Fraud Alert

Insights on fraud detection and deterrence

YEAR END 2009

Contemplating a merger?
Don't get blindsided by fraud

Conducting a year end fraud sweep

How software can prevent theft

Two things are inevitable: Fraud and taxes

Red Flags Rule boosts business security requirements

Wilson & Turner Incorporated

Investigative Consultants

2752 Mt. Moriah Parkway
Memphis, TN 38115

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

www.wilson-turner.com

Contemplating a merger? Don't get blindsided by fraud

Mergers are like marriages: Success depends on any number of factors, but failure may be a result of one overriding flaw. In the case of business combinations, that flaw often is lack of thorough due diligence. With investors, lenders and other stakeholders noticeably skittish in the wake of corporate accounting scandals and a weak economy, it's more important than ever that you know whom you're marrying before you walk down the aisle.

You may be able to get some of the information you need about a potential acquisition from public documents and interviews with senior executives. When it comes to unearthing creative accounting practices and fraud, though, you'll likely need outside help. Forensic accountants know where and how to look for financial irregularities that could prove fatal down the road.

An antifraud culture

Premerger due diligence begins with your own assessment of a potential acquisition's corporate culture. One warning sign is a company that hasn't demonstrated a commitment to fraud prevention or implemented best practices for governance. It's important that the organization have well-defined and regularly reinforced codes of ethics, as well as strong internal controls that are periodically reviewed and tested for compliance.

Companies that demand unreasonable financial performance from their managers are more likely to be defrauded.

Another potential problem is a management team that doesn't communicate well. A CFO with an intimidating or dictatorial management style, for example, might feel free to bend accounting rules because other employees are too fearful to question his actions.

Of course, any effective due diligence includes intensive scrutiny of corporate, financial, tax, loan and regulatory records. It should encompass short-term debt retirement capabilities, liquidity, profitability and the ability to meet long-term obligations. This is where an experienced forensic accountant can add value to the process.

Digging for dirt

Experts look for documentation of any financial claims and are alert to signs of cleverly hidden shenanigans. If, for example, a company says it has brought its income recognition policies into compliance with new SEC standards, a forensic accountant will consider what effect the change has on previous figures. The expert also will examine earlier figures to see if they reflect any financial irregularities.

A forensic accountant may devote much of his or her attention to earnings that are subjective, too. Reserves, accruals and estimates all can be manipulated for income management purposes. If

Get the word out

One mistake many companies make during merger and acquisition transactions is overlooking the importance of a good communications strategy. Employees — especially if they're also shareholders — investors, lenders, customers and suppliers all want to know how a merger will affect them. Explain in as much detail as necessary why the deal makes sense and how it will benefit stakeholders.

Early on, determine how you'll describe strategic goals, as well as how you'll communicate, monitor and report progress toward them. Don't be overly optimistic, but attempt to minimize uncertainties and avoid undue disruptions. Be honest about the effects you expect the merger to have on earnings and return on invested capital — and then let the world know whether you were right. If problems arise, address them openly.

If a merger begins with negative perceptions outside the inner circle of top executives, it can be difficult to turn those perceptions around. Mergers are complicated, but they're not — or shouldn't be — top secret. Communicating what you can as soon as you're able will help you avoid undue pressure to turn in unreasonable numbers once you've signed the deal. And pressure to perform is the last thing you need if you want to avoid fraud.

accruals, for example, have increased significantly in recent months, it's important not to blindly accept the company's assurance that these increases are due to normal fluctuations. Forensic experts insist on specifics: What causes the fluctuations? Why are they handled this way? Is there a better approach? If so, why isn't it being followed?

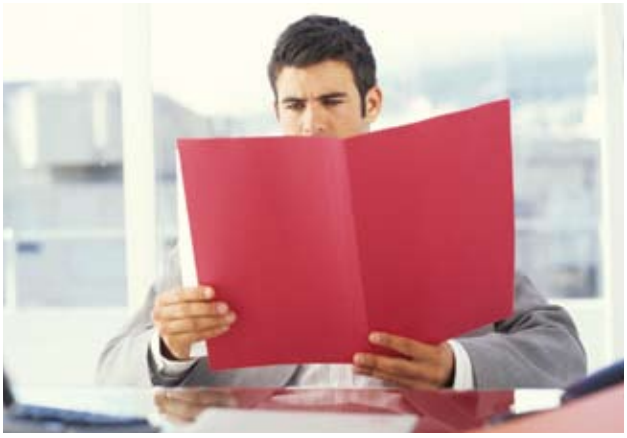
Experts also look beyond the numbers and examine the opportunities and potential reasons for fraud or misstatement. Companies that demand unreasonable financial performance from their managers, for example, are more likely to be defrauded than are companies with realistic expectations.

No hiding, please

Forensic accountants can discover hidden liabilities, overvalued receivables or securities, understated liabilities, and overstated inventories — any or all of which can create an inaccurate picture of a company's true value. Signs of potential fraudulent reporting include:

- Excessive restrictions on auditors,
- Material (more than 5% of market value) related-party transactions,
- Individuals or executive "cliques" dominating corporate management,
- High employee turnover, and
- Excessive tax-driven earnings reductions.

