

# Lions Gate Investigations Group

**This article and the information contained here-in, is posted for the interest and education of clients of the Lions Gate Investigations Group, as well as others who have been or may become the victims of fraud.**



## Guarding Against Fraud

*CSO Magazine (08/09) Vol. 8, No. 6, P. 28; Collett, Stacy*

A study from the Association of Certified Fraud Examiners indicates an increased incidence of fraud perpetrated by employees driven to such extremes by downsizing and other fallout caused by the economic downturn. There are a number of strategies chief security officers (CSOs) can follow to fortify their defenses against occupational fraud, such as implementing policies and procedures to detect illicit activity faster. These can include audits and monitoring, data access control, employee education, physical security, and discreet fraud disclosure techniques. Spot audits should be an essential component of a fraud monitoring program, and security consultant Adam Safir says accounts ought to be reconciled every day with no fluctuations. Physical security measures can include security guards, locking cabinets containing sensitive data, proper and careful disposal of sensitive documents, and giving employees access to confidential data on a need-to-know basis. The call center is another area that needs security, so background checks should be performed on all employees before hiring them. When employees are on the job, their computer activity should be monitored, and CD drives or USB ports should be deactivated to thwart copying of information. Occasional surprise visits from supervisors can be an effective deterrent against fraud from employees who work at home, while Hunton & Williams partner Lisa Sotto suggests segregating the PC from family members and using strong encryption and password protection for PC access. Employee awareness and training about fraud protection and security is one of the easiest and least expensive fraud reduction strategies, while antifraud policies and procedures should be elements of an overarching security program, with input from the general counsel. "A good CSO doing the job proactively and doing it well ends up speaking the language of and servicing the general counsel whose basic duty it is to ensure on behalf of the board that upper management isn't doing anything [fraudulent]," Safir says.

## How to Stop Fraud

## **The Madoff and Stanford cases may grab the headlines, but the temptation of fraud appears at every corporate level**

By [Stacy Collett](#) - July 06, 2009

Bernard Madoff, Allen Stanford and California money manager Danny Pang may be the latest examples of outrageous fraud. But what about the little guys? The administrator, middle manager or call-center rep?

It doesn't take a high-profile, multibillion-dollar scandal to rock an enterprise. These days, when employers are cutting salaries, staff and bonuses—and staff is uncertain about the [next round of layoffs](#)—more employees are committing fraud, according to a study by the Association of Certified Fraud Examiners. More than half of fraud examiners surveyed said that the level of fraud has slightly or significantly increased in the previous 12 months compared to the level of fraud they investigated or observed in years prior.

U.S. organizations lost 7 percent of their annual revenues to fraud between 2006 and 2008 for an estimated total cost of \$994 billion in losses, according to the ACFE. That's a slight uptick from the 5 percent loss reported for the two-year period ending in 2006.

What's more, about half cited increased financial pressure as the biggest factor contributing to the increase in fraud, compared to increased opportunity (27 percent) and increased rationalization (24 percent).

Fraud can include minor things like expensing personal items or major, fraudulent billing schemes carried out over months or years. "They're using the corporate credit cards for expenses that are really tying back to people in the accounting department to fill their own needs," says Adam Safir, COO of security consulting firm Safir Rosetti in New York. "We've had clients where individuals have racked up \$500,000 worth of transfer payments to various parties that were done piecemeal through small [charges]" over several months.

[Also see the in-depth Anatomy of a Fraud](#)

Making matters worse, layoffs are affecting organizations' internal control systems, according to the ACFE study. Nearly 60 percent of companies say they had experienced layoffs during the past year. Among those who had experienced layoffs, more than a third said their company had eliminated some controls for preventing fraud.

