fraud alert

february/march 2005

Worst case scenario

Fraud contingency plans are an unpleasant necessity

Change for what?

Train your employees to spot bogus bills

Alter ego companies tempt troubled business owners

New tools help fight online payment fraud

The perks and perils of workplace instant messaging

McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

Worst case scenario

Fraud contingency plans are an unpleasant necessity

You've spent considerable time getting your business ready to cope with any natural or man-made disaster — from fire, flood and earthquake to massive computer failure or even terrorist attack. If you haven't established a fraud contingency plan, however, you're not fully prepared for all the emergencies a business can face.

As the high-profile collapses of Enron and WorldCom have proved, fraud can cause as much damage to a company as any hurricane or hacker, both financially and in terms of your firm's good name.

Address urgent needs

A contingency plan works as a road map to help you minimize damages, protect evidence, maintain client relationships and even deal with media publicity during a highly stressful time. It sets objectives such as recovering losses, identifying and punishing the perpetrator, and deterring future fraud.

Equally important, a contingency plan addresses immediate needs such as ensuring that ongoing business is properly managed while an investigation is under way and outlining steps to rectify any loss the fraud has created. To catalog those losses, you need to take an immediate inventory of assets and evidence, which means you must retain an investigator promptly.

Hold your fire

An instinctive reaction to uncovering fraud is to fire the offender on the spot. That's understandable, but it's not necessarily a good idea in the early stages of an investigation.

If you're absolutely certain you know the suspected offender was responsible for the fraud, that the employee acted completely alone, that you know the full extent of the fraud and that you know where the proceeds are stashed and how to recover them, you may want to fire the perpetrator. If not, consider suspending the employee instead.

In either case, you want the suspect off the premises as quickly and quietly as possible, and need to take steps to ensure the employee isn't readmitted without your permission. Then start searching the suspect's office or workspace for evidence.

This is when your contingency plan must be very specific. While an initial examination of documents and personal papers may reveal certain ambiguities and irregularities, you must know when to call in outside help.

Forensic accountants and computer experts understand what proof is required for legal action. More important, they know how to extract that proof without destroying its evidentiary value. An inexpert review of computer files, for example, could damage user logs or file access data that might prove the suspect opened the incriminating records.

Likewise, an expert can add value to the process of interviewing the suspected perpetrator. Not only can an expert craft questions and understand technical obfuscations that you may miss, but having an expert conduct the interview can help establish its validity in court.

Control the leaks

You must also consider publicity when developing a fraud contingency plan. Eventually, you may want to give the evidence you've assembled to the police for potential criminal prosecution. While the police don't necessarily publicize all of their investigations, they may have no choice but to release some information if there is considerable media interest in your case.

If you've already determined a media strategy — preferably working with your forensic accounting experts — you'll be able to decide what information should be released and then be ready to immediately deflect criticism and help preserve the company's good name. You may not be able to prevent some information from getting out, but you can make sure it's your message that the public is hearing, rather than rumor or misinformation.

How to conduct a fraud interview

At some point during a fraud investigation, you'll probably want to question witnesses or suspects, either alone or accompanied by an experienced investigator.

Before you start, decide what information is relevant to your investigation and what is simply distracting. This requires you to study the case file, both to remind yourself of the main issues and to be sure nothing important has been overlooked.

While questioning a suspect, keep in mind what you're trying to learn, but don't close the door on potentially relevant information of which you may not be aware. Also keep in mind that a nonaggressive, nonthreatening tone and demeanor will do more to loosen tongues than an "in-your-face" attitude.

Ask different types of questions (open, closed, leading) in a variety of ways and work hard to avoid giving the impression that you're simply attempting to verify a foregone conclusion.

You'll get more information and maintain more goodwill if you can remain nonaccusatory, professional and calm throughout the interview process — regardless of how angry or biased you may feel on the inside.

Like any contingency plan, a fraud contingency plan must receive a stamp of approval from the upper levels of your company — including the board of directors. It must clearly delineate actions to be taken, establish limits on the internal investigation team, and identify how and when outside investigators, including police, will be called in. It also must be flexible enough to adjust quickly to unforeseen circumstances.

In some cases, the fraud you uncover may seem too minor to fully mobilize the contingency plan. But you never know when a small incident will turn out to be the tip of the iceberg. Even if it is minor, putting the contingency plan into action helps assure that you use your best practices to address it and you avoid mistakes you later regret.

Let cool heads prevail

Corporate fraud has wide-ranging ramifications for any company. When it is revealed, emotions run high, especially because much corporate fraud is committed by employees of long standing and high regard. Crafting a fraud contingency plan when heads are cool can be enormously helpful when fraud rears its ugly head.

Change for what?

Train your employees to spot bogus bills

Last summer, when a store clerk in Pennsylvania accepted a $200 bill that can best be described as goofy, many wondered how anyone could be that stupid. For business owners, however, a better question might be, "Could this happen to me?"

Admittedly, the Pennsylvania case was a little extreme. A woman paid for merchandise with a $200 bill with a picture of President George W. Bush on the front and an image of the White House fronted by placards such as "We Like Broccoli" on the back.

