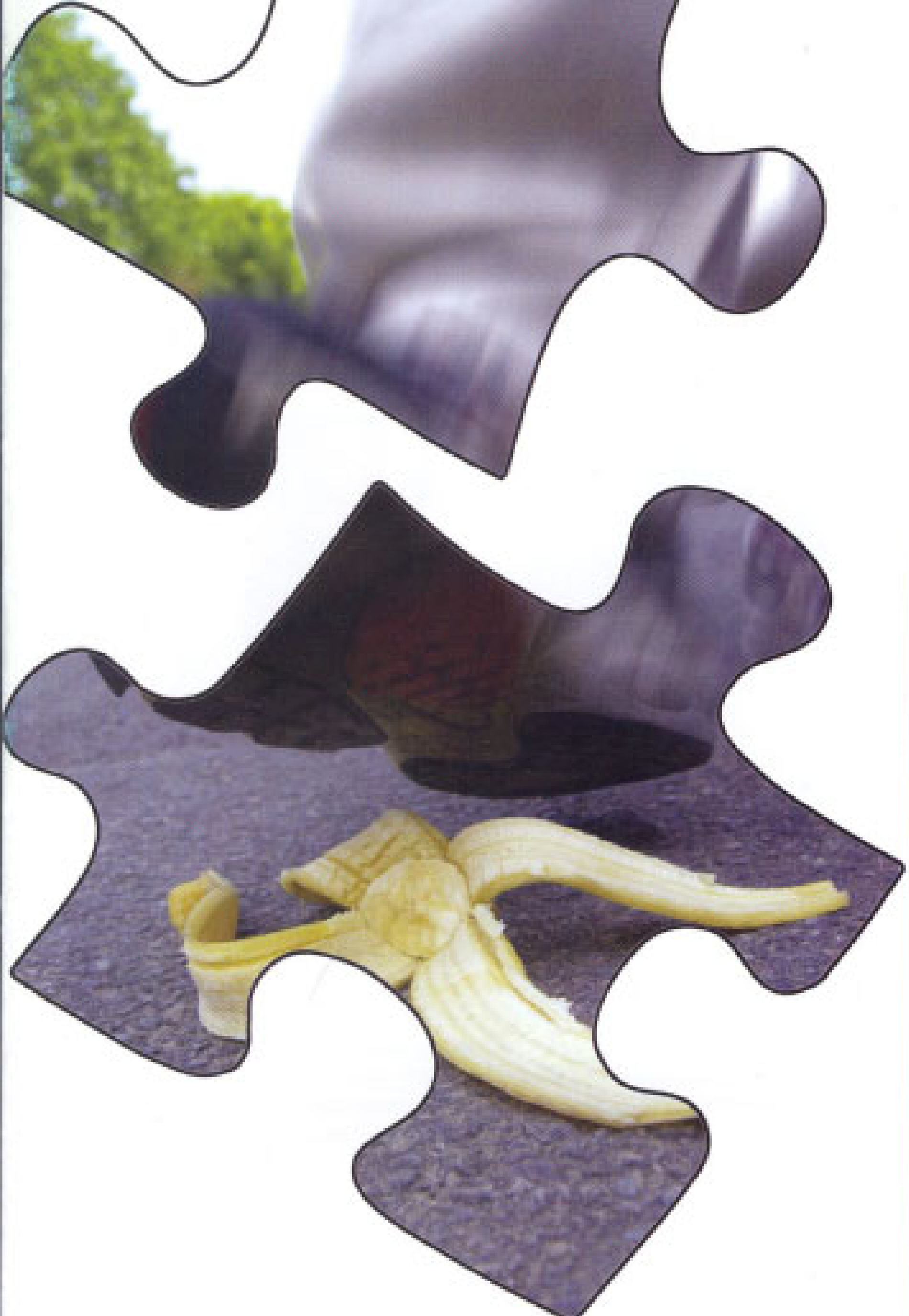


fraud alert

april/may 2004

Heading off a bad merger

When management companies skim profits

What's in a 1040 — and what's not

Recovering "lost" evidence with the help of computer forensics

Protect computers from employee theft

ROGERS, LYNCH & ASSOCIATES LLC

7051 Argonne Blvd. New Orleans, LA 70124 Phone: 504.282-1441 Fax: 504.282-6641 www.rlastars.com

Heading off a bad merger

How forensic accountants can reduce the risks

Mergers and acquisitions are filled with challenges and risks, some of them unavoidable. But you can reduce the danger with careful advance work by a forensic expert.

Take, for example, a $100 million deal between a major financial institution and another company. A week before the deal was to become final, the buyer decided to do a last-minute check on the target company's key management personnel.

