

# fraud alert

june/july 2006



**Data mining can be a goldmine for fraud investigation**

**Survey suggests best fraud prevention measures**

**I didn't order that!**

Don't be fooled by false billing schemes

**Lack of faith**

When fraudulent insurers profit from wrongful denial of claims

**Fraud to watch for:**

**Pharming**



**McGOVERN & GREENE** LLP

Certified Public Accountants & Consultants

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

# Data mining can be a goldmine for fraud investigation

Artificial intelligence, or AI, sounds like something out of a science fiction film. Computers that can mimic the way humans think are believable on the big screen, but can they work on real world problems like preventing and uncovering fraud?

They already are with data mining — the process of analyzing information and finding patterns from data in large databases. In the financial industry, for example, data mining has been used to detect credit-card fraud since 1982. Neural networks, or statistical programs that classify complex data sets by grouping cases together, are credited with cutting credit-card fraud significantly.

## Beyond logic

Data mining isn't just deductive query processing on steroids. Also called knowledge discovery, the process goes beyond logic to "intuit" data relationships. If you shop online, for example, you've likely seen the results of data mining yourself: It's the technique retailers use to come up with recommendations for future purchases.

Data mining for fraud deterrence assumes a more serious purpose. With models built from historical data of fraudulent behavior, fraud investigators can use data mining to help identify similar occurrences.



For example, it might help detect people who stage auto accidents to collect insurance settlements, or expose rings of doctors involved in medical fraud. Fraud investigators have examined patterns of telephone calls to detect blanket medical screening requests for inappropriate treatments. That and similar knowledge from data mining has helped them break up fraud rings and save insurers and the government millions of dollars.

*In many ways, data mining software reaches the same conclusions humans would, given the same information.*

## Looking for patterns

Data mining software looks for relationships and patterns by:

**Class.** This includes stored data, such as purchase records, sorted into predetermined groups. This information might, for example, tell fraud experts when people are most likely to drive off from gas stations without paying.

**Clusters.** Data is grouped by logical relationships. Managers' vacation time preferences — or refusal to take vacation time — could suggest fraudulent activity that might be discovered in their absence.

**Associations.** These might suggest fraudulent data manipulation is more common in certain seasons or on certain days of the week.

**Sequences or trends.** These patterns can predict, for example, how likely it is a 30-year-old man with a house in the suburbs will defraud his employer.

In many ways, data mining software reaches the same conclusions humans would, given the

same information. But humans would have to sift through reams of paper — or scroll through thousands of computer data screens — to assimilate the information.

### Concerns remain

There are some concerns about the use of data mining. One is data integrity related to the GIGO (garbage in, garbage out) theory. When conflicting or redundant information from several databases is integrated in a central data warehouse for analysis, data mining software must be able to translate the data and select the appropriate information for analysis.

Another issue is privacy. Data mining can glean significant information about individuals' habits and preferences, as well as personal information —

such as Social Security numbers — that must be protected if it could be used to perpetrate a crime or if it would identify someone involved in medical treatment or a financial transaction. Experienced fraud examiners, therefore, have in place safeguards to prevent inappropriate disclosure of data.

The cost of data mining might also be a concern. To be of maximum value, large amounts of data may need to be collected. As the process is more widely used, however, its cost is going down.

### Worth the effort

Even acknowledging such concerns, fraud experts are finding great benefits in data mining. Having their very own “Hal” gives them a significant advantage over the criminals they pursue. 🔑

## Survey suggests best fraud prevention measures

Companies that use multiple layers of fraud controls detect more fraud and suffer less severe financial loss from fraud than do those that rely on only one or two detection devices. In addition, fraud risk management programs are most successful when they're based on trust rather than on control.

PricewaterhouseCoopers' *Global Economic Crime Survey 2005* came to these and other conclusions. The survey also showed an 8% increase in reported incidents of fraud over 2003 results. Nearly half the world's businesses reported being victims of fraud in the two years since the last survey, and on average they were hit eight times.

### The bigger, the harder hit

Large companies — those with more than 5,000 employees — were disproportionately affected: 62% reported fraudulent activities over the two-year span, compared to only 36% of firms with fewer than 200 employees.

Because large companies are more operationally complex and offer staff relative anonymity, they can



create greater opportunity for fraud. Still, more than 10% of the smaller companies that reported fraudulent activity said they had lost more than \$1 million as a result. And it's notable that companies of every size detected more fraud than in the past. But there's some good news: The majority of defrauded companies that had more than five fraud control measures in place recovered at least some of their losses.

More than half (51%) of the businesses that use five or more controls — external audits, internal audits, internal controls, fraud risk management systems and corporate security — detected fraud during the survey period. And 52% of them were able to recover some or all of the losses attributable to fraud. By comparison, only 39% of companies with fewer than five controls discovered fraud in their midst; only 43% of them recovered any of the stolen money.