There is, of course, no such thing as a $200 bill in the United States — regardless of whose picture is on it — and there is certainly no bill of any denomination featuring a sign-studded White House lawn.

But with the increasing sophistication of personal computers, and scanning and copying software, counterfeiters can create real-looking but bogus currency with relative ease. And most of it isn't as simple to spot as a $200 bill.

Technology aids prevention

A consortium of 27 central banks in the United States, Canada, Japan and Europe has, with the full cooperation of the U.S. government, established the Central Bank Counterfeit Deterrence Group to

make it more difficult for counterfeiters to produce and use counterfeit currency.

One of the more technologically advanced methods the group uses is anticounterfeiting software that won't let users scan or print copies of the new $20 and $50 bills. Known as the Counterfeit Deterrence System, the technology is being kept secret and officials won't say which hardware and software companies' products carry it.

Spotting fakes

The U.S. Secret Service notes, however, that today's counterfeiters can produce computer-generated currency with basic computer training and some trial-and-error techniques. The high-resolution color reproductions they create could fool a tired or inexperienced employee.

While few reproductions will get past a bank or the Federal Reserve, most monetary transactions don't involve either. Instead, your first line of defense must be your employees.

If you haven't taught employees who handle cash how to spot a counterfeit bill, do so as soon as possible. If you have offered such training in the past, it may be wise to provide it again, both for new employees and as a refresher course for those who could benefit from the reminder.

The government has taken a number of steps to make it easier to differentiate between real and counterfeit currency, including embedding a vertical thread to the left of the Federal Reserve seal on all bills except the $1 bill. This thread, which cannot be duplicated by counterfeiters, is invisible until the bill is held up to a light.

Also, a watermark on each bill "shadows" the face of the person depicted on the bill. This watermark is also invisible until held up to a light.

On the other hand, signs of a fake include:

- Fuzzy, flat portraits rather than crisp, lifelike images,
- Blurred, indistinct margin lines and scrollwork,
- Serial numbers that aren't uniformly spaced or that aren't printed in the same ink color as that of the Treasury seal, and
- Tiny red and blue lines printed on the paper, rather than fibers embedded in it.

Another fairly common and frequently successful ploy used by counterfeiters is to glue numerals from a higher-denomination bill onto the corners of one of lesser value. For example, the counterfeiter would glue a "10" onto a $1 bill.

A quick comparison of the numbers in the corners and the denomination written across the bottom of the bill will expose this trick, but it's easy for the unwary to overlook.

Front-line defense

Counterfeiting isn't a new pursuit, and the Secret Service has made strides in containing it in recent years. Unfortunately, computers capable of producing realistic currency are easy to come by and many counterfeiters produce only small amounts of bogus bills — making perpetrators difficult to apprehend.

Your best defense, therefore, is a well-trained front line, staffed with people who know that if a bill looks wrong, it probably is.

Alter ego companies tempt troubled business owners

For some business owners, bankruptcy is simply not an option — even when it's the only option. Faced with impending financial collapse, some business-people instead set up alter ego companies that allow them to divert assets while hiding income and ownership from existing creditors.

This isn't a particularly novel approach to a problem; it's been used in organized crime, loan and bankruptcy fraud, and cases of marital dissolutions and stockholder disputes. But it can be difficult to prove that one company is really just a disguise for another.

Shams vs. legitimate companies

Alter ego companies are essentially sham subsidiaries set up by parent corporations with something to hide. Owners divert assets such as inventory and accounts receivable payments from the failing company into the alter ego company — and their own pockets — before the original company is forced out of business.

The first company may have virtually no financial worth, but the assets of the alter ego company are protected from bankruptcy proceedings by virtue of its seemingly separate operating status.

One problem in identifying fraudulent subsidiaries is that it is perfectly legal for corporations to limit risk by setting up separate, subordinate firms. Even if they are wholly owned, these companies function independently in terms of sales, billings, assets and management. Legitimate reasons for such companies include tax and profit-sharing advantages as well as liability limitations.

Legitimate subsidiaries, however, won't use their parent companies' letterhead or telephone numbers. Often, they won't share officers, directors or employees or work with the same attorneys and accountants.

The parent company won't pay most of the subsidiary's expenses. In many cases, the parent and subsidiary aren't even involved in the same business.

Asking the right questions

Of course, fraudulent companies aren't always easy to spot. They generally require financial experts to expose them and multiple pieces of evidence to support any legal action against them.

Key questions experts might ask include:

- Has there been a substantial reduction in sales at the original company? If so, have customers actually stopped buying or are they just being billed by the alter ego company?
- Have all accounts receivable payments been properly deposited in the original company's account?
- Have all shipments been recorded in the original company's log?
- Are the two companies' product lines identical?
- Does the original company dictate policies and procedures for the subsidiary?

Investigators also consider the number of "related-party" transactions between the companies. Related parties are those that either control or are controlled by a company, as well as officers, directors and their families.

In transactions involving an alter ego company, there may be special terms or conditions that help the original company redirect funds to the subsidiary.

Signs are subtle, not invisible

Alter ego companies, as opposed to legitimate subsidiaries, typically have one purpose: to help their owners perpetrate fraud. The signs may be subtle, but forensic accountants and other experts can expose these schemes and help creditors and others recover what's owed them.