Any of these may be significant, but limiting auditors' access to data, senior executives or operational personnel generally is considered a sign that something is amiss.



More than compatibility

When it comes to mergers, compatibility is, of course, important. As in a marriage, one party's strengths can compensate for the other's weaknesses. But some weaknesses can be crippling, so it's essential that you examine your potential partner for fraud before you make the leap. ■

Conducting a year end fraud sweep

The average U.S. business is estimated to lose 7% of its annual revenues to occupational fraud, according to a survey by the Association of Certified Fraud Examiners (ACFE). For companies with close profit margins, that could mean the difference between closing the year in the black and closing in the red.

You can help start the new year right by performing a fraud protection analysis now. A thorough, objective review can unveil suspicious losses and the weaknesses that leave you vulnerable to fraud perpetrators.

Turn over rocks

There are hundreds of ways to commit fraud, and the signs aren't always obvious. Enlist the help of a CPA to perform a financial audit of bookkeeping records, invoices, bank statements, payments, journal entries, financial reports and other records with an eye toward identifying doctored, forged or missing documents.

For your part, review your company for telltale fraud signs that include:

Missing documents. Pay attention to how long it takes employees to produce documents for your expert's audit. If some records are missing, ask why and what steps employees took to find them. Documents that can't be located are a red flag for fraud.

Out of balance books. When stolen assets aren't covered by a fictitious entry, the books will be out of balance. An end-of-year inventory of merchandise or cash can bring missing assets to light.

Excessive journal entries. Be wary of unusual numbers of journal entries posted near the end of the financial year. They could be adjustments made to cover theft or misappropriation.

Adjustments to receivables or payables. When customer payments are misappropriated, fraudsters may adjust receivables to cover the shortage. Similarly, adjustments to payables may signal phony billing schemes.

Excessive payroll. Missing or otherwise unaccounted-for employees could indicate a "ghost" employee scam in which perpetrators pay nonexistent employees, pad time records, falsify salaries or commit withholding fraud. One way to expose the presence of ghosts is to hand out year end paychecks or bonuses yourself. If you have leftover checks, investigate further.

Unusual behavior. Employees who are reluctant to take time off around the holidays or when they come down with the winter flu may fear someone else will uncover their illegal activities in their absence. Those stealing from the company also may seem irritable or defensive when asked to comply with your fraud sweep.

Confront the results

If something looks suspicious, confront it — resist the temptation to explain away exceptions. Then keep digging. Don't assume, for example, that the first employee you find cooking the books is the only one exploiting the gaps. Unfortunately, fraud schemes often involve more than one person. And fraud also can be committed by people outside the company or by a combination of employees and outsiders.

But keep in mind that warning signs don't always lead to a thief. Genuine errors or an ill-designed process may be at fault for accounting irregularities. Better training or process improvements can prevent honest mistakes in the future.

Stay in control

The end of the year is also an ideal time to assess the effectiveness of your fraud controls. A system that may have been effective two years ago or that was appropriate for one job may not meet your organization's changing needs or address the risks associated with other jobs.

If you haven't already established a system for employees, vendors, customers and the public to report suspicious activities, do so. Public companies are required to provide a confidential hotline and private businesses are strongly encouraged to offer one.

Start the year right

Even the most trustworthy employees are capable of misappropriation and other fraudulent acts. Auditing financial records, scouring your business for fraud warning signs and reviewing controls right now will put you in a more financially sound position to start the new year. ■

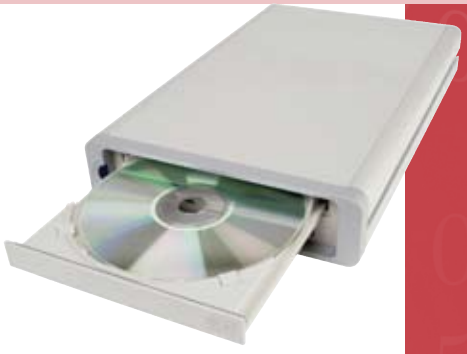
How software can prevent theft

The Sarbanes-Oxley Act of 2002 (SOX) requires public companies to document and monitor their financial controls. Often, this means cross-referencing reports in accounts payable, general ledger, payroll and other accounts at risk for fraud. Initially, many companies met the requirements manually, eating up countless staff work hours and counting on human eyes to spot new risks.

But in recent years software companies have launched dozens of fraud detection programs to take the guesswork out of monitoring financial controls — and to close gaps when they're detected. Today, even private companies consider such programs essential. Fraud detection software may cost money, but it may also prevent businesses from losing even more to theft.

Looking for patterns

Fraud detection software does what human resources typically can't: finds patterns of activities and flags anything that doesn't fit those patterns. A program can, for example, look for matches between vendors' names, bank accounts and addresses and those of employees. It might identify segregation-of-duty conflicts and find employees whose access rights would allow them to cover up fraud.