The forensic accountants assigned to the task discovered an undisclosed indictment of the top executive of the target company on state and federal charges of manipulating financial statements and evading taxes. The indictment, not yet public, cast doubts on all the target company's financial statements and sank the deal.

Spotting cooked books

In cases like this, forensic investigations can help spot cooked books or other forms of deceptive accounting used to inflate earnings and distort the value of the target company. If not spotted in time, these practices can mean disaster after a merger goes through.

For example, after consumer services merchant CUC International Inc. merged with HFS Inc. in 1997, the Securities and Exchange Commission determined that senior CUC executives had used faulty accounting practices to create $500 million in revenues out of "thin air" during the three years before the merger.

In another case, health supplies distributor McKesson Corp. spent more than $14 billion acquiring health care software designer HBO & Co. Inc. — only to encounter postmerger problems. McKesson blamed the problems on alleged accounting improprieties overstating HBO revenues.

Avoiding missteps

To reduce the risk of missteps like these, acquirers call on forensic accountants to find out if the target has hidden liabilities or is faking performance figures. Forensic accounting combines accounting knowledge with investigative skills that dig beyond basic financial statements to spot questionable accounting practices.

In the case of Quaker Oats Co.'s $1.8 billion acquisition of Snapple Beverage Corp. in 1994, for example, the lead forensic accountant had warned Quaker that Snapple used an unusual accounting method that reported current expenses in prior fiscal years. This mixing of data produced more impressive results than those resulting from comparing figures from the same year.

Unfortunately, the investigator's warning remained unheeded, the merger went through and Quaker ended up selling Snapple for $300 million four years later, taking a loss of $1.5 billion.

Warning signs in a premerger investigation

Forensic accountants are on the lookout for subtle warning signals that may indicate trouble in a company targeted for acquisition. Among the danger signs they look for are:

- Excess inventory,
- Increased accounts payable and receivable combined with dropping or stagnant revenues and income,
- An unusually high number of voided discounts for returns,
- Lack of sufficient documentation in sales records,
- A large number of account write-offs, and
- Increased purchases from new vendors.

Manipulating income figures

Some accounting practices adopted to present a company in the best light, though questionable, may be perfectly legal. Manipulating income figures, for example, usually involves mismatching revenue with expenses rather than simply inventing numbers from whole cloth — which constitutes outright fraud.

Manipulated figures create a more favorable framework for viewing actual numbers. For example, a company that had previously amortized its goodwill over 20 years increased the amortization period to 35 years. The change softened the impact of goodwill on earnings and offset the company's failure to meet its income target.

Since major frauds often stem from weak internal controls, forensic accountants critically evaluate the target company's internal controls. Weaker or less sophisticated controls than those of the acquirer draw special attention.

Investigators want to determine if false numbers result from incompetence or systematic manipulation designed to mislead lenders and investors.

Preventing surprises

They also look for instances of disapproval by regulators and complaints by customers. This kind of careful investigation can help prevent unwelcome surprises, such as the postmerger discovery by one acquirer that the target company had manufactured and sold substandard items not recorded in the company's books.

To remedy damage to the company's reputation from inferior goods flooding distribution channels, the acquirer had to buy back the shoddy merchandise.

Looking at relationships

Supplier and customer relationships are important considerations in determining company value. You can't assume that all suppliers are reliable — some may actually present a competitive threat.

Investigators take a special look at relationships with overseas suppliers that the target company provided with tooling. One acquiring company learned too late that an overseas supplier used the target company's tooling to manufacture and sell components to the company's competitors.

Similarly, a target company may have "captive customers" that would disappear after the acquisition — for example, entities owned by relatives of target company management.

Conducting due diligence

Sums involved in mergers and acquisitions are substantial, so acquirers need to conduct thorough due diligence of the target. Careful investigation by a forensic accountant can reveal the true financial story of the target company, even when a rosy mask conceals questionable activities.

When management companies skim profits

How suspicious business owners can get facts

When business owners suspect their management agents of self-dealing, attorneys often call on forensic experts to help sort out the facts. An operational audit can determine if the management company is complying with the management contract, sometimes leading to favorable renegotiation of the contract.

For example, an experienced real estate property developer hired Marriott International to run his big new hotel in Quincy, Mass., and installed his own executive to oversee operations.

Soon, disputed invoices caused friction between the owner's representative and Marriott, culminating in a request that Marriott explain an invoice to the hotel for $3,000 in unspecified sales and marketing services.

Marriott refused to provide the information and ousted the owner's representative from the hotel office. The hotel owner sued Marriott, accusing it of fraud, accounting irregularities, mismanagement and taking kickbacks from suppliers.

