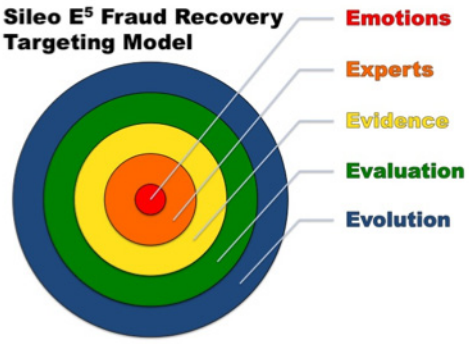
Fighting Friendly Insider Fraud: 5 Targeted Response Strategies

GT43FFWP

Most small business owners never see it coming. They rarely understand that fraud can consume enough time and energy to potentially destroy their company and certainly alter their lifestyle. And in almost every case, they fail to suspect the most common mastermind of fraudulent schemes — a highly trusted, inside advisor. In fact, **fraud is a crime rooted in trust, particularly in misperceptions of trust**.

In many cases, it is a business owner's unwarranted confidence in a key employee that not only opens the door to fraud, but actually encourages the crime. When we speak of **friendly fraud**, we are referring to a trusted insider who gains an owner's deep trust, a position of power and an unethical approach to opportunism. Spotting the signs of fraud and the tools of fraudsters is something we covered in Safeguard's newsletter article, *Fighting Friendly Fraud*, so here we'll focus on building a roadmap of steps you can take should you suspect fraud inside of your organization.



To understand the importance of following a wise and rational path in the face of friendly fraud, take the failure of my forty-year-old business as a by-product of embezzlement fraud. Two years wasted, $300,000 lost and many lawsuits later, I learned that business owners need help to avoid a drawn out disaster like ours.

Instead, you need to understand the **importance of targeting or prioritizing your attack** should you suspect fraud. Moving forward impulsively *will* jeopardize your case and put you at risk of legal liability, which only makes the nightmare worse. For starters, you need to ignore your desire to confront the culprit and fantasies of revenge for the moment and adopt a methodical approach to the challenge. And that's the first of our *5 Targeted Response Strategies*.

1. Control Your Emotions.

Being victimized by friendly fraud is like discovering that your spouse has been *having an affair with your best friend.* I don't make this reference in a casual way; I make it because there is a highly charged emotional component in both scenarios. **Your first response (e.g., to confront the person) is likely to be dangerously reactive — driven by emotion rather than reason**. Knowing the criminal who harmed you adds an emotional dimension that often gets in the way of good decisions. If you suspect that someone is defrauding you or your business, you might be tempted to make impulsive accusations, to retaliate or to contact law enforcement. Don't allow your fight or flight mechanisms to override your self-control. Instead, take these steps:

- Resist the urge to make unsubstantiated accusations. Following incorrect procedures in accusing someone of fraud can end in a defamation lawsuit, even if the suspect actually committed the crime. In many cases the fraud in question was not committed by the initial suspect, so be careful not to warn the real culprit of your investigation.
- Limit the number of people you tell about the fraud. Not only does fraudulent behavior suddenly disappear at the first sign of suspicion, it also commonly involves multiple players in the same business.
- Become highly methodical and detail oriented in building your fraud case. Make sure that you log every irregularity you detect and every action you take, as these notes might prove important in court. Additionally, take detailed notes when you meet with your team of experts.

2. Build a Team of Experts.

> *"In one case of fraud recovery, we saw complete server hard drives wiped clean, backup disks destroyed, laptops stolen, files removed and a suspect who left the country, all between midnight and 6 a.m."*

It's easy to convince yourself that you are at fault for allowing fraud in the first place and therefore are solely responsible for solving the problem. This isn't only incorrect (preventing and detecting fraud is rarely one person's responsibility), it is naïve and potentially harmful to your cause. **Unwinding a case of true fraud requires help — trained professional help**. This is where your team of experts comes into play.

Small business owners often balk at the costs of hiring true experts. But if you've lost substantial sums of money or are considering prosecution, taking the cheap route is like skipping the malaria shot on your way to the jungle. If you're going to play the game, play it smart. A weak or non-existent team can be even more costly in the long run as you deal with incompetence, counter lawsuits and wasted time. Your team will need at least three key players as well as a supporting cast:

- *An Employment Lawyer.* You need to make sure that you follow correct legal procedures for ethically monitoring, documenting and terminating an employee involved in fraudulent behavior. Employment laws can vary by state, so use advisors well versed in both state and federal employment law.
- *Not Just Any Accountant.* You will save yourself hours of time and thousands of dollars by hiring an accountant who knows where to look for the fraudulent needle in the credit/debit haystack. Hire a CPA that specializes in forensic accounting and is a Certified Fraud Examiner (CFE).

