McGovern & Greene, LLP
Certified Public Accountants & Consultants

fraud alert

august/september 2006

Out of control
Management overrides can thwart fraud prevention measures

Don't let fraud cut into your online profits

Ghost employees and other specters could be haunting your payroll

Boomers poised to go bust?
More fraud targeting retirees expected

Fraud to watch for:
Student banking scams

McGOVERN & GREENE LLP
Certified Public Accountants & Consultants

105 W. Madison Street, Suite 406
Chicago, Illinois 60602

Out of control

Management overrides can thwart fraud prevention measures

A company may have strong fraud prevention controls in place, but what happens when senior managers override those controls? The American Institute of Certified Public Accountants calls management override the Achilles' heel of fraud prevention — one that can effectively undermine even the best-designed fraud prevention system.

In the worst cases, senior managers may alter records, manipulate financial results, intentionally misstate the timing of transactions or use any of dozens of other tactics to hide financial problems — simply by overriding the financial controls they helped to design and implement.

When something isn't right

Management override of financial controls can be difficult to detect. Often, however, these types of manager activities send off subtle warning signals:

- Frequent disputes with auditors on accounting or reporting matters,
- Failure to identify business risks in a timely manner,
- Failure to correct known reportable conditions in a timely manner,
- Unwillingness to discuss issues that could require financial adjustments,
- Lackluster enforcement or support of company antifraud controls, and
- Overly optimistic reports and analyses regarding the company's current or future performance.

These and other behaviors, including attempts to justify suspected accounting irregularities, don't always mean fraud is occurring. They do, however, at minimum indicate that you need to improve or open new paths of communication and remain vigilant, even when working with employees you've known for years.

Hard though it may be to envision any of your senior management team as a fraudster, the reality is that most people who commit fraud aren't career criminals. They're employees who may have been above reproach before they launched their fraudulent activities. So you must be willing to investigate evidence of fraud if it surfaces — regardless of whom it implicates.

Fostering a healthy business culture

Another protective undertaking is to build a business culture that encourages honesty and supports employees who speak up when they suspect something's wrong. Employees a level or two below senior managers are those most likely to observe management overrides that could indicate fraud is occurring.

Giving them a confidential mechanism with which to communicate those concerns increases the likelihood fraud will be exposed before it seriously harms your business. And if you extend hotlines or other reporting mechanisms to vendors and customers, you'll increase your chances for learning of improprieties early.

As you're examining the ethical health of your company, also consider whether your business places demands on senior managers that unwittingly encourage fraud. If your industry has seen increased business failures, for example, your senior managers may feel they're under additional pressure to keep your profits at specified levels. They might also feel stressed if their compensation depends in large part on achieving stretch goals for cash flow or operating results — either for the company as a whole or within their areas of influence.

Talking with business unit leaders may give you insights into the level of risk you face. If these

leaders feel that senior managers are under pressure to meet financial targets — or worse, if any of them has been asked to participate in questionable actions related to such targets — you'll want to know about it sooner rather than later. Such conversations may also reveal any pressures the business unit leaders themselves feel from senior management — pressures that may make them more prone to fraud, as well.

Internal and external auditors

Information available through internal auditors and external consultants and advisors can also help you identify areas of risk for management override of financial controls. You may find it beneficial to meet periodically with them, to discuss fraud risks.

This can help increase your chances of identifying potentially dangerous gaps in controls and procedures. In addition, inconsistencies in the data that auditors, consultants and advisors collect may be the first sign that one of your managers is committing fraudulent acts.

Of course, to recognize fraud, you must first understand your business's financial reports. Not every variance is due to fraud. There may be legitimate reasons, for example, for a senior manager to postpone planned transactions or delay expenses if the company isn't meeting its earnings goals. Internal and external auditors can help identify when financial reports reflect legitimate adjustments and when a changing or unexpected pattern of transactions should serve as a warning signal.

Where the fraud is

How are senior managers most likely to override internal financial controls? According to the American Institute of Certified Public Accountants, revenue recognition is virtually always a risk for fraud. Fictitious or premature revenue recognition may result when a manager hides or falsifies true contract terms. Managers may also overstate assets or understate expenses by failing to recognize asset impairments or loan losses or to accrue liabilities.

Sales activities can also harbor any number of distortions. If true contract terms are hidden or falsified, managers may be involved with side agreements or fictitious shipping plans, altered cancellation or refund provisions, or recorded sales that actually were canceled.

Due vigilance required

The risk of management override of internal controls to distort financial performance is real for any organization. Market shifts, aggressive performance targets, industry uncertainties, personal financial stress and a host of other factors may enter into a senior manager's decision to undertake fraudulent activities. You probably can't change those drivers, but you can maintain vigilance over your business. In fact, it's a necessity.