There are a number of variables to be considered in analyzing the report's results, such as increased regulatory pressure for strong corporate governance and a growing awareness among businesses of the need for more sophisticated controls. Indeed, the increase in reported fraud could indicate better detection rather than heightened activity. The study's authors, however, doubt it: "It is our view that the levels of reported fraud are, in many cases, only the tip of the iceberg."

### Reports just a start

How, then, can companies find and, more important, prevent fraud? The answer appears to lie in developing complementary layers of fraud control measures and in creating an ethical business culture that fosters employees' social and emotional identification with their company.

Noting that unearthing fraud early limits damages and increases the likelihood of recovering lost assets, the report suggests companies make an effort to do the following:

- Assess risks and vulnerabilities particular to their organization.
- Proactively monitor risky areas of the company.
- Develop whistleblower policies and protections.
- Actively communicate — and adhere to — a corporate antifraud culture.
- Develop robust fraud response plans.

Because companies with strong internal audit processes were more than 10% more likely to uncover fraud, these are also recommended.

## Collateral damage can be significant

In assessing their risk of fraud, companies must not overlook the "collateral" damage fraud can cause, according to the PricewaterhouseCoopers *Global Economic Crime Survey 2005*. More than 40% of surveyed respondents said fraud resulted in significant damage to their brand or reputation, a decline in staff morale or impaired business relations — damage that's difficult to quantify but potentially catastrophic.


Fraud can also erode confidence in any company's quality of leadership. And, in some cases, employees may be encouraged to copy the perpetrators. It's imperative, therefore, that companies have fraud response plans in place. These plans should clearly indicate management's commitment to immediately correcting any fraud situation that arises, as well as the steps being taken to do so.

Having a multifaceted fraud prevention program in place may be particularly important during times of change. Companies that reported being in a period of change were 20% more likely to become victims of fraud than those in stable operational periods. Change can disrupt not only day-to-day business activities, but also fraud control mechanisms — creating more opportunities for fraud.

On the other hand, in your zeal to root out fraud, take care not to create an atmosphere of distrust. Employees who feel they aren't trusted may be more motivated to commit fraud. The report cites studies confirming that employees rate fair, honest treatment above material advantage when asked about job satisfaction.

### Strength in layers

While the PricewaterhouseCoopers survey demonstrates that companies have made significant progress in detecting fraud, it concludes that the battle is far from won. More than a third of the reported fraud was exposed by accident — either through an unexpected tip-off or some other "chance" occurrence.

That, the report points out, could indicate that many companies' confidence is misplaced when they say their existing risk-management program is reducing fraud. "If companies are serious in their desire to mitigate not only the financial and collateral threats from fraud itself, but also the threat of penalties from the ever-growing arm of the regulator, significantly more layers of control need to be added," it concludes. 

# I didn't order that!

## Don't be fooled by false billing schemes

You're adept at identifying — and hanging up on — telemarketers at home, but are you and your employees aware of the ploys unscrupulous operators use to bilk your business? False billing schemes come in all kinds of packages, including telemarketers.

If your business is like most, you're bombarded with requests for donations and advertising inserts from charitable organizations and other solicitors — most of which are legitimate enterprises. It's the ones that use false billing schemes that can wreak havoc with your company's bottom line.

### Counting on confusion

Often false-billing swindles involve persuading businesses to pay for ads in fictitious publications. In one popular scheme, a telemarketer calls to “verify” the billing address for an ad. You may not remember ordering the ad, but the caller's spiel is so good, you're not sure you didn't. The invoice arrives, and you remember talking to the telemarketer. So even though you still don't recall ordering the ad, you pay for it.

Another, related scam involves fake office supply orders. An invoice may be sent to you for supplies or services you received but never ordered, and unless you look closely you may never notice the fine print stating the “invoice” is a solicitation. You may be less inclined to scrutinize the inflated price when the merchandise being invoiced has already been moved to storage or is in use.

Many companies erroneously believe they must pay for merchandise they use, even if they didn't order it. But if you didn't order something, you can treat it as a gift; it's illegal for the sender to either bill you for it or ask for it back.

### Beware of two-fers


When fraudulent telemarketers solicit office supply business, they may claim to have sold you supplies in the past, or say they're sending you a promotional item. The promotional item arrives with an invoice. If you return the single item they sent, they might claim you received two items and are required to pay for the one you kept.

Other tactics false billers use include:

- Quoting prices per item rather than per box or case — offering, for example, a box of pens at \$10, without saying it's \$10 per pen, rather than \$10 per box,
- Sending additional bills and shipments to businesses that pay for initial unordered shipments,
- Sending “past due” notices for renewals on fictitious previous contracts, and
- Shipping incomplete or inferior products.

