RSM McGladrey
Accounting | Tax | Business Consulting

white paper

The Threat Within: Employee Fraud Detection and Prevention

A recent survey conducted by the Association of Certified Fraud Examiners suggests that businesses have more reason than ever to be concerned about fraud. But it also suggests that causes can be understood, behaviors identified and actions taken to effectively address this serious problem.

Last year, fraud cost American businesses $994 billion – excluding Madoff's historic crimes. That amounts to seven percent of all revenues.

As disturbing as those aggregates are, they do not fully convey the impact to a business from an incident. Many businesses never recover from the damage. More than 60 percent of schemes cost their organization more than $100,000 per occurrence. Given these figures, it is not surprising that employee theft causes more bankruptcies than other crime.

Fraud prevention is of special interest to privately held businesses. Small and medium entities are especially vulnerable. They suffer larger losses on a per incident basis than the largest of organizations. And, because equity can be wiped out before lender interests and unsecured debt, equity interests are the most exposed stakeholders.

A deepening problem

Unfortunately, the problem is getting worse. During the past year, both the number of fraud incidents and the dollar value of fraud increased dramatically, with 55.4 percent of respondents reporting increased fraud in the past twelve months.

The economy has driven much of the growth. "Increased pressure" is cited as by far the biggest factor contributing to fraud. At 49.1 percent, it is comfortably ahead of increased opportunity (27.9 percent) and more than twice the rate of "rationalized" acts by the perpetrators (23.7 percent).

As in prior downturns, the problem is expected to worsen. More than 80 percent of respondents indicated that they expect the incidence of fraud to increase. Thirty-six percent expect it to increase significantly.

The greatest emerging source of fraud is employee embezzlement which accounted for a disturbing 48.3 percent of last year's increase. Internally generated fraud — e.g. corruption, financial statement fraud, and embezzlement — are also expected to continue to grow substantially.

Unfortunately, the poor economy is increasing the pressure to commit fraud in two ways. In addition to placing more personal economic pressures on employees, layoffs are depleting internal control systems. Nearly 60 percent of CFEs who work as in-house fraud examiners reported their companies had layoffs in the past year. Among those who had layoffs, almost 35 percent of companies had eliminated some internal controls.

An equal opportunity challenge

No industry is immune, with banking/financial services and government/public administration experiencing the most frequently and telecommunications organizations suffering the greatest average losses.

The threats come from all parts of the company. Accountants, because of their expertise and proximity to financial records, commit the highest percentage of frauds at 26.9 percent of all cases. Legal employees inflict the most damage per incident, with median costs per incident reported to be $1,100,000.

Executives/upper management rank second in both percent of incidents (17.8 percent) and median impact per incident at $853,000.

The front-line employee skimming from the cash drawer constitutes a relatively minor part of the total fraud picture. While customer service was fifth in number of cases, they were last in average incident impact at $45,000. Cash register disbursements account for less than 3 percent of all incidents.

To illustrate is the breadth of exposure to potential employee fraud, consider that while research and development employees perpetrated only seven frauds, those incidents averaged $562,000 each. Internal audit employees committed six frauds.

Fraud occurs in three major ways, with offenses falling into three categories:

- Corruption: using influence to procure a benefit contrary to one's duty to one's employer – e.g., conflicts of interest, bribery, illegal gratuities and economic extortion. Corruption accounts for 26.9% of reported cases.
- Fraudulent statements: the falsification of financial statements, which can take both financial forms (e.g., understating revenue) and non-financial ones (e.g., falsifying credentials). Fraudulent statements, cash larceny, and payroll schemes account for approximately 10% of incident each. Fraudulent statements expose businesses to the greatest risk. The median loss is a stunning $2 million, more than four times the median loss associated with corruption.
- Asset misappropriation: the theft or misuse of a company's assets. Asset misappropriation takes the most forms, including cash and non-cash versions of larceny and skimming as well as fraudulent cash disbursements.

Frauds happen over significant periods of time, and they are usually exposed by accident or by a tip. Check tampering and financial statement fraud last an average of thirty months. By contrast, cash on hand fraud typically last seventeen months.

Employees are by far the biggest sources of tips at 57.7 percent. Internal measures – controls and audits – currently less catch a small percentage of fraud, although internal controls do catch 23.3 percent of all fraud. They are less successful at catching schemes over $1 million. But the evidence suggests that internal controls are underemployed rather than ineffective.

The warning signs

To defeat efforts at fraud, it helps to understand who commits fraud and why.

The average perpetrator is a male rank-and-file employee who is acting alone. He typically has a high school education or less. And while you will always want to do background checks, most perpetrators have not been charged with, or convicted of, a crime. But, this is only a broad composite. All employees are capable of inflicting fraud.