New tools help fight online payment fraud

Online sales are a virtual necessity for most businesses. Not only do customers demand the 24-hour convenience of shopping from their homes, but an Internet presence immeasurably expands market reach.

The problem is that identity theft, phishing (using fake e-mails to obtain personal financial information) and other types of Internet-based scams are damaging not only to the consumers they target, but also to the businesses that unwittingly sell to fraudsters.

Costly and time-consuming

According to the fifth annual CyberSource Fraud Survey, merchants lost 1.7% of their revenue to online fraud in 2003. The good news: That figure is down from 2.9% the previous year. The bad news: Implementing antifraud measures to realize any reduction in fraud is still costly and time-consuming for most companies.

Your company may be one of the many firms, for example, that now conduct manual checks on up to 25% of their online orders by contacting customers to validate information.

The proliferation of fraud on the Internet means consumers will need to be more patient and businesses more vigilant.

While that practice can be somewhat effective in stopping fraud, it raises personnel costs and is far from foolproof. Not only do bogus orders get through, but legitimate orders may be rejected — resulting in a loss of customer goodwill.

Fighting the techno-fight

More and more companies, therefore, are using automation to fight online scammers. The Worldwide E-Commerce Fraud Prevention Network, for instance, reported that 70% of respondents to its March 2004 poll use address verification systems (AVS).

An AVS compares the house number and ZIP code provided for the online order with those on file with the bank that issued the credit card. If they don't match, the business is notified and can decline the order or seek more information from the customer.

More verification required

Companies also are increasingly asking customers to provide the card verification numbers from the backs of their credit cards or requiring passwords during the checkout process.

Some companies have stopped accepting orders from free e-mail sites, requiring instead that all orders originate with Internet service provider or domain-based e-mail addresses that make it possible to track users when fraud is suspected.

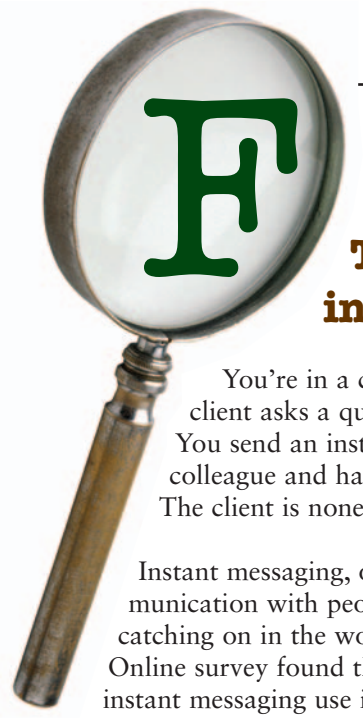
Unfortunately, this practice eliminates potential customers who don't own computers and use public computers, such as those available in libraries, to complete online transactions. But if your business is losing thousands of dollars each year to online fraud, the benefit may outweigh the cost.

In the end, you stand to lose more than customers when identity theft or stolen credit cards enter the online picture. Consumers are liable for only $50 for all fraudulent charges on their cards; merchants, on the other hand, are hit with chargebacks for every fraudulent purchase.

The Worldwide survey found that 50% of businesses responding lost between $1,000 and $10,000 to online fraud, while 19% experienced losses of more than $100,000.

Safety for all

Online sales can be a blessing to both businesses and consumers. But the proliferation of fraud on the Internet means consumers will need to be more patient and businesses more vigilant, to make sure those sales are legitimate and safe for all concerned.



Fraud to watch for:

The perks and perils of workplace instant messaging

You're in a conference call when a client asks a question you can't answer. You send an instant message (IM) to a colleague and have the answer in seconds. The client is none the wiser.

Instant messaging, or real-time online communication with people on a "buddy" list, is catching on in the workplace. A 2004 America Online survey found that 27% of those who use instant messaging use it at work — up 71% from 2003.

E-mail remains more popular than instant messaging for the time being, but two recent Pew Internet & American Life Project surveys showed that more than 53 million American adults use instant messaging and 11 million of them use it at work.

Popular but vulnerable

IM's popularity is understandable: It can save time, improve teamwork and even offer moments of relief from the daily grind. On the other hand, IM interruptions can be distracting and constant communication can turn into time-wasting gossip.

Also, like any Internet-enabled program, IM is vulnerable to outside attack. Most free IM software was developed for scalability rather than security, and there is nothing to prevent someone from sending messages — perhaps with a screen name that is similar to that of the company president — to everyone on purloined buddy lists.

Take action now

Personal firewalls and antivirus software on all computers and handheld (PDA) devices can help mitigate the risk, but you also need to have clearly established rules and best practices in place.

You can help prevent hacker attacks by doing the following:

- Keep IM and antivirus software up to date.
- Let employees know that hackers can intercept messages or use IM to spread worms and viruses.
- Have employees separate their personal and business buddy lists.
- Make sure employees understand appropriate uses of IM at work.

Instant messaging appears to be poised for explosion in the near future. Take steps now to close the door on potential abuse before hackers realize it's open.

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