

fraud alert

april/may 2006



An inside job

**Protecting computers
from employee attack**

**When disaster strikes,
don't let fraud deliver
a second blow**

**Promissory notes may
not be all they promise**

**Conduct a productive
fraud interview**

**Fraud to watch for:
Voicemail fraud**



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

An inside job

Protecting computers from employee attack

Much has been said about the dangers hackers pose to corporate e-mail accounts, Web sites and computer-based business applications. In response, many companies have taken steps to guard against external attacks. What they haven't done is establish sufficient protection against the greatest threat of computer fraud: insider abuse.

Employees should be required to change their passwords regularly to prevent other employees from accessing their computer.

Employees understand their jobsite computer systems. Therefore, they may be able to work around controls or take advantage of gaps in the system to establish phony accounts, siphon money from existing accounts, create phantom transactions or buy products for personal use. Those with grievances — real or imagined — can destroy data or infect corporate computer systems with viruses that can cripple internal and external operations.

Employee know-how

While it's impossible to eliminate all threat of internal computer fraud or abuse, companies can make it more difficult, thus discouraging employees from exploiting the system. In doing so, however, business owners must be careful not to implement so many layers of control that employees' ability to do their jobs effectively is compromised.

In fact, some of the most effective controls don't involve technology at all. Companies that reward their employees with adequate pay and

fringe benefits, meaningful work, job security and opportunities for promotion are less likely to find those employees engaging in fraud.

Equally important are management controls, operational reviews and a corporate culture that expects high-quality, ethical behavior from all employees. Clearly defined and regularly communicated corporate policies and priorities help establish such a culture.

Get technical

Of course, computer controls are also necessary. A thorough risk assessment helps identify areas of vulnerability — which differ from company to company. But general safeguards such as passwords, encryption of stored and transmitted data, internal firewalls, and authentication controls can keep unauthorized employees out of sensitive files, prevent viruses and hackers from entering the system, and protect information during transmission and in storage.

Employees should be required to change their passwords regularly to prevent other employees from accessing their computer. And, while remote access from home or a hotel may benefit salespeople and




executives, such access should be limited to those who genuinely need it. When would-be fraudsters can't easily access the files they need, they may not be willing to risk spending the time and effort it would take to find ways around the barriers.

In addition, it's important that small companies not rely solely on a computer-savvy employee for information technology services. Either hire or out-source trained IT staff who can monitor systems, update virus protection and security as patches and upgrades become available, adjust access as staff and responsibilities change, and troubleshoot technical problems without endangering other elements of the computer system.

Trained employees also are less likely to complicate matters should suspicion of fraud arise. Simply

turning on a computer can destroy or alter key information, and IT professionals can take the steps necessary to secure existing files before a suspect employee can alter them. IT staff also can make it impossible for employees to access a system after an investigation is underway.

Shore up interior walls

Information technology is critical in today's business environment, but it comes with its own set of risks for fraud. Business owners who focus on protecting their computer systems from outside attacks may be overlooking an even greater threat inside their walls. Taking some simple precautions to protect computers from internal no-gooders is just good business sense. 

When disaster strikes, don't let fraud deliver a second blow

Business owners whose facilities have been damaged or destroyed by a disaster are understandably eager to get their businesses up and running again as quickly as possible. Unfortunately, scam artists are only too willing to help.

Fraud has followed inevitably in the wake of the hurricanes, tsunamis, earthquakes and tornadoes that wreaked havoc worldwide in 2004 and 2005, as shady operators have offered inspection, repair and insurance services to distraught business- and homeowners. Fraudulent activity was so prevalent after Hurricane Katrina, in fact, that the federal government established a Hurricane Katrina Fraud Task Force to identify and prosecute perpetrators in the affected regions.

Caution speeds recovery

Much of the initial fraud stemming from Katrina involved invalid claims for the \$2,000-per-household immediate relief the government provided while suspending customary verification procedures. More insidious, however, have been the fly-by-night



contractors and fraudulent inspectors who've surfaced after disasters to take advantage of people who suspend their usual caution in the interest of getting back to normal as quickly as possible.

Too often, business owners find they've hired contractors who don't deliver as promised, can't be found for follow-up or are too inexperienced to do the job

properly. Some even encourage owners to participate in insurance scams. For those contractors, the goal is to make a fast buck rather than proper repairs.

When disaster strikes, it's important that business owners overcome their impatience long enough to ensure fraudsters don't deal them another blow. An unsolicited offer of quick repairs should be regarded as suspect. When it's accompanied by a "special discount" — pricing that's good for only a short time — or requires that the full amount be paid in advance, the offer is virtually guaranteed to be fraudulent. Reputable contractors won't require anyone to sign a contract on the spot, and their estimates will be valid for a reasonable period of time.