It also can keep up with the constant flow of new information as it's added to business systems — expanding its watch daily to include new folders and databases. It can even weigh existing activity patterns against previous, fraudulent patterns and sound alerts before an employee attempts the same scheme twice.

Researching the options

As the options for fraud detection software grow, so does the need for you to research them before you buy. A wide range of add-ons and customizations is available. But you don't want to make the mistake of paying for features you won't use — particularly if you lack other features you really need.

Before you invest in fraud detection software, evaluate it for:

Performance. Will the software impede your file servers or user access?

Scale. How much additional data can the system accommodate without upgrades or more hardware?

Installation. Can the fraud detection program be installed without disrupting your business operations? Will it require specialized installation services, or can your IT staff handle it?

Ease of use. Is the system intuitive? Will training be minimal, and on-site, or will it require off-site sessions for some personnel?

Functions. Does the system offer automated data permission revocations, data audit reports, data entitlement review, stale-data identification, data migration and other minimum requirements?

Integration. Can the system blend with and support your existing file servers and storage devices?

The system you choose should offer a low total cost of ownership by saving you time and resources.

Invest wisely

Fraud research shows that companies lose billions of dollars to scam artists every year. Whether you implement a companywide system all at once or choose a gradual implementation that targets your highest-risk areas first, it's worth learning what fraud detection software can do to protect your interests. ■

Two things are inevitable: Fraud and taxes

Just when you think you've heard it all, fraudsters come up with another way to separate you from your money. The newest ruses use the name of the IRS — and they're very convincing.

Dialing — and phishing — for dollars

In one of these new schemes, someone posing as an IRS employee phones fraud targets and tells them that they're eligible for tax refunds as rewards for filing their taxes early. But there's a catch: The thief claims that refunds are available only through direct deposit. If a target isn't willing to provide bank account information for the "deposit," he or she won't receive the refund.

A similar scam uses e-mail to offer specific refund amounts. Targets might be asked to click on a link to a claim form that requests personal information such as their date of birth or mother's maiden name. Scammers then use that information to access bank or credit card accounts.

In a newer version of the scheme, scammers e-mail notifications that tax accounts will be audited. Unlike most fraudulent e-mails, these messages may be personalized to recipients and appear very authentic.

Corporate victims

Businesses aren't immune to these schemes. Some scammers send e-mails to companies that purport to contain "tax law changes." They instruct recipients to click on links to download information on topics such as retirement plans and excise taxes.

Whatever you do, don't click on links or provide any information to callers.

Instead of providing helpful advice, the links download malware (malicious codes) that can give fraudsters remote access to the target's computer or network. Or they might install keylogger programs that send passwords and other security information to the perpetrators.

Spot the fake

Keeping your computer security software up-to-date is essential, as is knowing the signs that an "IRS" phone call or e-mail is fake. For example, the IRS:

- Doesn't use e-mails or phone calls to notify taxpayers, but instead uses the U.S. Postal Service,

- Never needs anyone's mother's maiden name, and already has taxpayers' dates of birth and Social Security numbers on file, and
- Doesn't give additional tax refunds.

If you or your employees receive phony IRS phone calls or e-mails, forward them to phishing@irs.gov, or report them toll-free at 800-366-4484. Whatever you do, don't click on links or provide any information to callers.

Taxing issues

Talk to a forensic accountant about updating your fraud prevention program to include these new schemes. And be sure to instruct employees on how they should handle suspicious communications. ■

Red Flags Rule boosts business security requirements

Most companies want to do their part to help stamp out identity theft. But the federal Red Flags Rule, now scheduled to go into effect on June 1, requires many companies to shoulder more of the load. Are you prepared?

New rules

Although the Federal Trade Commission has delayed enforcement of the Red Flags Rule several times, affected organizations shouldn't take such delays as an excuse to procrastinate. The rule is an expansion of the Fair and Accurate Credit Transactions Act of 2003. It's intended to curb fraud in the opening of covered accounts — those that are established primarily for personal, family or household purposes and are reasonably vulnerable to identity theft.

By June, all financial institutions and creditors need to have programs in place that enable them to detect and prevent identity theft and to identify certain patterns and practices that suggest fraud. Businesses that collect or use customer loan or credit information — such as auto dealers or retailers — are considered creditors and, thus, must comply with the rule.

Patterns and practices

Some requirements, such as ensuring that a customer's driver's license photo matches his or her face, are easy enough to implement. Others, including reporting patterns or practices that might indicate potential identity theft, take greater effort and may require expert assistance.

Suspicious activities are likely to vary from one business to the next but could include customer address discrepancies, an unusual number of newly opened credit accounts or incomplete personal information on a credit application. To report them, train employees to recognize unusual activities and take appropriate steps to validate and mitigate risk.

A forensic accountant can help you develop a written program that includes policies and procedures to define and detect red flags when they arise and respond appropriately to them. Programs must be updated regularly to reflect changes in risks. Additionally, you must put systems in place to verify change-of-address requests and to notify the account holder if an address provided substantially differs from the one you have on file for the holder.

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