In at least three other recent lawsuits, owners of Marriott-run hotels have made similar allegations, and Marriott is not the only big hotel management company facing these accusations.

Charges of fraudulent practices and irregularities have been lodged against both Hyatt Hotels (*Government Guaranty Fund v. Hyatt Corp.,* 3rd Circuit, CA, 1996) and Starwood Hotels and Resorts (*2660 Woodley Road Joint Venture v. ITT Sheraton Corp.,* Delaware, 1998).

Purchasing practices

Most lawsuits against hotel management companies target purchasing practices, and a forensic expert can help ferret out irregularities. An investigation, combined with the threat of a lawsuit, strengthens the owner's hand in renegotiating the management contracts on more favorable terms.

In one case, a forensic expert discovered hundreds of contracts with manufacturers and suppliers bringing millions of dollars in undisclosed rebates to the management company. The investigation also uncovered hidden management company ownership interests in some vendors.

The management contract restricted management company compensation to basic fees and incentives provided by the contract. When a management company fails to disclose the rebates it receives from its vendors, it changes the character of such rebates to bribes.

Since a management company serves as an agent for the hotel owner, agency law applies, with its prohibitions of agent self-dealing without disclosure to, and approval by, principals. But some hotel management operators hide rebates, levy extra fees and conceal associated documents from owners. These payments represent profits unlawfully withheld from hotel owners.

In 1992, Donald Trump engaged a forensic expert to investigate the financial transactions of Hyatt Corp. Resulting evidence of mismanagement and fraud helped Trump reach a $125 million out-of-court settlement.

In the *2660 Woodley Road Joint Venture* case, a U.S. District Court in Delaware awarded $30 million to the owner of a Sheraton hotel after determining that the management company, Starwood, had received vendor payments that were, in fact, rebates rightfully belonging to the owner.

Fee clarification

If the purchasing clause in the management contract specifies that the only compensation for purchasing services of the management agent is a purchasing fee, a forensic investigation can help owners recover all or a substantial part of vendor discounts and rebates. Findings can also help hotel owners negotiate new purchasing agreements that provide substantial proceeds from rebates or discounts.

In addition to rebates, forensic experts can alert hotel owners to other frequently overlooked costs. Sometimes, management companies are unwilling to explain extra fees, which can double or triple the charges specified in the management contract.

For example, the Quincy, Mass., hotel owner alleged in his lawsuit that independent agents who completed a Marriott's training program received 10% commissions when they booked guests into Marriott hotels, compared with 8% commissions paid to other agents.

Challenged surcharge

The surcharge, paid to the management company despite the fact that the basic management fee covered commission costs, was nearly double the core fee the hotel paid the management company.

Business owners can't operate with blind trust in management companies. To ensure a decent rate of return on their investment, owners need to evaluate the true costs of hiring management companies. Forensic experts can help them reach an informed conclusion.

What's in a 1040 — and what's not

Tax returns lead to hidden evidence

In a fraud case, the suspect's tax return can be a gold mine of information. From it, the fraud investigator can learn about the taxpayer's sources of income, expenditures, real estate holdings and other business interests.

Besides suggesting where the fraudster is hiding ill-gotten gains, Form 1040 can lead to evidence of how the suspect committed the fraud. Studying the returns, a forensic expert can decide where to dig deeper for hidden evidence.

Start at the beginning

Evidence from individual income tax 1040 return forms isn't part of every fraud case, mainly because the forms are difficult to get. In a civil case, counsel may obtain returns via a subpoena or a request to produce documents. A criminal case may need a subpoena from a grand jury or administrative officer, an ex parte order or a search warrant.

Form 1040 can lead to evidence of how the suspect committed the fraud.

But for cases that do include 1040 evidence, the forensic expert analyzes returns for all years under investigation. In civil cases, this is usually the last five years, but in a criminal case, all years in question become part of the analysis.

The return's income and expense numbers are important, because the suspect can't deny them without admitting tax evasion. But the listed information is really only the tip of the iceberg for fraud purposes.

Ruling out known sources of income and expenditures, the investigator can move on to hidden ones. Current and former addresses may lead to a search for property sale proceeds. Social Security numbers indicate the state of issue, often helping to reveal the subject's maiden name or parents' names and possible hiding places for missing assets.

An investigator may find similar information by checking the "doing business as" names of businesses in which the suspected fraudster has an ownership interest as well as their business addresses and employer identification numbers.

Then branch out

Schedules attached to the 1040 also offer leads. The forensic expert looks at itemized deductions, interest and dividend income, profit or loss from business, capital gains and losses, and supplemental income and loss forms.

