

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

VOLUME 6 NO. 6
JUNE 2004

YOUR SECRET WEAPON IN THE WAR ON FRAUD

IN THE NEWS

Gartner Weighs the Big Phish

Approximately 57 million Americans received E-mail "phishing" messages in the past year. More than 30 million were "absolutely sure" they were targets of a phishing attack. The remaining 27 million said they had received what "looked like" a phishing attack.

Problem for E-commerce companies: As the number of phishing victims continues to skyrocket, consumer confidence in Internet-based communications and commerce is being eroded.

Key finding: Nearly 11 million on-line adults—almost 20% of those attacked—have clicked on the link in a phishing attack E-mail. Of them, 1.78 million Americans, or 3% of those attacked, actually gave the phishers financial or personal information at a spoofed Web site.

Cost: Direct losses from identity theft fraud against phishing attack victims—including new-account, checking account and credit card account fraud—cost US banks and credit card issuers about \$1.2 billion last year.

Urgent now: Faster implementation of preventative solutions, such as digitally signed E-mail and managed anti-phishing applications.

White-Collar Crime Fighter source: Avivah Litan, Research Director, Gartner, Inc., leading IT researchers and consultants. She is author of *Underreporting of Identity Theft Rewards the Thieves*, a Gartner research analysis, www.gartner.com. Avivah can be reached at Avivah.Litan@gartner.com.

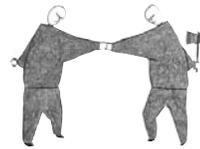
IN THIS ISSUE

- **DOCUMENT DANGER**
Outsmart high-tech forgers... 3
- **TERRORIST MONEY WATCH**
Wire transfers..... 4
- **GUARDING THE GOODS**
Inventory theft..... 5
- **THE CON'S LATEST PLOY**
Law-enforcement successes from around the country..... 7

Charles A Sennewald, CPP, and John K. Tsukuyama, CFE

THE NON-INTERVIEW

How to Interrogate Fraud Suspects



Much good advice has been published on the subject of effective interviewing technique for fraud investigators. But frequently, interrogation is the appropriate technique for getting to the truth in a fraud case.

Key difference: The person in the seat facing the investigator. In fraud-related interviews, the subjects are typically not, at the time of the interview, suspects in the case. They are witnesses or others who may have information pertinent to the investigation, but aren't believed to be directly involved in the crime itself.

Contrast: Interrogation involves questioning individuals who are already suspects. Interrogations inevitably become accusatory and are therefore commonly referred to as a "grilling" or the "third degree."

Result: In an effort to reduce the stress of these sessions, many law enforcement and corporate investigators have made a point of referring to *all* questioning sessions as interviews.

ESSENTIALS OF EFFECTIVE INTERROGATION

Seasoned investigators can switch easily between an interviewing approach and an interrogating one. In interrogation mode, basic rules of the game are...

• **Be physically prepared.** When setting the tone of an interrogation, your physical appearance makes a significant impression. Avoid distracting items such as lapel pins or fancy tie tacks...and especially a miniature handcuff tie tack!

Female interrogators should avoid wearing jewelry other than a finger ring, a

watch and a bracelet. No broaches, necklaces or conspicuous earrings.

Reason: In a tense interrogation session, you don't want your subject eyeing a piece of jewelry you're wearing and pretending to be interested in it by asking a disruptive question such as "What kind of stone is in that lovely necklace?"

• **Be substantively prepared.** Walk into the interrogation room knowing as much as possible about the subject's background. To establish your credibility, know where the person was born...schools he or she attended... details of work experience, family situation, etc.

Example: If you know that the subject's brother is a law enforcement officer, ask a question such as "What would your brother John the FBI agent think if he knew you were in this jam?" Giving the subject the impression that you know everything about him or her can be very disorienting, creating vulnerability that you can exploit with tough follow-up questions.

Also effective: If there is no file on the individual, create a phony one. Fill a file folder with lots of forms and printed reports...to reinforce the subject's impression that you are totally clued in to all aspects of his or her life.

The file also can serve as a useful "prop"—by giving you the opportunity to "review" the file when it is necessary to take a step back and collect your thoughts.

• **Commence the interrogation on a pleasant, low-key note.** During questioning, avoid a confrontational attitude as much as possible. This doesn't mean side-

stepping tough, penetrating questions. But avoiding heated arguments is essential for getting to the truth with guilty employees.

Best: Pleasantly introduce yourself and your partner or witness as agents of the company. Ask the subject to take the seat directly across from yours, and simultaneously take your own seat.

Important: The way you initiate your questioning will vary depending on the unique details of the case. But in most cases, the questioning should be started along such lines as...

"Mary—may I call you Mary? Good.

Mary, we have a very important subject to discuss...important to you and important to us. In fact, it might

be the most important discussion you've ever been engaged in. But, before we get to the subject, I'd like to ask you a couple of questions, okay?

"Are you sick in any way?"

Answer: "No."

"Are you thirsty?... do you need a glass

of water?"

