# fraud alert

june/july 2005

## Nothing personal
**Corporate identity thieves aim for bigger targets**

## Find the smoking gun
**Forensic experts uncover evidence to bolster fraud cases**

**Corporate espionage: Is there a spy in your loop?**

**Why smaller companies are more vulnerable to embezzlement**

**Fraud to watch for: Disaster scams**


McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

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

# Nothing personal

## Corporate identity thieves aim for bigger targets

Identity theft has gained notoriety in recent years, with frequent media reports about scammers using stolen credit card numbers and other personal information to establish false accounts. While you're guarding your personal identity, though, you should also be on the lookout for corporate identity thieves.

### Varied approaches

This growing group of fraudsters uses a number of approaches to adopt the identities of legitimate businesses and perpetrate a variety of scams. In one widely published case, the International Chamber of Commerce uncovered a global Internet banking scam that involved theft of nearly $4 billion.

In that case, the thieves set up 29 Web sites that looked like those of legitimate companies in the United States and Europe. They used the sites to sell fake securities and investments, directing victims to the sites to verify where their investments were going.

In other instances, hackers have exploited weaknesses in legitimate corporate Web sites to steal customer lists or sales databases, or to hijack e-mails — any or all of which may undermine the true company's business.

Although the Internet and wireless worlds are corporate identity thieves' favorite hunting grounds, they aren't the only opportunities for fraud. Fraudsters have been known to use stolen company names in newspaper ads offering to advance loans in return for "commitment fees." They have also used counterfeit checks with stolen corporate account numbers and hijacked corporate identities to create bogus payroll checks.

### Combating Internet schemes

Of course, the Internet is the most anonymous — and easiest — vehicle for corporate identity theft. There are ways to combat such schemes, however, and to protect your business and also retain customer loyalty and market confidence.

Take these proactive steps:

- Make it easy for your employees, customers and suppliers to report suspicious e-mails or Web sites. Set up an "early warning" program that allows them to forward potentially fraudulent materials before significant damage is done.
- Limit employee access to sensitive information such as personnel records.
- Encrypt all sensitive electronic information transfers, but remember that not all data requires top security. Be sure the security level matches the value of the information.
- Let your customers know that you will never ask them to share personal or financial information via e-mail, and make sure you have and enforce a strict policy that ensures it doesn't happen.
- Educate customers and suppliers about the dangers of clicking on links that arrive in unsolicited e-mails — even ones that appear legitimate. Let stakeholders know that it's all too easy for experienced spammers to create fraudulent e-mails so authentic that even experts may have difficulty seeing the difference.
- Have an easy-to-find Web site and suggest that customers and suppliers bookmark your address. Keep your site address simple, and promote it heavily in your advertising and marketing materials to limit the need for online searches.

Finally, pay attention to who else may be interested in using your domain name and monitor new registrations for any that include your name or trademark. You may even want to register names similar to yours — perhaps those with common typos or

misspellings of your name — so you can automatically redirect people to your correct address.

### Be prepared

Even if you've taken precautions, you may still become a victim of identity theft. Therefore, you need to decide how you'll respond in the event of an attack. Trade associations, law enforcement agencies and other parties often have committees or task forces that share best practices. Establishing relationships with these groups in advance may help smooth the way if and when you need their help.

Unfortunately, because many corporate identity thieves operate outside the United States, it's difficult for legal authorities to find them. Therefore, taking steps to combat fraudsters before they strike is a wise business decision you're unlikely to ever regret. Consulting a computer forensics expert, in particular, can help you identify internal weaknesses before identity thieves find and exploit them.

# Find the smoking gun

## Forensic experts uncover evidence to bolster fraud cases

Forensic evidence — financial data, correspondence and, increasingly, various types of electronic files — is the foundation upon which many fraud cases are built. Compiling information that can be used as evidence and help win a case can be challenging, though. Forensic accountants and other fraud experts can help.

### Initial investigation

When occupational fraud is suspected, fraud experts can support an initial investigation by helping businesses and attorneys figure out what went wrong, why, how and by whom. Forensic accountants might start by gathering relevant financial records and retrieving electronic files.

Details about possible misdeeds might also be collected through employee interviews, which many fraud experts are specially trained to conduct. These professionals typically start with the least suspicious individuals, gathering as many facts as possible before finally interviewing those who appear most culpable.

Based on their findings during this initial investigation, fraud experts will usually develop a theory about what has occurred. The possibilities might include asset misappropriation, corruption (for example, accepting bribes) and falsifying financial statements. Once they develop a fraud theory, experts can then help determine whether the investigation should move to litigation.

### Building a case

If the case appears strong enough to proceed to court, forensic accountants can assist attorneys during the discovery process. Fraud cases can be won or lost in the fact-finding phase of litigation, so it's essential to gather as much documentation about the other parties' facts and theories as possible. This is done through court-issued subpoenas and search warrants that require parties to produce case-related documents.