Real estate taxes listed on Schedule A, for instance, can help the investigator track parcels of real property bought with fraud proceeds. The same is true of personal property taxes on autos, boats and airplanes.

Interest payments reported on Schedule A also tell a tale. If home mortgage interest appears small in relation to the home's value, the subject may have made a large down payment or principal payment. If so, it's logical to ask where the money came from. Investment interest can indicate fraud proceeds are stashed in offshore accounts or companies.

And if interest and dividends listed on Schedule B raise a red flag, lead counsel may decide to subpoena brokerage firms, banks, partnerships or sub-S corporations to learn about account balances and activity.

Even income from a legitimate business declared on Schedule C can yield fraud evidence, because certain cash-intensive businesses may provide a cover for money-laundering operations or unreported income. If the subject has filed Schedule D, *Capital Gains and Losses,* the investigator can acquire further information about legitimate income. If needed, counsel can issue subpoenas to uncover what hasn't been declared.

Find ill-gotten gains

Although fraudsters won't list their ill-gotten gains on tax returns, they'll often provide insights into what they did with those dollars. If you're investigating a fraud, be sure to include key information listed on returns as you pursue evidence.

Recovering "lost" evidence with the help of computer forensics

How much fraud evidence can be gleaned from a business computer? Probably more than you think, if an expert does the research. Even if fraudsters have deleted documents and e-mails and reformatted hard drives, a surprising amount of data still remains in various digital hiding places.

Computer forensics can help resolve fraud cases involving bankruptcy, embezzlement, harassment, and theft of trade secrets and other intellectual property. Forensics experts also can provide evidence needed to discipline or suspend problem employees and resolve contract disputes.

What kinds of information retrieval are we talking about? Some examples:

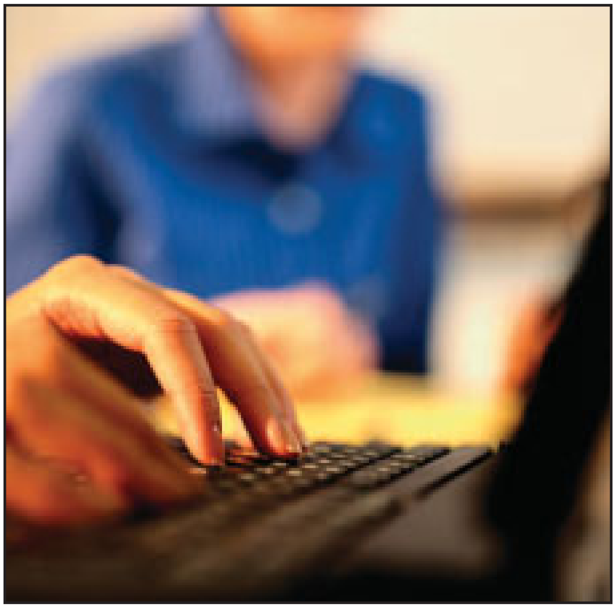
- Temporary or hidden files,
- Deleted files and e-mails,
- Data from reformatted or damaged drives,
- Information from encrypted or password-protected documents, and
- Search engine results and Web sites visited.

For the most part, courts are willing to accept digital evidence. The problem is that companies lack the knowledge, technical skills and time to sift through large amounts of information to find and extract key data that will be admissible in court. This is where a computer forensics expert can help.

Preparing the way

In computer forensics, preparation is key. Companies that want a forensics specialist to provide quick and effective service when needed should prepare before they suspect any problem. Follow solid day-to-day practices regulating employee computer use.

Have your legal counsel write an "acceptable use" computer policy. All employees should know that what they do on company computers is not private and that you may monitor and inspect past, present and future computer activity without notice. And if they connect remotely to the company's system from computers in other locations, your employees should know that you own all data and communications generated in these activities.



Checking configuration

Next, determine if your computer system is configured to provide data needed in a forensic examination quickly and easily. Ensuring that it is can save time and money later, and help preserve important evidence.

Surprisingly, the average computer system is capable of delivering data needed for most computer forensics procedures — but its capacities are often disabled.

Today's networks have extensive logging and auditing capabilities useful in a forensics investigation, but to save data storage space, many businesses don't set these functions to operate automatically. Some even turn them off entirely. Either policy is unwise if you have any reason to foresee a computer forensics investigation.

To be sure your system is set to help in any investigation, have a consultant review its logging and auditing capabilities, set them properly and check them regularly to detect possible tampering.