Don't let fraud cut into your online profits

These days it's almost impossible for your business to stay competitive unless you accept online orders. But how can you protect yourself from the credit card fraud that accompanies them? According to the 7th Annual Online Fraud Report by CyberSource Corp., some methods are more successful than others at thwarting online fraud.

Losses significant

American businesses lost an estimated $2.8 billion in online revenue to fraud in 2005, the survey reported. And smaller companies experienced higher rates of online fraud than did medium or large companies, but the smaller companies' rates of loss declined last year, while medium and large companies saw increased rates.

Direct revenue loss due to fraud has been less than 2% of online revenue each year, but hidden costs such as time spent verifying customer information or the loss of legitimate orders that are rejected push totals higher. Clearly, there is good reason to implement fraud protection measures if you engage

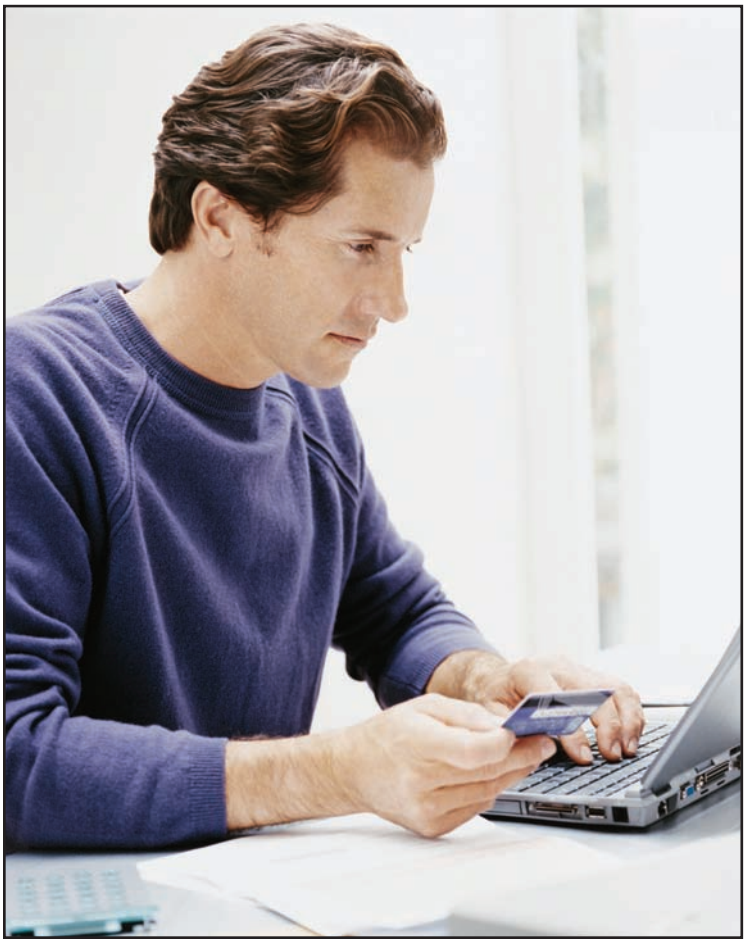
in online sales, but you need to stop short of becoming so cautious that you drive business away.

Protective measures

The CyberSource survey noted that most businesses use three or more protective measures to help thwart online fraud, and 70% agree that such tools help keep it to a minimum. These are the most popular:

Address verification system (AVS). Rated as the most effective deterrent to online fraud in a Worldwide E-Commerce Fraud Prevention Network survey released in April, AVS compares data from cards used for Internet purchases with information on file from the banks that issue the cards. While the scrutiny is effective in detecting improper use of cards, it also is subject to "false positives," in which legitimate transactions are denied, and to approving cards that should be rejected. The inaccuracies may be due in part to outdated or incomplete bank records, but they also underscore that technology isn't perfect. This is why most businesses use more than one tool.

Real-time authorizations. These systems approve credit cards when the numbers are submitted, so you aren't exposed to the risk that accompanies a turnaround time of hours or days. They can't, however, determine whether the person submitting the card is the authorized user, which is why many businesses turn to customer follow-up or card verification numbers for additional security.



American businesses lost an estimated $2.8 billion in online revenue to fraud in 2005.

Customer follow-up. Some businesses randomly sample customers to verify orders. In addition to helping to identify fraud, such calls are opportunities for businesses to get direct feedback on products and services. Calls are time-consuming, though, and many businesses say they're not as effective as some other fraud-control efforts.

Card verification codes. These three- or four-digit numbers are on either the back or front of every credit card to help ensure customers have the card in their hands when they place an order. The numbers aren't shown on receipts or credit card statements, making them somewhat more secure than card numbers. Still, fraudsters can obtain verification codes the same ways they obtain many credit card numbers — by stealing the cards.