Just as significantly, the perpetrator has a motive. They may feel dissatisfied or unfairly treated. They may be experiencing personal financial pressures or other situational pressures. Or they may simply want the notoriety of pulling off a successful theft. Whatever their motive, they will want to be able to rationalize their act.

In addition to motive, the perpetrator usually has an identifiable opportunity. They may perceive a lack of internal controls. They may have concentrated power and authority, so they cannot be easily checked. They may also sense that there are no consequences to their behavior.

Fortunately, there are signs which can be observed, if one knows what to look for. Take a close look at your daily business practices for:

- Irregularities in bidding processes
- Changes in business practices
- Invoices for unspecified consulting or other poorly defined services
- Vendor anomalies
- Erratic documentation and record keeping
- Checks made out to “cash” that are greater than petty cash allotments
- Missing checks/check numbers out of sequence

Failure to segregate responsibilities also helps create an environment where fraud can occur. Ask yourself, are the functions below being improperly segregated?

- Authorization of transactions
- Execution of operations
- Custody of assets
- Recording keeping of transactions

Review your internal controls. Check these processes for proper checks and oversight:

- Cash receipts and disbursements
- Accounts receivable and sales
- Inventory and cost of sales
- Accounts payable, other liabilities and purchases
- Payroll

Finally, look at your employees and your HR practices:

- Is an employee living well beyond his means?
- Are employees permitted to take home confidential documents?
- Are employees required to sign a non-disclosure agreement?
- Is your company contracting with companies owned or controlled by an employee?

What you can do

Not surprisingly, 77.6 percent of organizations modify their controls after discovery of fraud. And 56 percent of those changes focus on management reviews and expanded internal controls. These include:

- Surprise audits
- Fraud training for executives and employees
- Job rotation
- Improved anti-fraud policies
- Internal audit procedures
- Codes of conduct
- External audits and procedures
- Fraud hotlines
- Employee rewards for whistleblowers and other support programs

Of the various measures being taken, audits are the most popular. When internal audits/fraud exams are conducted, the average loss drops from $153,000 to $87,500. Among cases involving a loss of $1 million or more, external audits accounted for 16 percent of the detection methods versus 9 percent for all other means. Surprise audits are particularly effective. They account for a 66.2 percent reduction in median losses. These audits further help to convey a culture of responsibility, honesty and responsiveness by the organization. This is crucial since 46 percent of all fraud cases are detected by tips from loyal employees.

Background checks can also yield significant savings. When used, the average loss drops from $130,000 to $90,000. Checks should include criminal record, professional license, previous employment, credit report and education.

When one remembers that fraud is often committed by dissatisfied employees, it follows that measures designed to reduce dissatisfaction may reduce fraud. You can reinforce a "culture of integrity" by ensuring that you are paying employees a competitive wage, fostering honesty, providing a forum for employee input and responding to that input, and having plans in place for terminated employees.

If fraud is committed, proper checks will help ensure that it is caught. In addition to the audits discussed above, these measures include:

- Creating a fraud reporting system
- Matching expenses to travel itineraries
- Rotating employee duties
- Requiring employees to take vacation
- Assigning and limiting employee access to accounts, records and databases as needed for the position

Insist on specific expenses and facilitate fraud reporting. And don't allow company positions to become personal fiefdoms.

Tangible and tactical suggestions

Of course, there are a number of specific ways in which fraud can be thwarted. Many of them provide additional ways to break up closed-off silos or encourage specific reporting.

To protect cash and cash receipts, have checks mailed by someone other than the preparer after signing, have bank statements delivered to the owner unopened and have the bank accounts reconciled by someone independent of the cash receipts and disbursement functions.

To protect inventory and minimize your cost of sales, periodically count cost and compare inventory to control accounts and/or perpetual records. Pre-number documents and account for the sequence when you develop forms for purchase orders, receiving, inventory transfers and shipping. You will also want to take some very concrete actions: Store expensive components, products or tools in a locked closet. Designate a single exit door for your employees. And, of course, check the trash.

Segregated functions and specific purchases are your best strategies on the expense side. Separate requisitioning, purchasing and receiving functions from invoice processing, accounts payable, cash receipts and disbursements, and general ledger functions. Develop an approved vendor list to discourage under-the-table arrangements and shell vendors.

In conclusion

The bad news is that fraud is a growing problem. But the good news is that it doesn't have to be. Look for dissatisfaction, encourage a culture of honesty, minimize opportunity and initiate controls. Do these things and you can minimize the effect of this drain on your equity.

For more information, please contact
RSM McGladrey at 617.279.2800.