Obtaining evidence, however, can be the simple part; interpreting it is another matter. Documents such as ledgers, transaction records, bank statements and tax returns are complex and require financial expertise, which is where forensic accountants can be particularly helpful.

The assistance of computer forensic experts — who are skilled at constructing electronic evidence — may also be required. Today, the majority of forensic evidence is electronic, including word processing documents, customer databases, scheduling programs, operational logs, voicemail recordings and e-mail messages. But electronic

evidence is fragile and can be easily damaged or destroyed by improper handling and examination.

### Chain of custody

Forensic accountants maintain a chain of custody throughout the evidence-gathering process, meaning all evidence they receive and handle is properly recorded, inventoried and stored. This is important, because courts normally attach much greater credibility to evidence with a properly maintained chain of custody. In fact, a broken chain of custody can severely compromise a case.

Indeed, a meticulous approach to evidence gathering is necessary if you hope to achieve the best possible outcome for your fraud case. Engaging experienced forensic professionals who understand how and what must be gathered is an important step in this direction.

# Corporate espionage: Is there a spy in your loop?

The first thing you need to know about corporate espionage is that it can happen to you. In fact, some experts say the odds are good that it is happening to you. The next thing you should know is how to prevent it, and that's a little more complicated.

Corporate espionage (or economic or industrial espionage) is theft of a company's intellectual property or trade secrets, and it happens regularly in the United States. The problem was significant enough to prompt Congress to pass the Economic Espionage Act in 1996, making it a federal crime to steal trade secrets. Nevertheless, according to ASIS International (formerly the American Society for Industrial Security), it costs American businesses billions of dollars every year.

### Precautions justified

Some companies are so concerned about corporate espionage that they don't allow visitors to bring camera cell phones into their facilities unless the lenses are covered with plastic stickers. Their caution is probably justified: Companies have been known to deploy "business intelligence units" that use tactics from dumpster diving to bribery to gain inside information on their competitors. (Dumpster diving, or going through a company's trash, is legal; bribery is not.)

The greater danger for corporate espionage, however, is internal. Employees who have access to trade secrets may take the information with them when they leave — whether they quit or are fired. Or they may pad their paychecks by selling information to rivals while still employed.

Other employees may simply not realize they are passing along trade secrets. An engineer, for example, may be willing to help a "student" doing research on a particular electronic device, or an operations manager may participate in a "customer satisfaction survey" by a box manufacturer.

In the latter case, telling a competitor how many of certain size boxes your company used may be equivalent to releasing sales specifics. Even harder to prevent is the practice some companies have of sending "eavesdroppers" to listen to the

conversations at bars and restaurants where competitors' employees gather.

## Protection plan

Given the ingenuity of corporate spies, how can you protect yourself from theft of trade secrets? The first step is to identify what information should be guarded. Some of that is obvious and some isn't: New technology or market strategies are clearly sensitive, while customer complaint or component purchasing data may or may not be valuable to competitors.

As you determine what information needs to be protected, also look at whom it needs to be protected from. Which competitors would benefit from what information?

Next, determine how much of your sensitive information is at risk and where the vulnerabilities lie. In making your assessment, and a subsequent protection plan, don't be tempted to rely too heavily on technology. Passwords, firewalls and the like are important components of any security plan, but they aren't invulnerable.

Look at who has access to sensitive information and how your business processes drive the manner in which such information is used. Then develop a security policy that considers your business methods, potential external weaknesses and staffing patterns, as well as the need to protect vital information. Revisit the plan periodically as your business and competitors change.

Make your employees aware that the threat of corporate espionage exists and let them know how to report suspicious activity such as people asking for details about their jobs. Emphasize that secrets can be revealed inadvertently, and educate them on the importance of being aware of who may be overhearing their public conversations.

You also must clarify, however, that not all research into your company is illegal. Public documents such as Federal Communications Commission and regulatory filings, published articles on your firm, and other readily available documentation can give an experienced business analyst a fairly accurate idea of what you're doing. But actual corporate espionage involves theft of information that has not been made public, and that the public would have no reasonable method of obtaining.

### What to do if you become a victim

If you become the target of corporate espionage, there are several ways you can respond:

- Turn your evidence over to the FBI for criminal prosecution under the Economic Espionage Act. Individuals found in violation of the act face penalties of up to 15 years in prison and fines of up to $500,000. Companies caught buying trade secrets risk fines of as much as $10 million.
- Pursue civil action by filing a lawsuit seeking immediate return of and an injunction against use of the stolen material. If you choose legal action, there is no reason not to pursue both criminal and civil cases, even simultaneously.
- Realize the risk of legal action may outweigh the rewards. Legal actions are public, meaning your loss of information will be revealed. Publicity could damage confidence in your company, leaving shareholders, investment bankers and even potential employees wondering whether the damage is irreparable.

Once a trade secret has been stolen, some damage to your company has been done. You and your advisors will need to determine whether exposing that damage will do more harm.

