Fraud Alert

Insights on fraud detection and deterrence

OCTOBER/NOVEMBER 2010

Data mining drills to the heart of fraud

Big potential, big risk
Doing business in China

Are your employees flying the red flags of fraud?

I didn't order that!
Don't be fooled by false billing schemes

E-mail can be an evidence challenge

Wilson & Turner
Incorporated
Investigative Consultants

2752 Mt. Moriah Parkway
Memphis, TN 38115

Voice (901) 546-8585
Fax (901) 546-8584

www.wilson-turner.com

Data mining drills to the heart of fraud

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 the early 1980s. Neural networks, or statistical programs that classify complex data sets by grouping cases together, are credited with cutting credit-card fraud significantly.

But this tool's use isn't limited to the financial industry. Data mining can be used by many companies to detect everything from financial statement manipulation to fudged expense reimbursement reports. When employee theft is suspected, but the company doesn't know how to gather the evidence to confirm it, data mining can help.

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.

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 40-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.

Potential concerns

There are some concerns about the use of data mining. One is data integrity related to the GIGO (garbage in,

One of these things is not like the others

In a fraud investigation, an expert might use data mining to look for activity that diverges from behaviors typically associated with nonfraudulent transactions. Data mining, for example, could find:

- ✧ Records with missing information,
- ✧ Multiple vendors using the same address,
- ✧ Unusually high payments to vendors or other transactions outside the normal range,
- ✧ Payments for large amounts near the end of a quarter,
- ✧ Vendor invoices with consecutive numbers, suggesting the vendor has no other customers,
- ✧ Payments just under the amount requiring manager approval,
- ✧ Payments to terminated or nonexistent employees, and
- ✧ Transactions with future dates.

Innocent explanations are always possible, but any of these occurrences merit further investigation.

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.

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. ■

Big potential, big risk

Doing business in China

China offers plenty of opportunities for American businesses looking for lucrative new markets. But if your company has Chinese operations or intends to start doing business in China, be certain you understand the risks. Rudimentary government regulations and certain local customs can encourage fraud in the Chinese marketplace. Western companies, in particular, are vulnerable to such fraud.

Familiar fight, new battleground

In many cases, the kinds of fraud experienced in China are the same as those found anywhere — as are the tools to fight them. The problem is that differences in language and culture, as well as geographic distance, make it easier for the unscrupulous to conceal occupational theft.

American companies depend on legal contracts and formalized corporate governance, but China for centuries has relied on "guanxi," or personal connections. Nepotism, therefore, is an accepted way of doing business, and handshakes seal many deals.

Lack of government oversight makes it easy for local employees to set up companies that compete with their foreign-owned employers' businesses — often using the foreign company's technology and other resources. They also may use foreign investors' assets to secure loans for themselves. This is made relatively easy by China's still-developing regulatory and auditing systems. In many cases, Chinese lenders and government authorities don't even have the resources to verify assets pledged as collateral.

Other common fraud schemes in China include:

- Billing foreign investors for more than the cost of goods and services,
- Falsifying production records and selling products off the books, and
- Collusion with, or bribery involving, government officials.

Unfortunately, when books and records are thousands of miles away, in an unfamiliar language and a country where accounting standards are still evolving, it can be impossible to know whether discrepancies are a result of sloppy bookkeeping or outright fraud.

Distance breeds discrepancies

Western companies have stepped up their efforts in the past five years to minimize risks associated with doing business in China, but there's still plenty of room for improvement. According to a 2010 Ernst & Young survey of companies with Chinese operations, 62% offer a confidential fraud reporting hotline, 59% have policies to promote adherence to international anticorruption legislation and 39% maintain a fraud database.

Unfortunately, what managers who work in the United States believe, and what's actually happening at their China division, can be very different — particularly if the company relies on local managers. Chinese managers who are compensated based on their ability to minimize costs may be tempted to hide irregularities in hours worked or workplace conditions, as well as suspect financial dealings.

Proceed with caution

One solution is to proceed cautiously into the Chinese market. Chinese law requires foreign enterprises to partner with Chinese nationals, and it's imperative that you investigate potential partners thoroughly before embarking on a joint venture. The Foreign Commercial Service offices in U.S. consulates, trade associations such as the U.S.-China Business Council, local consulting firms and companies in China that specialize in due diligence all are sources that may be able to help.

Other best practices include:

- Placing at least one expatriate resident manager on site to monitor day-to-day activities,
- Enlisting the help of independent auditors to regularly review the books rather than rely exclusively on internal accounting personnel, and
- Implementing and enforcing strong internal controls and antifraud policies.

Because poor management-employee communication and insufficient training can hamstring even the most effective program, both should be an ongoing part of every antifraud undertaking.

Change comes slowly

The good news for foreign investors in China is that the Chinese government, particularly in the wake of food and other product contamination scandals over the past few years, is actively working to clean up fraud. But change of this scale takes time.

For now, American businesses should move slowly into this market and remain vigilant once they get there. Even though China is making rapid progress, the risk of fraud remains real. ■

Are your employees flying the red flags of fraud?

Owners and executives are a company's first line of defense in spotting fraud. While a forensic accountant generally is the best person to unearth the "hows and whys" of workplace theft, it's up to a business's leaders to know when it's time to call in professional help. The signs can be easy to miss, but if you look closely they're usually there.

When something doesn't belong

Occupational thieves may use anything from fictitious vendors to false invoices to cover their tracks. Look for duplicate payments, out-of-sequence entries, differences in handwriting, entries by employees who don't usually make them and accounts that don't properly balance.