According to the CyberSource survey, these and other measures are adding new levels of protection for e-commerce. It also mentions two other measures that are likely to be the most widely adopted tools in the near future: 1) Card association payor services, in which card issuers such as Visa and MasterCard authenticate card usage, helping not only to deter fraud, but also to shift liability for fraud back to the card-issuing bank, and 2) Automated order screening programs, which evaluate orders in real time, using each business's rules to detect probable fraud.

Plan to succeed

As more businesses rely on online sales to bolster their bottom lines, it becomes more important than ever for them to have fraud protection in place. Make sure you plan your fraud controls as carefully as you plan your ordering system.

Ghost employees and other specters could be haunting your payroll

Justin could have been a good employee. For the salary he was earning, he certainly should have been. The only problem was that he didn't exist. Justin was a figment of John's imagination. John, a trusted long-term employee, had a carefully concealed gambling problem that was getting him deeper and deeper in debt. Enter Justin.

Recognizing that his company's payroll controls were loose enough to be exploited, John invented Justin and opened a bank account in Justin's name. Then he put Justin on the payroll, arranged for direct deposit of paychecks into Justin's account, and used the fruits of Justin's "labor" to ease his own financial troubles.

John and Justin are *both* fictitious, but they have all-too-real counterparts in businesses throughout the country. "Ghost" employees go unnoticed in many companies because the businesses trust their employees too much and have inadequate or nonexistent internal controls to protect their payroll systems.

Small businesses vulnerable

Although it may seem like it would be easier to hide ghost employees in large firms, it's actually easier to hide them in small businesses where a single employee may handle all the payroll accounting. In some cases, a fraudster enlists a friend or relative to forge endorsements or deposit checks; in others, no assistance is necessary. He or she simply exploits weaknesses in the payroll system.

But ghost employees are just one way in which creative employees can manipulate the payroll system. Perhaps the easiest scam to perpetrate is to overpay withholding or payroll taxes. The government sends a refund to the business, and the employee deposits it in an account in his or her name. Other methods of defrauding your payroll system include falsifying hours or salaries; increasing commission rates or exaggerating sales; and filing false workers' compensation claims.

Follow the tracks

The good news is that, regardless of how ingeniously payroll fraud is arranged, it's likely to leave some tracks you can follow. These include:

- Paychecks with no tax or Social Security deductions,
- Dual endorsements on paychecks,
- Duplicate names, addresses or Social Security numbers in payroll records,
- Higher-than-budgeted payroll expenses, and
- Unusual spikes in the number of payroll checks presented for payment.

While there may be legitimate reasons for any or all of the above, it's always wise to investigate suspicions. And if you don't already, segregate payroll duties. If one employee writes checks, reconciles statements, keeps the books and distributes payroll checks, that employee may be tempted by fraud — particularly if he or she feels overworked or underpaid.

You might also consider outsourcing your payroll process completely. If that's not practical, make sure your computer system is secure and that all records are password-protected and access-limited. Encourage direct deposit to mitigate the opportunities for check-related fraud, and occasionally hand-deliver payroll checks to employees who don't have direct deposit. If you have any left, be sure they're for real people, and not imaginary employees such as Justin.

Take control

Payroll fraud can be easy to initiate, but it may also be easier than you think to prevent and detect. You just need to take control.

Boomers poised to go bust?

More fraud targeting retirees expected

According to the U.S. Administration on Aging, people over 50 control 70% of the nation's wealth, and research firm Cerulli Associates estimates that baby boomers will inherit at least $7 trillion from their parents in the next 40 years. Boomers already hold $8.5 trillion in investable assets, and they'll be looking for places to put those assets when they're ready to retire. As they move into retirement, though, their combination of age and wealth will make them increasingly attractive targets for fraudsters.

Shady estate planning services, promissory notes, unregistered securities, lottery scams and a host of other schemes aimed at seniors are likely to proliferate as boomers age. Consumer Action, a consumer advocacy group, estimates that, although people over 60 represent 15% of the population, they're the victims of 30% of fraud. Embarrassment may make baby boomers accustomed to seeing themselves as savvy and successful less likely to report fraud, meaning the percentages could creep higher in coming decades.

Age + money = scams

Financial seminars geared toward seniors are already surging, and the first of the baby boom generation has only just turned 60. Most often, these seminars are legitimate, but they can be hunting grounds for fraud. Disreputable insurance agents have been found to sponsor seminars to dupe seniors into liquidating their assets and buying inappropriate annuities. These questionable products are expensive and carry stiff penalties for withdrawing money before surrender periods of up to 15 years have expired — longer than people 60 or 70 years old typically can afford to wait.