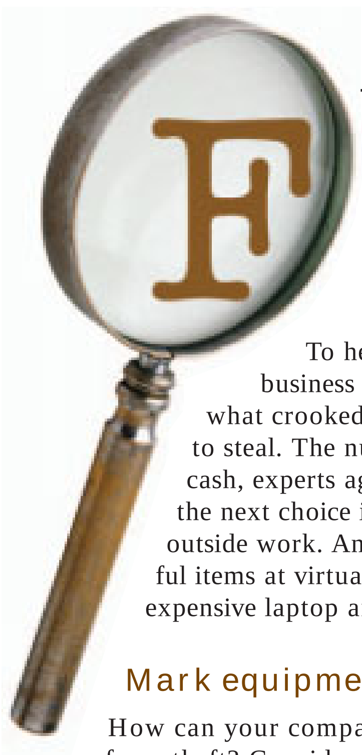
Assisting the investigation

If you suspect computer fraud, immediately stop all use of the affected system and call in a computer forensics investigator. After a preliminary analysis, the expert can evaluate potential evidence and tell you how to establish a custody chain to ensure that the data will be admissible in court with minimal business disruption.

Any time that litigation or a criminal investigation looms, quick action is important. With every day that passes, valuable evidence may vanish. So for best results, shut down the system at the first suspicion and get a computer forensics expert to work quickly.

Finding the evidence

If you suspect fraud, call in forensic investigators quickly to preserve evidence. In addition to recovering and evaluating evidence, they can assist with analysis and courtroom presentation and serve as expert witnesses.



Fraud to watch for:

Protect computers from employee theft

To head off employee theft, business owners need to know what crooked employees are most likely to steal. The number one preference is cash, experts agree, but if that's off limits the next choice is something they can use outside work. And, of course, the most useful items at virtually all companies are expensive laptop and desktop computers.

Mark equipment

How can your company protect its computers from theft? Consider adding security plates and indelible markings. These additions can help to track stolen equipment, inhibit resale and discourage theft.

Security software also can track a stolen computer using the Internet. As soon as the thief connects, the software contacts the security firm's monitoring system, which traces the machine's location using caller ID tools.

Fasten it down

To keep laptop and desktop computers where they belong, you can lock them down with cables and attach motion sensor alarms. You can even secure a desktop computer's keyboard and mouse with cables. If you store numerous laptops on your premises, consider locking them in heavy-duty cabinets or carts when not in use.

To further deter desktop computer theft, consider a locked steel case bolted to the desktop. If you prefer not to drill holes in furniture, you can attach super-strength adhesive security pads to desks or other furniture to keep thieves from lifting the equipment off the surface.

Security plates and indelible markings can help track stolen equipment, inhibit resale and discourage theft.

Keep it safe

You have numerous choices in fighting theft of computers — and other office equipment — but many companies don't take the time to investigate the possibilities. It's worth the extra effort to explore your options for adding extra security and keeping computers and other items where they belong.

Don't Let Fraud Ruin Your Business

Occupational fraud and abuse costs American businesses an estimated $600 billion annually — roughly $4,500 per employee. Small businesses are the most vulnerable to these crimes. But you don't just have to stand there and be victimized by them.

Let Rogers, Lynch & Associates LLC assist you in combating fraud and abuse. We offer a wide range of forensic accounting, and fraud-related services, including:

- Litigation Consulting and Support
- Expert (Witness) Services
- Fraud Detection and Deterrence
- Insurance Claim Analysis: Loss Profits, Business Interruption, Surety Bond Claims, Fidelity Bond Claims
- Divorce/Community property Partition
- Evaluation of Internal Control Systems
- Financial Statement Analysis and Interpretation
- Bankruptcy and Reorganization
- Asset Recovery
- Track and Locate Assets Misappropriated

Since our firm's founding in 1989, we have been committed to providing our clients professional service of the highest quality. Our clientele includes family and closely held businesses, public corporations, and commercial lenders throughout the United States.

We would welcome the opportunity to help you prevent, detect, or prosecute fraud. Please call us at 504-282-1441 or visit our Web site: www.rlastars.com, and let us know how we can be of assistance.

Patrick M. Lynch, CPA, CFE, DABFA, CrFA, CPCU, CLU, AIC
Managing member has over 30 years experience in fraud detection and deterrence and has testified as an expert witness in US Bankruptcy Court.

Penny Rogers, CFE, DABFA, CrFA
Managing member has over 20 years experience in fraud detection and deterrence and has testified as an expert witness in US Bankruptcy Court.

Rogers, Lynch & Associates LLC
Certified Public Accountants • Certified Fraud Examiners
Certified Forensic Accountants • Business Consultants
7051 Argonne Blvd. New Orleans, LA 70124
504-282-1441
www.rlastars.com