If your warehouse manager buys a luxury car and installs a backyard pool, you may have to ask how that's possible on the salary you're paying.

Scan transactions for amounts that appear too large or too small, as well as those that occur too often or too rarely. And if no one can explain an unusual journal entry or adjustments to inventory or accounts receivable, it merits further investigation.

An increase in the number of customer or vendor complaints is another warning sign. An investigation may lead to a relatively innocent cause, such as a glitch in your shipping system — or it may lead to a fraudulent billing scheme. Pay equally close attention to declines in product quality. They could just stem from a faulty batch of paint, or they may indicate that a fraud perpetrator is working in your purchasing department.

Look for la vida loca

Changes in an employee's lifestyle may be evidence of fraud. Few thieves, after all, steal to invest the money in U.S. Savings Bonds. Lifestyle changes can be difficult to spot, at least initially, but over time patterns are likely to emerge.

One piece of expensive jewelry could be a gift, and a good return on an investment may supply the funds for an exotic vacation. But if your warehouse manager starts wearing a new pair of expensive shoes every day, buys a luxury car and installs a backyard pool, you may have to ask how that's possible on the salary you're paying. In short, if someone's ship seems to have come in, ask where it's docked.

Multiple personalities

When employees steal, especially if they're first-time offenders, their behavior may change. In fact, you may not even recognize them. People who have always been cooperative may become argumentative. Or, alternatively, someone who typically has been difficult may suddenly act like everyone's friend.

If an employee starts drinking to excess or takes up smoking, ask what's wrong. If they can't sleep, worry obsessively about the possible consequences of actions, resent other employees' opinions or participation in "their" projects, or even just sweat a lot, be concerned. They may be wrestling with a

personal problem such as divorce or bereavement — or they may be stealing you blind and feel guilty or worried about getting caught.

Getting managers involved

If you don't have contact with most employees on a daily basis, educate your managers about the warning signs of fraud. Mid- and upper-level managers working in close proximity to staff members are more likely to notice when something — such as an employee's spending habits or demeanor — has changed. If such signs exist and you've unearthed evidence of theft, don't hesitate to call in a fraud expert to investigate further. ■

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 company? False billing schemes come in all kinds of packages, including telemarketers.

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

E-mail can be an evidence challenge

When fraud incidents end up in court, e-mail evidence can be critical to proving or disproving a case. Nevertheless, many companies continue to take a haphazard approach to handling e-mail. Now more than ever, it's important that you and your managers understand how these types of communications can be used as evidence.

In addition to their express messages and attachments, e-mails can reveal a wealth of information. They might provide evidence on matters ranging from intent, offer and acceptance, and relationships to infringement, prohibited disclosures, privacy violations, and security breaches.

The nature of e-mail means it also can be difficult to handle. In particular, it is:

- Easily duplicated,
- Long-lived — often enduring longer than expected or intended,
- Vulnerable both to intentional and unintentional alteration, and
- Packed with metadata.

E-mail proliferates in ways not visible to the naked eye. Copies appear in the sender's Sent folder and recipient's Inbox and Deleted folders. They also might appear on hard drives, network backup systems and the systems' backup tapes. If sent or received via web mail, such as Yahoo! Mail or Gmail, copies may exist on the service provider's servers. And if a PDA was used as part of the communication, a copy probably resides there, too.

Not only can e-mail evidence enable your company to prove its case against a thieving employee, but you may be required to produce it in the event of many types of litigation. Litigation discovery requests may dictate retention duties. But, at the very least, your company's employees should be alerted to the need to preserve evidence and trained on how to treat existing and future e-mails.

Forensic experts can help to copy hard drives of company computers, along with drives on PDAs and cell phones. Backup tapes from the tape rotation also will need to be pulled, so they won't be copied over unknowingly. Indeed, to protect against any inadvertent data loss, it's essential to call in forensic experts as soon as you suspect fraud or other circumstances that could eventually pave the way to court.

Know who to trust when fraud occurs

When it comes to fraud impacting a business, the unfortunate reality is that the question is "when", not "if." Wilson & Turner Incorporated specializes in identifying, isolating, and unraveling financial fraud schemes and plotting a path toward financial recovery for the victim organization.

Fraud is present in almost all businesses, with only the internal control and audit processes to keep it in check. When those functions fail, or are circumvented, frauds can quickly grow to devastating proportions.

WTI was established in 1996 to help business, industry, and governmental organizations successfully resolve white collar crime related matters. The firm has particular expertise in resolving employee fraud issues, recovering losses, and protecting corporate assets. WTI provides consulting and expert services to corporations, banks, major law firms, and national and state governments.

WTI specializes in:

- **Fraud solutions**
- **Independent investigations**
- **Employee dishonesty**
- **Due diligence**
- **Commercial litigation**
- **Insurance claims**
- **Computer forensics**
- **Anti-fraud training**
- **Expert witness testimony**

Focused on the investigation and recovery aspects of financial fraud, WTI is experienced in dealing with transition periods, including growth and re-engineering processes; business changes, including takeovers, mergers, and spin-offs; and insurance claims, including professional negligence, Directors & Officers (D&O), Fidelity Bonds, and contractual disputes.

Using sophisticated analysis techniques, WTI conducts forensic and investigative exercises to track fraud losses and identify scheme participants.

Wilson & Turner Incorporated

Investigative Consultants

2752 Mt. Moriah Parkway
Memphis, TN 38115

Voice (901) 546-8585
Fax (901) 546-8584

www.wilson-turner.com