- *An IT Wizard.* So much business data is stored electronically these days that you will need an expert to track down digital files, unlock password-protected evidence and eventually restrict user-level access after termination. If the person you suspect of fraud is in information technology, they are already many steps ahead of you in disguising electronic evidence.

3. Collect & Protect the Evidence.

One crucial reason to control your emotions and proceed methodically grows from an unfortunate reality: a fraudster's initial, panic-stricken reaction will be to destroy everything that might be considered evidence. **In the digital age, evidence destruction can happen in the blink of an eye**. In addition to missing proof, this often leads to a great deal of collateral damage that affects business operations beyond the fraud. In one case of fraud recovery, we saw complete server hard drives wiped clean, backup disks destroyed, laptops stolen, files removed and a suspect who left the country, all between midnight and 6 a.m. The loss of these items can mean the loss of your legal case, the inability to recover funds and, far too often, the downfall of the business. Take these steps to collect and protect your evidence:

- Make physical copies of key documents and store them off site
- Create an offsite backup copy of all files on all systems. This can be implemented immediately (and quietly) using a system like SOS Backup.
- Don't make any accusations until your evidence is rock solid and you are fully prepared to deal with the consequences, including escorting the employee out of the building
- Never hold the termination meeting in the suspect's office, as this allows for the undetectable destruction of evidence. Confiscate all mobile computing devices that are the company's property.
- Always have a highly credible witness in the room during termination

- Have your technician or IT department immediately restrict the employee's access to all systems and networks including website logins, remote devices and virtual private networks
- Consider changing the locks or keycard access codes if necessary
- Immediately inform other employees that the suspect should under no circumstances, be allowed back in the building or access to their login credentials

4. Evaluate Your Options.

Every business owner must make their own decision on what options to take once they have terminated the fraudulent employee. Many decide to prosecute and attempt to recover the funds. **Other times, however, the best response to fraud is to eliminate the fraudulent employee(s), write off the loss and *move forward without prosecution***. Determining the best way to recover from fraud should be a business decision that you make with your lawyer, your accountant and your closest advisors, not an emotional decision that you make in the heat of the moment. Often, your return on investment from the prosecution path is abysmal, especially when you factor in hidden costs beyond the billing rate of an accomplished attorney:

- Lost time focusing on a court case rather than your business
- The emotional toll of having fraud become your full-time job
- Time away from your family while you fight the battle
- The chances that you will lose the case or face counter suits
- The very real chance that the employee has no way to pay back what was taken (fraudsters aren't generally very responsible with money)

In certain cases, we have seen defrauded business owners negotiate a contractual repayment plan in exchange for a promise not to prosecute. This and all other options should be discussed with your lawyer.

5. Evolve Your Processes.

Even after getting hit by fraud, many businesses fail to evolve their outlook and processes — they keep the same bad habits. The most frustrating result we see once a business has completed the fraud recovery process is to do nothing to prevent another case. **The costs of prevention are a fraction of recovery, just like exercising *before* the heart attack**. Just because the case is over doesn't mean your work is complete. Make sure that you take the following steps to discourage future cases of fraud:

- Train your staff to recognize the signs of fraud and let them know you are constantly watching out for fraudulent behavior
- Conduct regular, highly visible fraud detection audits that send a clear message to any potential fraudsters that they will get caught
- Install proper oversight of fraud hot spots such as accounts payable, accounts receivable, check signing, payroll "ghosts", credit card reconciliation, bank transfers, ACH permissions, inventory shrinkage and financial reviews
- Modify your hiring practices to include aggressive background checks, social media research, credit history and driving record verification
- Require employees to sign an acknowledgment that they have given notice of your expectations of behavior and the consequences of committing fraud
- Verify that you have a strong fidelity bond or "dishonest employee insurance" to cover your assets in case it does happen

Above all else, recognize the **importance of carefully reviewing your company's financials yourself**. Only a highly engaged business owner will be prepared to detect suspicious behavior, and that takes extra effort. One of the harshest realities in small businesses is this — the owner is often times the only person in the company who cares enough to stop fraud. For everyone else, it's just a job.

John Sileo became an expert in small business security the hard way — by losing $300,000, his business and two years of his life to friendly fraud. Bouncing back, John became an award-winning author and keynote speaker on fraud, identity theft and online privacy. He is CEO of The Sileo Group, which advises teams on how to balance risk and defend privacy. His clients include the Pentagon, Pfizer, the FDIC and Homeland Security, and he's recently appeared on 60 Minutes, Anderson Cooper and Fox.