### **Warning Signs of Fraud**

- Excessive or inappropriate contact with a particular vendor, or a familial relationship between an employee and vendor, can lead to fraud. Sloppy record-keeping can also mask illicit activity.
- An employee who is living beyond his or her means or is known to be having financial difficulty may become desperate enough to commit fraud.
- "We've seen people withdrawn or becoming very hostile," who were committing fraud, says Adam Safir, COO of Safir Rosetti. There are also cases where employees maintain a low profile and "fly under the radar" while keeping a fraud scheme going for months.
- "Keep your ear to the ground," Lisa Sotto, a partner at Hunton & Williams adds. Sometimes rogue employees can't keep their mouth shut, she says, so listen to what employees are chatting about at the water cooler.

"I don't think this is anything new, but with the economy down and people getting desperate, this is a methodology that they use that takes advantage of a typical weakness," such as poor oversight or holes in security procedures, Safir says.

Fraud examiners expect that number to rise during the next 12 months, especially embezzlement cases and an increase in Ponzi schemes investigated by the SEC, says Bruce Dorris, ACFE program director. "The credit market is drying up and there's not as much capital to raise for those types of frauds, so you're going to see a lot more reporting" as investors realize they've been defrauded.

In these tough economic times, CSOs need to harden their defences against fraud.

## **Fraud Frenzy**

Embezzlement accounts for 70 percent of fraud cases. "That's employee theft across the board" from C-level execs to administrative staff, Dorris explains. That's anything from fabricating vendors to charge payments to corporate credit card misuse, taking petty cash "down to stealing pencils, pens and notepaper."

Vendor fraud is also on the rise. Examiners are detecting fraud schemes in contract and procurement areas, where, for example, a vendor suddenly shows a marked increase in contracts over the previous year—especially low dollar amount, no-bid contracts, which may indicate kickbacks to employees.

Data fraud cases continue to concern employers, but now many employees who fear losing their jobs are using stolen client lists, marketing data or company secrets to leverage new jobs. Some 59 percent of employees who leave or are asked to leave a company are stealing company data, according to a report by the Ponemon Institute, and two-thirds of them admit to using their former company's confidential, sensitive or proprietary information for new employment.

But even without economic pressures and downsizing, data theft "certainly is an issue that has existed and continues to exist" on a daily basis, says Lisa Sotto, a partner and head of the privacy and information management practice at Hunton & Williams, which represents companies who have suffered a security breach, often by rogue employees.

[Call center agents, for instance, are highly susceptible to breaches because they have easy access to customer data](#), and callers are willing to give up sensitive information, such as credit card numbers, Sotto says. What's more, healthcare and insurance providers often use Social Security numbers to authenticate a patient's identity on call center inquiries.

## **Fundamentals of a Good Anti-Fraud Program**

Some fraud schemes have taken up to two years to detect. Illegal activity can be detected faster by having policies and procedures in place that include audits and monitoring, data access control, physical security, employee education and discreet ways to report fraud.

**In the Accounting Department.** Look at relationships between vendors and employees, such as familial relationships between vendors and purchasers or a sudden increase in contract awards to a particular vendor, which may lead to fraud, and set policies regarding those relationships.

A fraud monitoring program must include spot audits. Accounts should be reconciled daily with no variances, Safir says. That way, "you know immediately that you have a problem that requires further investigation. At some companies, their accounting department becomes too complex and they'll carry over imbalances" — a very unsafe practice, he adds.

Also, [separate duties](#) between accounts payable and accounts receivable. "You could train a non-accountant to do your payables. That person would not be reconciling your pay statements like an accountant would," Safir says.

Surprise audits continue to prove effective in catching fraud. "If they know that corporate security is doing audits on the first Tuesday of the month, they take care of everything on Monday. But if they don't know they're coming, they're more likely to catch a fraud in place," Dorris says. Also, when employees know that a surprise audit looms, "they're less likely to [commit fraud] because the opportunity has been removed."

Simply [checking financial statements](#) can uncover fraud. "Why is there a tremendous increase this month in accounts receivable? Are they inflating numbers to make the bottom line look better, to increase earnings per share? Those don't require a tremendous amount of resources—that gives you some predication to look and see an anomaly—and investigate it a bit further," Dorris says.

