



FINANCE

✉ CLAUDE.SOLNIK@LIBN.COM

☎ 631.913.4244

🐦 @CLAUDESOLNIK

F for fraud

Study finds employee tips, phones best ways to catch fraud

By CLAUDE SOLNIK

If you want to find fraud, who are you going to call? Your accountant? Not necessarily.

Many people think traditional audits are likely to detect fraud. But firms hired to review financial statements rarely detect fraud, in part because it's usually too small to catch that way. Instead of calculators, the phone, including tip lines, has proved to be the most effective tool to fight fraud, according to a recent study.

The Association of Certified Fraud Examiners' 2016 Report to the Nations on Occupational Fraud and Abuse — which essentially means fraud in the workplace — found 5 percent of annual revenues typically are drained due to fraud.

The average fraud in the United States cited in the study cost \$120,000, far less than the \$245,000 in the Asia-Pacific and \$268,000 in Western Europe.

The higher up someone was in the organization, the bigger the fraud, with owners typically siphoning off \$703,000, managers taking \$173,000 and employees taking \$65,000 on average.

But if you think routine audits frequently unearthed these problems, you'd be wrong. External audits detected a minuscule 3.8 percent of frauds, in part because they're not fundamentally designed to ferret out fraud.

"A lot of businesses seem to rely on auditors and accountants to detect fraud," said Michael Kupka, director of forensic accounting and dispute resolution services at Manhattan-based Mazars USA, with Long Island offices in Woodbury. "Auditors aren't hired to uncover fraud."

Routine audits are designed to catch massive or material errors and frauds, but not specifically to detect the full range of frauds.

"If the fraud is large enough, the auditors are responsible for it," Yigal Rechtman, forensic principal at Grassi & Co. with Long Island offices in Jericho, said. "The purpose of the audit is not to catch fraud. However it is to catch any mis-statement, no matter what the reason."

A forensic audit, a different process done to investigate possible fraud, is more likely to find out what occurred. But that's typically done to verify a suspicion.

"It's much more action-driven," Kupka said. "You come in and address specific issues the management may have."

So what works? The phone turns out to be the most powerful tool to bust fraud: Tips, typically through hotlines, detected 39.1 percent, or more than one in three, identified frauds.

That's far more than the 16.5 percent detected through internal audits, while management reviews found 13.4 percent and sheer accident unearthed 5.8 percent.

"The best way to do it is anti-fraud tools. Tip lines are big," Kupka said. "And putting systems in place that uncover the fraud."

Rechtman said tip lines let employees who see something say something anonymously, although most companies don't have these lines. The Association of Certified Fraud Examiners and answering service companies help firms set up hotlines.

"You give them a script and questions to ask," Rechtman said of answering services. "And you have to publish it to your vendors, customers and employees."

The front lines of fraud

Fighting fraud, however, begins with preventing rather than detecting. If corruption is part of a company's culture, the firm is likely to become a victim of it.

"It starts with the environment established by top management levels," Kupka said. "The first step is to take fraud seriously."

The way people are treated matters as much, or more than, how much they are paid. Employees who resent their firm are more likely to steal from it.

"Most people do not look at their salary as an indication of how happy they are at the office," Kupka said. "How do you treat your employees? How flexible are you? What type of environment do you create in the office?"

Olga Danilycheva-Averin, a partner in forensic accounting and evaluation services at Prague Motio CPAs, with Long Island offices in Woodbury, said internal control portions of audits can help prevent fraud.

"Internal controls are part of every audit," she said. "It's not looking at the records. It's how the system works." Segregation of duties helps prevent fraud by reducing opportunity. If one person writes the checks and keeps the books, there's more temptation to skim.

"The same person who receives the inventory may count and ship the inventory when there's a sale," said Matthew Jahrdoerfer, a principal at Bardon with Long Island offices in Jericho. "With larger entities, you have different people doing different functions."

'WHEN YOU FIND IT, YOU NEVER KNOW HOW BIG OR LITTLE IT WILL BE, UNTIL YOU DIG INTO IT. IF YOU FIND SOMEONE STEALING A HUNDRED BUCKS, HOW DO YOU KNOW THEY DIDN'T DO THAT 1,000 TIMES?'

Small companies have strengths and weaknesses. The owner may find problems, if he's familiar with internal operations. But small business people frequently believe they are immune to fraud: Dualist creates fertile ground for fraud.

"I think maybe people get lax with their controls, because they do trust these people," Jahrdoerfer said. "If someone's been an employee for 20 years and never had an issue, they trust them."

Hiring people not particularly susceptible to fraud can help. Making honesty a hallmark of a company can benefit it.

"This comes down to the hiring practices," Kupka said. "You want to weed out people with issues in their lives, to the extent possible. People with fraud in their background: You try to weed them out."

The fraud triangle

In order to fight fraud, it probably helps to understand what leads to it. It's frequently a convergence of opportunity and adversity. A fraudster typically feels pressure (often financial), has opportunity and seeks to justify stealing.

"They have to rationalize it," Kupka said. "The owner's abusing the powers. I'm working extra hours, doing more than I was supposed to. I'm entitled to this benefit. No-



YIGAL RECHTMAN: Anonymous tip lines provide an effective tool to detect fraud.

body's recognizing these efforts. I haven't got a raise in a year or two."

Employee fraud typically means the thief is at the network, cubicle or at least within the company. That leaves plenty of time to notice changes.