Answer: "No."

"Do you have to use the restroom?"

Answer: "No."

"Good. One final point before we get started: Lying. You have my promise that at no time during our discussion will I lie to you. The issue we'll be addressing is too important for you to worry about me deceiving you. But at the same time, I'm asking you to be completely truthful with me as well...no matter how much the truth hurts. Do you understand that?"

Interrogation involves questioning individuals who are already suspects

Establish an atmosphere of conciliation. This phase of the interrogation

comprises a series of benign questions about the subject's job...as well as a few innocent questions about his or her off-the-job activities.

Aim: To evoke "yes" answers and thereby establish a pattern of saying "yes." This often makes it easier for your subject to provide truthful answers to the real questions.

Build on admissions of guilt. As is widely known, most guilty employees want to confess their wrongdoing. Good interrogators know how to be patient in order to earn the respect of the subject, thereby enhancing the chances of getting an initial confession.

Strategy: Once the interrogation moves into the "tough question" phase, gradually "turn up the heat" with harder and harder questions...and use some theatrics, such as standing up when you hear a contradiction while asking, "Do you realize what you just said...?" These tactics are a good way to progress toward the confession you need.

Critical: Once you get that initial admission, coax more from the suspect.
Example:

Employee: "OK, you've got me now. I put the carton of CD players in my trunk just before I locked up for the night.

Interrogator: "What made you do that?"

Employee: "I just needed the money."

Interrogator: "How much did you get for the carton?"

Employee: "\$200 bucks."

Interrogator: "Who gave you the \$200?"

Employee: "A guy named Willie. I don't know his last name."

Interrogator: "Did you know Willie wanted to buy before you took the car-

WHITE-COLLAR CRIME FIGHTER

Editor

Peter Goldmann

Consulting Editor

Jane Y. Kusic

Managing Editor

Juliann Lutinski

Senior Contributing Editor

Linda Stockman-Vines

Associate Editor

Barbara Wohler

Design & Art Direction

Ray Holland, Holland Design & Publishing

Panel of Advisers

Credit Card Fraud

Barry F. Smith, BFS (Bankcard Fraud Solutions), Inc.

Forensic Accounting

Steven A. Pedneault, Manager, Forensic Accounting Services, Haggett Longobardi & Co., LLC

Victim Services & Support

Debbie Deem

Financial Crime Victim Advocate

Corporate Fraud Investigation

Barry Brandman, Danbee Investigations

Corporate Integrity and Compliance

Martin Biegelman, Microsoft Corporation

Securities Fraud

G.W. "Bill" McDonald, Investment and Financial Fraud Consultant

Prosecution

Phil Parrott, Chief Deputy District Attorney

Denver District Attorney's Office, Economic Crime Unit

Computer and Internet Investigation

Donald Allison, Senior Consultant Stroz Friedberg LLC

Public-Private Sector Cooperation

Allan Trosclair, Former Executive Director, National Coalition for the Prevention of Economic Crime

White-Collar Crime Fighter (ISSN 1523-0821) is published monthly by White-Collar Crime 101, LLC, 213 Ramapoo Rd., Ridgefield, CT 06877. www.wccfighter.com. Subscription cost: \$275/yr. Canada, \$299. Copyright © 2004 by White Collar Crime 101, LLC. No part may be reproduced without express permission of the publisher.

Mission Statement

White-Collar Crime Fighter provides information of maximum practical value to organizations and individuals involved in all facets of investigating, detecting and prosecuting economic crime.

This community includes law enforcement officers...regulatory officials...corporate security professionals...business owners and managers...private investigators...and many more.

The editors of *White-Collar Crime Fighter* strive to gather and compile the most useful and timely information on economic crime issues.

Comments, suggestions and questions are welcome. Please fax us at 203-431-6054, or E-mail us at editor@wccfighter.com. Visit us on the Internet at www.wccfighter.com.

Dos and Don'ts of Effective Interrogation

Do use silence as a weapon. Ask a direct question and then wait for the response. The silence may seem lengthy, but it is shaking the foundation of the subject's emotions to whom it feels like an eternity.

Do keep questions short.

Do ask only one question at a time.

Do question responses that don't seem quite right.

Do avoid giving away critical information.

Don't make promises of any kind.

Don't lose your patience or persistence.

Don't show surprise at any answers.

Don't use profanity. Avoid lowering yourself to the level of the subject. Instead, insist that the subject refrain from use profanity as well.

Don't be a big shot. Arrogance can undermine your attempt to earn respect from the subject and make it difficult to elicit truthful answers.

Don't lie.

Don't lose your temper. If you do, you blow your credibility and probably the whole interrogation as well.

ton, or did you take the carton and then look for a buyer?

Employee: "Willie and me already had talked about it. In fact it was his idea, because he said they're easy to sell."