Guard against fraud

In the period immediately following a disaster, good contractors are likely to be in short supply. But you can find a reputable one and guard against becoming a fraud victim by following these steps:

Use only licensed contractors. Ask for the contractor's license number and verify it online or through the state's licensing board. Check for a certificate of insurance at the same time.

Get references. Ask the contractor for names of previous clients; then check that they do, in fact, exist and that the work the contractor did for them was satisfactory.



Ask around. Find out what friends, relatives, insurance agents, co-workers and others know about the contractor. Check with the Better Business Bureau (www.bbb.org) and National Association of Home Builders (www.nahb.org) to see if the contractor has been the subject of complaints.

Get it in writing. Ask for a written estimate that includes anything the contractor may have promised during consultations. In addition to pricing, the estimate should specify a reasonable time for completion, the scope of the work to be performed, the quality of materials to be used and any foreseeable conditions that could change the terms.

Contingency plans are essential

When you know a hurricane is on its way, you may have time to board up windows and retrieve crucial documents before the storm strikes. But that alone won't get you back in business when it blows over. And other disasters, such as fire, explosions and earthquakes, usually don't announce their imminent arrival.

The time to prepare for a disaster, therefore, is when nothing is looming. Consider not only how you'll replace windows and walls, but also how you'll restore processes and workflow if you're forced to relocate or data is lost. A business continuity plan will prepare you to cope with most catastrophes.

Consider hiring a consultant to help you identify risk and ways to mitigate it. One area in which you need to be particularly attentive is your vulnerability to fraud following a disaster. Work with information technology, financial and business experts to develop plans of action, backup networks and chains of command. Recognize that insurers, contractors (both building and IT) and other vital resources are likely to be overtaxed after a broad-scale disaster, and decide who will be responsible for coordinating each.

Don't sign anything immediately. Understand everything in the final contract, and ask legal counsel for clarification if necessary.

Don't pay in full too soon. Contractors customarily ask for partial payment before work begins to buy materials. But no contractor should ask to be paid in full — or request you to sign a certificate of completion — until the work is actually completed to your satisfaction.

Patience beats panic

Business owners can sometimes prepare for disasters, but they're unlikely to be able to avoid them. Those who remain cool-headed and exercise some patience, however, can avoid becoming victims of disaster fraud. ♪

Promissory notes may not be all they promise

When small companies need cash quickly, they may turn to short-term promissory notes as an alternative to more traditional financing arrangements. Promissory notes are essentially IOUs. Companies use them as short-term debt instruments, promising to pay the principal and fixed interest over periods ranging from 30 days to several years.

Legitimate promissory notes can be valuable both to businesses that need to raise money and to investors that buy the notes for relatively high rates of return. Fraud, however, has made this form of borrowing a risky business.

Signs of trouble

Promissory note fraud has several warning signs. Knowing them can keep borrowers and investors out of con artists' clutches. Beware of:

Short-term notes. Promissory notes for periods of less than nine months are exempt from federal securities registration — a loophole scam artists are quick to exploit. Unscrupulous operators can sell these notes without obtaining registered securities sales licenses (and without any of the protections such licenses offer investors).

Unregistered securities or sellers. Longer-term promissory notes are securities that must be registered and sold by licensed dealers, but fraudsters may sell the notes without registering them, so the sales aren't reviewed in advance by federal or state regulators.

Guaranteed or higher-than-normal investor returns. Returns on legitimate investments aren't guaranteed and should be at or near the current market rate for similar investment products. Unregistered, fraudulent sellers — typically hastily established "marketing" firms — may offer notes to investors with so-called guaranteed rates of return. Often, these guarantees are backed by fictitious foreign insurance companies.

Exorbitant commissions. Normal commissions usually don't exceed 30%. Shady firms offer significantly higher commissions to unwary insurance agents or investment brokers who recommend the


notes to their clients, unaware of the role they are playing in the scam.

Notes being sold widely to individual investors. Legitimate promissory notes are usually sold only to corporate or experienced individual investors. But fraudulent firms might sell the promissory notes much more widely, giving some of the proceeds to the borrowing company and another portion as commissions to the sellers, while leaving a large slice for themselves. Borrowers, therefore, may find themselves paying unnecessarily high interest rates and struggling with financial burdens they can't meet.



Companies considering borrowing with a promissory note and investors thinking about buying them can avoid problems by asking how the notes will be marketed, whether the marketing firm is a registered securities sales dealer and how the firm will pay investors. It's also a good idea to check with state insurance registration officials to be sure registration claims are valid.

Ask tough questions

Promissory notes can be legitimate options for investors and for businesses that need to borrow money quickly. With an increase in promissory note fraud, however, borrowers and investors alike should make sure they know the firms with which they're dealing — before any money changes hands. 