"Behavior is key," Danilycheva-Averin said. "When someone is committing fraud, they know they're doing something wrong. Something's got to change. If you see that person every day at the next table or the warehouse you'll notice."

Detecting changes in behavior also can reveal theft. People who won't go on vacation, for instance, may be afraid someone will find their fraud while they're away.

"Look for red flags," Kupka said. "If you see an employee living beyond their means, having issues where they need money, these are pressures."

Not all people are at equal risk. An employee working in finance is more likely to commit fraud than someone who has no access to a firm's finances.

"You should evaluate what the exposure is with that individual," Kupka said. "If that individual is a bookkeeper with no controls, you should probably pay more attention."

Danilycheva-Averin said certain patterns can be tell tale signs that an employee is doing more than their job, taking cash or data.

"If you see a co-worker spending more money than he used to," she said, "if he doesn't take vacations, it could be an indication that something could be found while he's absent. Nervousness. That's the first indication that something is wrong."

Cyber fraud

If the phone can help find problems, the computer has turned into another tool of choice for finding and committing fraud.

"What's fairly new is the influence of computers and IT ability to utilize technology in different ways than before from fraud prevention to perpetrating it," Kupka said.

Jahrdoerfer said financial and ERP (enterprise re-

See FRAUD, Page

FINANCE

Fighting fraud: ounce of prevention worth pound of detection

FRAUD. From Page 8

source planning) systems are better. Data not dollars, though, can be at risk in cyber fraud.

"A lot of smaller companies haven't been thinking about cyber issues," Kupka said. "Corporate secrets, espionage, taking information from the client lists, specs, formulas. If it's not protected well, it's open to theft."

He said computers make it easier to steal electronic data than boxes of paper, using a USB drive to walk off with customer lists, trade secrets and other information. Bidding processes can be compromised, while payroll, time cards and accounting entries can be changed.

"You can set up automatic payments to fake companies," Kupka said.

No cheap fix

While some measures to fight fraud are free, preventing fraud can be costly. Some companies may think it costs more to stop it than to let small fraud occur.

"The challenge is when you go to the client and tell them about the control issues, half of them will fix it," Kupka said. "The other half will not fix it."

Hiring an additional employee, so one person isn't solely responsible for writing checks and reviewing the books, may cost a lot. A firm may decide it's cheaper to live with the risk.

"If one person does everything, that's an internal control issue," Bechtman added. "If we tell them you need someone else, that may be too expensive."

Some people simply won't believe that they're at risk of fraud, insisting that it may happen, but not at their company. They won't believe their employees are susceptible

"One reason is ego," Bechtman said. "People think they do a good job, know their staff, customers and vendors. They don't think they will ever perpetrate fraud."

While doing too little's not good, it may not be worth it to devote resources to monitoring every detail. The price may outweigh the benefit at some point.

"As part of the control system, you have to establish what you're willing to live with," Kupka said. "Are you

'YOU SHOULD EVALUATE WHAT THE EXPOSURE IS WITH THAT INDIVIDUAL. IF THAT INDIVIDUAL IS A BOOKKEEPER WITH NO CONTROLS, YOU SHOULD PROBABLY PAY MORE ATTENTION.'

going to catch every time an employee takes a pen from a company or removes a stapler? No."

Still, it's not always easy to tell how big or small a fraud is. Finding fraud can be like tugging on a thread: The more you pull, the longer the thread turns out to be.

"When you find it, you never know how big or little it will be, until you dig into it," Jahnsoeder said. "If you find someone stealing a hundred bucks, how do you know they didn't do that 1,000 times?"

Frauds typically begin with someone creating an exception, taking money that they tell themselves they'll pay. But that soon leads to another and then another bite of the apple.



MICHAEL KUPKA: Routine audits don't detect many cases of fraud, in part because they're not expected to.

"It could be a situation where they do it once and keep doing it," Jahnsoeder said. "They might have personal financial difficulties or plans to pay it back, but it never happens."

■ CSOLN@LIBN.COM

For All Your Remodeling Needs!

WE GO TO EXTREMES TO BUILD YOUR DREAMS!

5 DAY BATHROOM by Alure

10 DAY KITCHEN by Alure

A COMPLETE GUT & REMODEL USING THE MOST POPULAR & COST EFFECTIVE PRODUCTS! CONVENIENT, LOW-COST AND TOP QUALITY WORK, COMPLETELY INSTALLED IN 5 DAYS!

WINDOWS SIDING BATHROOMS KITCHENS ROOFING PORCHES & DOORS

Alure HOME IMPROVEMENTS
 Serving Long Island Since 1946

877.44.ALURE
 877.442.5873 | alure.com

1999 Hempstead Turnpike
 East Meadow, NY

Sal Ferro, CEO/President

KITCHENS • BATH ROOMS • WINDOWS • SIDING • ROOFING • BASEMENTS • SUNROOMS • DOWNERS • EXTENSIONS

Learn More: www.alure.com | Phone: 877.442.5873 | 516.434.4181 | 516.432.4181



Fueling the economy...and our customers.

Empire National Bank helps Ramp Motors stay ahead of the curve. "Our business operates in the fast lane," said Wayne Rampone Jr., Vice President at Ramp Motors. "We needed a bank where decision makers are accessible and can get things done in a hurry. That's why we chose Empire." Read all about it at empirenb.com/testimonials. Or call Port Jeff Station Branch Manager Edy Meyer at 631.928.4444.



Empire National Bank
 Built for business...yours.

ISLANDIA | MANHATTAN | MINEOLA | PORT JEFF STATION | SHRLEY