Help for consumers

Consumer advocates are preparing for a wave of senior-related crime, or what Barry Minkow, a reformed con man who now is co-founder and executive for the Fraud Discovery Institute in San Diego, calls a "perfect storm" environment of age, assets and concern over weakened stock market returns.

Legislators, too, are taking a closer look at how to protect seniors from fraud. Last year, California's general assembly passed a law, effective Jan. 1, 2007, that requires financial institution employees to report suspicions of elderly exploitation — in much the same way doctors are required to

report gunshot wounds. About 20 other states have similar legislation in place to protect seniors.

At the federal level, versions of the Elder Justice Act were introduced in both the House and Senate last year. Both have been referred to committees. The Securities and Exchange Commission, however, isn't waiting for legislation. Regulators have launched new initiatives aimed at preventing financial seminar fraud against seniors, and promises swift action against those who attempt to perpetrate such schemes.

Shady estate planning services, promissory notes, unregistered securities and other schemes aimed at seniors are likely to proliferate as boomers age.

Successfully evading fraud

More legislation is likely to follow as this type of fraud gains wider recognition. In the meantime, boomers waiting in the wings to make triumphant entries into retirement need to be as meticulous in planning their finances as they are in planning their exotic travel.

Fraud to watch for:

Student banking scams

It's no secret that college students are perpetually short of cash. Fraudsters are taking advantage of that fact to recruit students into counterfeiting and check-kiting scams. As the school year approaches, bankers in particular should be certain their new account verification procedures are up-to-date and in force.

Lesson in temptation

Scams involving college students can take one of several forms, but they're typically aimed at out-of-town students and banks with multiple branches. In one ploy, organized fraud rings buy students' checks and ATM cards, and tell the students to report them as lost or stolen.

The fraudsters then write multiple bad checks on the accounts, allowing the students to believe, mistakenly, that they won't be held liable because they've reported the checks as missing.

Another scam has students opening multiple accounts at different branches of an interstate bank. In one Rhode Island case, the ringleaders asked students to deposit bad checks in accounts in one branch. The next day, they drove the students to different branches to withdraw as much as three times the amount on the worthless deposits before the bank caught on.

Educate employees

Banks can't and shouldn't decline new account applications simply because someone is — or claims to be — a college student. But they can make their employees aware of such scams and reiterate the importance of adhering to identification and verification procedures.

Accounts opened by students or self-employed people in their 20s, especially those opened via phone or Internet or with the minimum amount in cash, deserve heightened scrutiny. In addition to withholding ATM cards and check orders on all new accounts for a certain period, banks should identify and monitor high-risk accounts' activities daily.

Craig L. Greene, CFE, CPA

An internationally recognized public speaker, Craig has lectured on topics involving fraud and its detection to auditors, investigators and attorneys. He is a faculty member of the Association of Certified Fraud Examiners and Institute of Internal Auditors.

Craig works as a consultant and expert witness for major corporations, law firms, law enforcement and governmental agencies on cases involving allegations of fraud and misrepresentation. Craig is frequently quoted in major newspapers and publications throughout the U.S.

McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

Specialists in Fraud Examination and Litigation Services

If a business hasn't yet been a victim of fraud, it's been fortunate. According to the Association of Certified Fraud Examiners, fraud costs businesses in the United States billions of dollars every year. Small businesses are especially vulnerable because they often do not have controls in place to reduce the likelihood of fraud.

This is where McGovern & Greene LLP can help. Our firm specializes in helping corporations, attorneys, lenders, law enforcement and governmental agencies analyze financial records and contracts, identify and prevent fraud, recover and analyze evidence, and provide expert testimony in all of these matters. Our highly-experienced team of professionals includes certified fraud examiners and certified public accountants that are experts in the fields of fraud examination, forensic accounting, computer forensics, damage calculations, business valuations and audit services.

Our professionals can assist you in a wide range of matters, including:

- Fraud Examination
- Financial Investigations
- Forensic Accounting
- Asset Recovery
- Internal Audit Services
- Computer Forensics
- Training & Seminars
- Healthcare Audit
- Business Valuation
- Litigation Services
- Government Contracts
- Economic Damages
- Intellectual Property
- Contract Claims
- Construction Audits
- Electronic Discovery
- Profit Recovery
- Due Diligence

We welcome the opportunity to discuss your needs and answer any questions you might have about our fraud examination and litigation services.

Please contact us at 312.419.1961 or visit us at www.mcgoverngreene.com and let us know how we can be of assistance.

McGovern & Greene LLP
105 W. Madison Street, Suite 406
Chicago, Illinois 60602