Conduct a productive fraud interview

It's never pleasant to realize that someone in your business may be defrauding you. But interviewing employees to confirm your suspicions can be even more disturbing — not to mention tricky.

Prepare for the pros

When you suspect an employee of fraud, you'll want to enlist the help of financial and legal advisors to handle the bulk of the investigation. Before they arrive, however, you may need to perform interviews to help resolve any doubts and obtain information before memories fade. If so, conduct them as soon as possible after an incident, but plan your approach carefully.



Before requesting any meetings, decide what information you're looking for. Not only will knowing what you want help you get to the truth of the matter quickly, but it also will enable you to avoid getting sidetracked by extraneous information. Then identify who is best able to supply that information, and how you can obtain it fairly, impartially and objectively.

If you suspect one of your accounts receivable staff of siphoning money, for example, you may want to

talk to that person's supervisor and a member of your IT department to get information on work habits, unusual behavior or signs of file tampering on one or more computers. Remember, though, that people may be reluctant to share information if they feel it reflects poorly on them or that they will be responsible for landing someone else in hot water.

Just the facts, please

When you're ready to start talking to employees, set the tone with some introductory questions and ask the interviewee to agree to cooperate with the interview. In most cases, you'll be looking for corroborative or exculpatory information, and interviews will be fact-finding in nature. The interview should last long enough for you to obtain all the information each person has to offer, but don't prolong sessions unnecessarily.

During the interview, make sure you're a good listener. You should:

- Appear interested in what the person is saying,
- Aim for an informal, relaxed conversation, and
- Remain professional, calm and nonthreatening.

Don't, on the other hand:

- Interrupt unnecessarily,
- Let the employee feel you have preconceived ideas about who did what and when, or
- Try to impress the employee with your knowledge or authority.

If you suspect someone is withholding relevant information, try asking more detailed questions. Remember to focus on what is said, rather than the way it is phrased or the attitude of the person providing the information. People are more willing to cooperate if they see you as unbiased.

At the same time, you don't want employees to believe they can get away with telling lies. If someone says something you believe is untrue, ask for clarification. You might suggest that your question was

misunderstood or that the employee didn't give it enough thought before answering. Then ask it again.

Finally, never make threats or promises to encourage someone to change a statement or confess to anything. If the case ends up in court, such tactics may make the evidence you collect inadmissible. If someone persists in lying to you, ask them to put their statement in writing and sign it. Then thank them

and turn the statement — and your suspicions — over to experienced fraud investigators.

Interview, don't interrogate

Finding evidence of fraud is bad enough. Turning interviews into interrogations will only make matters worse and could hinder your ability to properly pursue and punish fraud offenders. ¶



raud to watch for: Voicemail fraud

In a world of increasing exposure to technology-related security threats, it's nice to be able to rely on voicemail for risk-free communication. The problem is, you can't: Even a seemingly innocuous voicemail system can expose you to fraud if you don't take minimal precautions.

Passwords as passports

The most common voicemail fraud, often perpetrated in businesses with multiple phone lines and extensions, involves hackers who determine passwords for individual voicemail boxes. Most frequently, they call numbers until they're transferred to voicemail, and then try different combinations of numbers until they find one that works. Once they're in a voicemail box, they change the greeting to authorize collect or third-party calls.

In some cases, hackers use voicemail to enable lengthy, international conference calls. In others, they distribute the compromised phone numbers to friends and relatives overseas. These individuals can then call the United States, asking that the calls be billed to their "home" numbers. Because such calls are typically placed at times when voicemail is likely to pick up, the voicemail greeting authorizes the calls and the home or business owner is left holding a bill that can add up to thousands of dollars. Phone companies may or may not waive such charges.



Unauthorized calls aren't the only way in which unauthorized users can exploit voicemail. Anyone who gains access to passwords can use them to listen to messages. Thus, hackers can get unlimited access to confidential business information or employees may even use passwords to monitor their bosses' messages.

Prevention is essential

Simple precautions can prevent these fraudulent activities. The easiest is to make sure everyone in your business creates a unique password. Hackers know that many people either don't bother to change the default "1234" password or simply use their extension numbers as their passwords.

Changing voicemail passwords regularly, just as with computer and e-mail logons, is another way to discourage voicemail fraud. Even better, encourage your employees to use six-digit — instead of the more common four-digit — passwords. Hackers would have to try 100,000 combinations to hit on the right one. It's much easier for them to find default passwords somewhere else.

Another prevention method is to ask employees to routinely check their greetings. Smaller businesses may also want to disable unused auto-attendant, call-forwarding and out-paging voicemail capabilities to foil hackers.

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



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.

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.mcgovernngreene.com and let us know how we can be of assistance.

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