Because these tactics can be sneaky and subtle, it's important to train employees to recognize scams. Assign designated buyers and instruct all orders to go through these individuals. When the buyers order merchandise, they should document the cost. Then they should make sure what they receive is the accurate quantity and brand, at the agreed-upon price.

### Know your suppliers

If you buy only from firms you know and trust, and your staff knows how to handle cold calls, you'll be ahead of the false billing game. Finally, if you do receive merchandise you didn't order, feel free to use it — but don't pay for it. 



# Lack of faith

## When fraudulent insurers profit from wrongful denial of claims

You pay your insurance premiums faithfully, secure in the knowledge you're covered if something goes wrong. Most of the time, you're right. Not only is it good business practice for insurers to cover legitimate claims, but it's illegal for them to deny them.

Unfortunately, not all insurers are good business-people, and some are even dishonest. Those few may be guilty of bad faith — wrongfully denying insurance claims — that can cost businesses significant aggravation, not to mention legal fees, to combat.

### Disagreement or bad faith?

An insurance policy is a contract. The insured agrees to pay premiums and take reasonable steps to prevent injury or damage; the insurer agrees to settle legitimate claims according to the terms of the policy.

There may be times when you and your insurer disagree about what is covered or what constitutes a reasonable delay or amount in settlement, but errors in judgment and offers of compromise don't

necessarily equal bad faith. Bad faith arises when the insurer sacrifices its insured customers' interests to enhance its own bottom line — and that can involve fraud.

### Shady tactics

Outright denial of claims is only one bad faith practice that indicates fraudulent insurance practices are being employed. Shady operators may also:

- Unreasonably delay investigating claims,
- Attempt to settle claims for less than the amount specified by the policy,
- Bog down the claim process by requiring multiple, duplicative proof of loss forms,
- Fail to settle one portion of a claim to influence acceptance of lesser settlements under another section of the policy, and
- Misrepresent policy provisions related to the claims.




If, after prolonged negotiations, the claim has gone to arbitration in an effort to resolve the issues without legal action, a bad faith insurer might threaten to appeal arbitration awards to pressure the insured to settle for less than the awarded arbitration amount.

Defending against such practices can be difficult. One problem is that there's no federal — only state — regulation of the insurance industry. Thus, scammers can illegally deny claims across the country, knowing that fraudulent insurance practices are subject only to state scrutiny and penalties. These penalties vary, but typically aren't stiff enough to be deterrents. In addition, such fines do nothing to compensate claimants who were wrongfully denied.

It's important, therefore, to deal with only reputable insurance companies. Before you buy, check with industry rating services such as A.M. Best (www.ambest.com) or your state's licensing board. Ask colleagues and friends for their recommendations, as well. If you have a claim, be sure to file it promptly and document all correspondence and communication relating to it.

## Insure against fraud

The financial incentives, coupled with a lack of consistent regulation across states, can make bad faith insurance practices very attractive to those bent on fraud. Basic preventive measures can go a long way toward helping you avoid these types of insurers. But if your insurer seems to be illegally denying your claim, you may, unfortunately, have to settle the matter in court. 



## fraud to watch for: Pharming

By now, most people are aware of Internet “phishing” attacks in which fraud operators cast an e-mail lure hoping to obtain personal information that can then be used for nefarious purposes. The good news is that every computer comes equipped with a “delete” button that makes it easy to swim away from phishing danger. The bad news: Phishers are becoming “pharmers” — or domain spoofers — using ploys that aren't as easy to detect or combat.

### Planting the seeds of fraud

With pharming attacks, all you have to do is type a Web page address into your browser. Pharmers plant the seeds of fraud underground, poisoning the domain name servers (DNS) to translate requests such as anybank.com into an Internet address that redirects your request to pages they control.

In many cases, you'll find yourself at a porn site or some other annoying page. More ominously, you may arrive at a site that looks like your bank's, but isn't. Your computer, the DNS and you all believe you're at the right site, but in reality you're visiting a “pharm” and may enter personal identification information that allows pharmers to steal your identity.

If the pharmer is simply a mischief-maker, rather than a criminal bent on identity theft, he or she may use page-jacking to scam you. This process makes digital copies of Web pages and inserts a change in them. Page-jackers then submit the



altered pages to search engines where unsuspecting people click on the links. In some cases, the page-jacker is making money through ads on the site.

### Retiring pharmers

While the phishing hole is drying up — thanks to consumer awareness and corporate monitoring — pharming remains fertile ground for scammers. DNS providers, however, are taking action. Some sites now offer certificates, with a pop-up dialogue box that asks users to be sure the name on the certificate matches that of the site they're attempting to reach. Such efforts, in combination with continually updated antivirus and antispyware programs, will go a long way toward retiring Internet pharmers.

# 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](http://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