*Companies have been known to deploy "business intelligence units" that use tactics from dumpster diving to bribery to gain inside information on their competitors.*

## Ignore at your peril

Corporate espionage is real, and it could easily happen to you. No company, regardless of size or industry, can afford to view security as optional. The cost of even the most elaborate security program is nothing compared to that of letting your competitors in on how you're staying ahead of them.

# Why smaller companies are more vulnerable to embezzlement

Theft is the illegal appropriation of money or property. But embezzlement takes theft one step further: It violates the trust placed in the embezzler by employers and co-workers. Most business owners and managers want to believe the employees they trust to handle accounting matters, inventory and other financially sensitive items are honest — and, for the most part, they are.

But studies suggest that greater caution is required. According to the Association of Certified Fraud Examiners, in 2004, U.S. businesses lost more than $600 billion to occupational fraud. And embezzlement and other forms of fraud occur in small businesses at a higher rate than in larger companies: Approximately 42% of fraud occurred in companies with fewer than 100 employees, whereas 30% occurred in public companies.

## Is your trust misplaced?

Two significant reasons for this disparity are a higher degree of trust and fewer internal controls in smaller companies — particularly family businesses. Generally employees in these organizations trust their co-workers to a greater extent than those in large ones. While this trust is often well-placed and may create a collegial atmosphere, it can also provide a breeding ground for embezzlement.

A higher level of trust means small businesses are less likely to implement internal controls such as background checks, anonymous hotlines and regular audits that are routine in larger companies and even required of publicly traded firms. The expense of providing these fraud-prevention mechanisms may also be a stumbling block for many small businesses.

## How can you prevent it?

Embezzlement is something of a catch-all term for many types of fraud. But it generally involves the misuse of a business's assets and can include making fraudulent disbursements, pilfering inventory or skimming revenues. While you don't want to turn your business into a police state or treat innocent employees like criminals, it's important to protect your business from these common schemes with a system of checks and balances.

The internal controls required by your business depend on the type and size of the company. A retail store, for example, might focus its efforts on protecting inventory with security cameras and by performing surprise inventory verifications. A manufacturing business with a large number of hourly workers might concentrate on preventing time card fraud with such tools as mechanical time stamp machines.

Regardless of your industry, however, doing the following can help reduce the incidence of embezzlement:

- Develop a fraud policy that outlines what actions you will take if an employee commits embezzlement.

- Run background checks on prospective employees, including screens for criminal records and financial problems.
- Perform regular cash reviews that reconcile receipts and disbursements.
- Regularly verify assets, including inventory and supplies.

Also segregate employee duties so, for example, the same individual doesn't handle both disbursements and revenues. If personnel limitations restrict your ability to segregate duties, consider outsourcing some of your business's functions, such as payroll processing and other accounting responsibilities.

### Are controls worth the cost?

Business owners and managers are sometimes wary of imposing internal controls because of the cost and time involved, and because they fear controls imply that they don't trust their employees. Internal controls not only help prevent embezzlement schemes, but also can create a more ethical work environment that honest employees will appreciate.

## Fraud to watch for:

### Disaster scams

It's horrifying enough to see televised reports of the effects of natural disasters such as the tsunami that struck Southeast Asia and the hurricanes that ravaged Florida in 2004. What makes these disasters even worse are the scams that arise in their aftermath.

Within days of the Asian tsunami several fraud schemes were active: fraudulent aid organizations, so-called Nigerian Scam letters claiming to be from homeless survivors or surviving relatives who needed donations or help transferring funds to their accounts, and an e-mailed plea for donations that actually delivered a computer virus. Similar scams, including fraudulent home repair offers, plagued Florida in the wake of the hurricanes.

Businesses can help ensure their corporate donations go for the intended purpose by being aware of the scams that may arise in the wake of natural disasters and separating reputable charities from the impostors. A number of Web sites, including the Better Business Bureau (www.bbb.org), the BBB's Wise Giving Alliance (www.give.org) and Internet Scambusters (www.scambusters.org), provide information on charitable organizations. State attorneys general also monitor charities.

While you should encourage employees to research potential beneficiaries, don't:

- Send cash donations — always make checks payable to the charity rather than to an individual,
- Be fooled by impressive-sounding names or those that resemble names of reputable organizations,
- Be pressured — legitimate charities should welcome your gift whenever you send it,
- Give to a charity you are unable to fully investigate with the BBB or your state's attorney general's office, or
- Click on a charity link that comes via an unsolicited e-mail from a source you don't recognize.

Everyone wants to help when disaster strikes. And by following a few simple steps, you can help ensure you and your employees don't become victims yourselves.



*This publication is distributed with the understanding that the author, publisher and distributor are not rendering legal, accounting or other professional advice or opinions on specific facts or matters, and, accordingly, assume no liability whatsoever in connection with its use. In addition, any discounts are used for illustrative purposes and do not purport to be specific recommendations. ©2005 FRAjj05*

**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