**Around the Office.** Physical protections in the building and its perimeter can also curb fraud. Do you have someone at the front door? Are you locking cabinets with sensitive data in them? Do you have a policy on transporting removable media like laptops and BlackBerrys? Where is the company trash going? Sotito recalls one multibillion-dollar, family-owned company that 20 years earlier donated reams of used paper to a preschool for a recycling drive. Recently, one of the preschool's parents called to report that one of her son's preschool art projects included names and social security numbers on the backside.

Any [sensitive documents should be shredded](#) or designated for burning.

Employees should have access to confidential data on a need-to-know basis. Review access rights weekly or quarterly, and terminate access immediately for any employee leaving the company. Make sure everyone has the right levels of access, and mask some of the data for some levels of access. Audit log software can also document who logged into what documents and systems, when and whether they made changes or exported files.

**In the Call Center.** Fraud prevention in the call center begins with [background checks for all employees](#) before hiring them. Once they're on the job, monitor their computer activity. "See what they're looking at and why," Sotito says. Deactivate CD drives or USB ports so information can't be copied. Adopt a paperless work environment so information can't be written down and documents can't be removed. Keep purses and backpacks outside of the call-center room.

**At Home.** Employees who work from home can be difficult to monitor. Sotito suggests occasional surprise visits from a supervisor. "Have policies in place where the PC is in a segregated area away from family, use strong encryption and password protection" for PC access, she adds. (Also see [Seven Deadly Sins of Home Office Security](#).)

**Hotlines.** Occupational frauds are much more likely to be [detected by an anonymous tip](#) than by audits, controls or any other means, according to the ACFE. Hotlines are one of the easiest ways of allowing those tips to come in. Sarbanes-Oxley requires public companies to establish whistle-blower hotlines, and many private companies are following suit. Other companies have set up anonymous e-mail programs "or a locked box in the coffee room for notes," Dorris says.

**Employee Education.** One of the easiest and most inexpensive ways to reduce fraud is through employee awareness and training about fraud protection and security.

Employees can be trained on how to handle sensitive documents left near printers, for instance. "They may be unknowingly printing important information that can be used in a fraud or theft context and leaving it near the printer," Safir says. "Most importantly, let employees know from their first day of employment of the company's rules and expectations regarding fraudulent activity—not after fraud surfaces."

## Connecting Fraud and Security Programs

Antifraud policies and procedures should be part of an overall security program, with input from the general counsel.

"Some CSOs work very closely with their general counsels, and some who are very skilled become relied upon as the 'finders of fact' for these very sensitive issues," Safir says. "A good CSO doing the job proactively and doing it well ends up speaking the language of and servicing the general counsel whose basic duty it is to ensure on behalf of the board that upper management isn't doing anything [fraudulent]."

In rare cases, CSOs can find themselves at odds with executives who might be engaging in rogue behavior themselves, over certain control environments or his or her responsibilities to the general counsel reporting to the board. A series of checks and balances can clear that impasse.

"You have a board of directors, an audit committee and control procedures that public companies need to comply with, and a lot of private companies have adopted this as a best practice," Safir says.

## The Tone at the Top

Internal controls are effective only if they are implemented from the top down. The "tone at the top" dictates the effectiveness of any fraud control program, Dorris advises. "If those C-level officers demonstrate integrity and honesty and being forthright with employees, directors, investors, customers and purchasers, those companies become more successful and less likely of fraud in the organization."

Sheilah Etheridge, owner of SME Management in Anchorage, Ala., makes a living by cleaning up "the aftermath of an unqualified accounting person or staff," and she has seen her share of occupational fraud.

"The recession will not cause anyone who is honest to become dishonest," Etheridge says. "But it may be a handy excuse for those that have thought about it before to act on it, or those already embezzling to up the ante."

The Lions Gate Investigations Group can be contacted by calling 604-684-7753 / 7313 or by emailing Scot Filer at [scotfiler@lgig.ca](mailto:scotfiler@lgig.ca) or Fred Pinnock at [fredpinnock@lgig.ca](mailto:fredpinnock@lgig.ca) .