pays the annual government filing fee, or who refuses to bill a client for any work done for a corporation.

Mail for a corporation for which no client file is opened, or billed, is an obvious red flag. So too if there are minute books kept and maintained in the lawyer’s office rather than with the corporate law clerk. Having a shell company is a tell-tale sign in itself. Pay special attention to payments to numbered companies. Clients or suppliers who are complaining of slow payment may be a symptom of a Ponzi scheme in which monies intended to pay them are being used to pay someone else.

Lawyers with a large amount of written-off WIP may be billing that time but not submitting the accounts through the accounting department, and appropriating the payments by endorsing firm cheques over to themselves or by directing clients to pay them personally instead of the firm. Accounts being billed and then written-off may be receiving a similar treatment.

Miscellaneous or general files are also good hiding places for fraud, particularly if the files are never billed. Invoices paid by the firm for even amounts like \$275.00, instead of an amount that reflects PST and GST, are a tip-off. Payments to credit card

How to respond to and investigate a suspected fraud

- 1) Rotate staff so that someone new either does the job of the person of interest (POI), or works for the person, and see if they notice anything peculiar in the ways things have been, or are being, handled.
- 2) Serve notice throughout the department that strict compliance with office procedures regarding separation of duties will be enforced so that the POI has to dupe as many people as possible each time a fraud is perpetrated.
- 3) Conduct surprise audits without it appearing that you are targeting anyone specific.
- 4) Hire independent counsel, a forensic investigator and possibly a forensic accountant for advice.
- 5) If you have a fidelity bond, follow the procedure stipulated in it.
- 6) Review the POI's terms of employment to ensure any investigation does not infringe their contractual rights or their right to privacy.
- 7) Search the server and all computer and accounting records available to you. Accumulate all documentary evidence you can.
- 8) Have the person take a holiday or work outside the office to give you an opportunity to investigate his/her office, subject to any privacy rights the POI may have. If necessary, investigate at night and weekends.
- 9) Change passwords, preserve evidence. Change passwords throughout the firm, and grant the POI only as much access as he/she would need to conduct legitimate business. It may be that the POI has unauthorized access because someone was lax with a password. Preserve evidence by photocopying documents and backing up electronic data on any servers. Don't forget data on desktop or laptop computers.
- 10) Investigate any suspicious documentation to see if there are independent witnesses or other documents to support it.
- 11) If one transaction is fraudulent, treat that transaction as a template for the POI's *modus operandi*, keeping in mind that fraudsters start small and rather crudely, and have bigger and more sophisticated transactions as they go on (with sloppiness creeping in as the person's confidence grows). It is very unlikely that there was only one fraud.
- 12) Interview co-workers, keeping in mind the motives and opportunities for fraud and taking copious notes. Better still digitally record these interviews, with their permission. Keep in mind that close co-workers may either be unknowing dupes or knowing accomplices. Interview more distant witnesses before investigating close co-workers who are likely to tip-off the POI. Interview the POI last.

companies without proper back-up may be paying the lawyer's personal expenses (payments on real estate, tax, litigation, or wills and estates files to the Receiver General are often paying the lawyer's personal taxes).

Anything unusual, or any change in pattern, such as a sudden increase in payments to a particular person, may indicate double-billing or cheques to non-arm's length or fictional persons. When employees embezzle from their employers, they generally alter, forge, or destroy checks, sales invoices, purchase orders, purchase requisitions, or receiving reports. Red flags to look for include: missing documents; names of payees or customers that are similar to those of firm members; addresses that are similar to firm members'; or P.O. boxes.

Further investigation to see if firm payments are being redirected by staff is also warranted if:

- the firm is getting past due account notices when it should not;
- if there are second endorsements appearing on firm checks when they come back from the bank;
- if documents appear altered, or handwriting on documents is questionable; or
- original documents are missing.

Finally, and most importantly, anonymous complaints from staff, or from clients, suppliers, or others, may be indicative of a larger problem. Having an anonymous whistle-blowing mechanism helps immensely in detecting and investigating fraud.

Co-worker vigilance

Fraud consists of the fraudulent act, concealment, and conversion. Co-workers often witness the fraudulent act and may comment on the "odd" way a transaction is being handled or explained. The accounting department does have a chance to find fraud at the concealment stage when it notices missing or altered documents, miscounts, or other anomalies. However, the accounting department often goes to the POI first for an explanation and, not suspecting fraud, is often satisfied with the explanation or allows the POI a second chance to "substantiate" the transaction with forged documentation.

There is no way auditors can know, for example, that an employee who used to drive a used, inexpensive car now comes to work in a brand-new expensive one or that an employee suddenly expresses changes in behavior. It is co-workers who have an opportunity to identify aberrant behaviour and a change of lifestyle, witness a fraudulent act or its concealment, and witness the POI's new found wealth as part of out of office friendships and office gossip. That is why most POI's are caught not by auditors, but by co-workers who provide their employer with an anonymous tip and why honest employees who are vigilant for fraud are your most important investigative tool.

Dealing with a suspected fraud

So what do you do if you suspect a fraud has taken place? You must respond with tact and care so you comply with your obligations under the LAWPRO policy, the Rules of Professional Conduct, and requirements under employment law.

Approach the investigation on the presumption that there is an innocent explanation for what has occurred. Only when all innocent explanations have been disproved can you conclude fraud. All exculpatory evidence must be recorded and investigated. Don't hesitate to pursue the investigation due to the fact the fraud appears to involve a long-standing and most trusted employee – they are the ones that have the greatest ability to misappropriate funds.

If the fraud involved client trust funds or there is a negligence claim, and even if there is only the possibility of one (remember that frauds often end up more complex than they first appear to be), report the fraud to LAWPRO.

Consider also your obligations under Rule 6.01(3) of the Rules of Professional Conduct – the Mandatory Reporting rule. Any misconduct by a lawyer or involving client trust funds will likely have to be reported to the Law Society.

The sidebar *How to respond to and investigate a suspected fraud* sets out the various steps you need to take to investigate a suspected fraud.

Confronting the suspect

Confront the suspect last. Be wary of an "incident" as people can react unpredictably if they have been under pressure for a long time or feel threatened. Any interviews should be done privately, with at least two management personnel present to serve as witnesses. Do not meet near other employees in the workplace, and meet before or after work hours (which is not a problem if the suspect is a workaholic).

Do not invade the person's privacy at the office (personal possessions such as briefcases) without express permission. A technology-use policy that explicitly gives you the right to review e-mail and data on a computer can be a huge help in removing any question as to the ability to access this data (See a useful technology-use policy precedent on the Law Society of British Columbia website www.lawsociety.bc.ca/practice_support/articles/policy-internet.html).

As part of the confrontation meeting, make sure you get all firm credit cards, keys, etc. from the suspect, and escort the suspect out of the building without returning to his/her office. Return personal property later. Be prepared to close all physical and electronic points of access. For an itemized departure checklist, see the *LAWPRO Checklist for a departing employee* (www.practicepro.ca/practice/pdf/EmployeeDepartureChecklist.pdf).

Terminating the POI does not mean that the POI has been proven a fraudster, and it should not be treated as such by the firm. Moreover, the person is usually a trusted long-standing employee or lawyer who has many friends in your firm. Therefore, all post-termination steps require a great deal of sensitivity and tact. See the *What to after the suspect has left the building* sidebar below for the steps you must follow.

David Debenham is a Certified Fraud Examiner and a past Director of the Association of Certified Forensic Investigators of Canada. He is author of The Law of Fraud and the Forensic Investigator published by Carswell. David currently chairs the Law Practice Management Section of the Ontario Bar Association. He practises commercial litigation in the Ottawa office of Lang Michener LLP, and has a Diploma in Investigative and Forensic Accounting from the University of Toronto.

What to do after the fraud suspect has left the building

- 1) The managing partner must “quarterback” the repair of your firm, exercising full authority over everyone in the firm to do what is needed expeditiously.
- 2) Make sure all points of access for the departed employee are closed – review and take all steps on the LAWPRO checklist (www.practicepro.ca/practice/pdf/EmployeeDepartureChecklist.pdf).
- 3) Move to protect clients immediately (their assets and their confidences and their right to a seamless transition in service). You may need to tell clients some details of what has happened.
- 4) Make sure clients, employees or your firm get ILA, if it is appropriate.
- 5) Archive all of the suspect’s files (paper or electronic), segregating his or her workspace to preserve the evidence.
- 6) Monitor the suspect’s voicemail, e-mail and regular mail within the limits of the law.
- 7) Be prepared to address the concerns of firm stakeholders and answer press inquiries. Depending on the scale of the incident and the likelihood of adverse media coverage, consider obtaining expert crisis communication advice.
- 8) Notify all fidelity insurers, and if appropriate, the Law Society, LAWPRO and any excess insurer of the status of your investigation, and your findings leading to the termination.
- 9) Have a replacement for the suspect in place forthwith (in a different workspace with a different phone and e-mail account) to ensure a seamless transition of service to the firm and clients. Calls for the suspect should be logged by the receptionist.
- 10) Be prepared to deal with co-workers in the grieving process over the sudden loss of the suspect when news of the departure has spread within the firm (this is highly combustible gossip after all). Disclosing the exact reason for the departure is likely not an option.
- 11) Act promptly to complete your investigation and take steps to ensure that shortcomings in the firm’s internal controls have been identified, and remediated with the assistance of an expert in the field with all due speed.
- 12) If the circumstances warrant, call the police.