Key: The longer you can keep this dialogue, the more useful details you'll collect for your investigators. It's remarkable sometimes how willingly guilty people will open up with valuable details once you've gotten an initial confession and launched into the "discussion" about details. ⚖️

White-Collar Crime Fighter source:

• Charles ("Chuck") A. Sennewald, CMC, CPP, independent security management consultant and founder of the International Association of Professional Security Consultants, www.iapsc.org.

• John K. Tsukuyama, CPP, CFE, Executive Vice President, Safeguard Systems, fraud and security consultants, Honolulu, HI, www.safeguardhawaii.com. They are co-authors of *The Process of Investigation*, 2nd Edition, Butterworth-Heinemann, www.bh.com, on which this article is partially based.

Sennewald and Tsukayama on: Deceptive Interrogation Tactics: Playing With Fire

As explained above, corporate investigators must establish an atmosphere of honesty in the interrogation room before the questioning begins. Promising never to lie to a subject, and obtaining the subject's mutual commitment to truthfulness are essential.

Here's why: Many law enforcement officers are taught that deceptive interrogation methods are acceptable within certain limits.

Key: When an interrogating law enforcement official testifies at a fraudster's trial, the jury usually accepts the admission of having used deceptive tactics as standard operating procedure for officers seen as simply trying to do their jobs.

But—when a corporate security officer uses such tactics while interrogating a suspected employee, he or she risks incurring the jury's displeasure with what they may perceive as a heavy-handed, greedy corporation's no-holds-barred practice of browbeating employees into confessions.

This jeopardizes the company's chances of winning cases against suspected internal fraudsters, and potentially puts the company at risk of counter-suits in civil court.

DOCUMENT DANGER

Katherine M. Koppenhaver
Forensic Document Examiners

Outsmarting Today's High-Tech Forgers & Counterfeiters



In the past decade, the proliferation of computer equipment and sophisticated graphics software has greatly simplified methods of creating forged and counterfeit documents.

Desktop publishing in particular has become a standard tool for fraudsters to create near-perfect counterfeit documents—from letters of credit to counterfeit checks to bogus wills and more. Moreover, the equipment is cheap. Hardware that used to be available to only a few well-to-do criminals is now affordable for fraudsters of modest means.

Example: Magnetic ink printers are now obsolete. But anyone, including counterfeiters and forgers, can use magnetic ink in their own printers. Presto, a powerful fraud tool for penies which can exploit the fact that banks, money order providers and many other businesses and government agencies use magnetic routing numbers to sort their financial documents and confidential forms.

THE ALL-POWERFUL PC

Bank robbers and counterfeiters/forgers don't have very much in common aside from the fact that they are all bad guys. But one other thing they do share is the need for weapons. The only difference there is that the bank robber's weapon of choice is concealed on his person, while the counterfeiter's plugs into the wall.

As has been widely reported, the personal computer is a powerful publishing tool when coupled with the right software and a high-resolution printer. It can store logos as well as type in all sizes and styles. With bank safety paper purchased at a local stationery store, literally anyone can copy

and print a legitimate check with a little practice. When you add basic word processing software such as Microsoft Word and a graphics application like Adobe PhotoShop to the arsenal, all a fraudster needs to start generating bogus documents is a little brainpower and a lot of desire to learn how to use these tools.

THE SKY IS THE LIMIT...

I have worked with people at many organizations that have been victims of forgery and counterfeiting who are stunned when they find out a particular document has been illegally reproduced. Naively, they wonder how and why someone would alter or counterfeit such documents as...

- Letters of recommendation
- Expense account receipts
- Diplomas
- Business contracts
- Letterheads used in business transactions

On the banking side, where forgers and counterfeiters have run amok for decades, the new technology has only enhanced the ease and reduced the cost of creating phony but authentic-looking corporate checks...cashier's checks...certified checks...letters of credit...and other negotiable instruments.

And don't forget such documents as property records, insurance claims, passports, birth records and college transcripts (yes, ambitious 20-somethings are getting into the forgery business too).

DEFENSIVE CHALLENGES

Many companies now print their own checks with computers that use

Continued on pg. 4

TERRORIST MONEY WATCH

TERRORIST WIRE TRANSFERS

Beware of New Approaches

Money laundering experts and government agencies have long known about terrorists' use of wire transfers to fund their murderous activities. Such common practices as using false identities, "straw men" or front companies in transactions to avoid detection are widely familiar, as is channeling funds through multiple financial institutions to make transfers appear to come from seemingly unrelated sources.

But—as usual—the bad guys are one step ahead. *Here are examples of recent innovations in terrorist wire transferring...*

Case 1: Terrorist funds collected in Country A transferred to a terrorist organization in Country B. **A terrorist group in Country X used wire transfers to move money to Country Y for purchasing components for explosives**

A terrorist organization used its overseas contacts to "tax" the expatriate community on their earnings and savings. The tax went to a "calling fund" and was then wired to one of the organization's representative offices, which happened to be the political wing of a terrorist group based in a neighboring country.

The neighboring country maintained a cross-border network of contacts in the "target" country, and weapons were purchased and smuggled across the border where the terrorist group carried out its attacks.

Case 2: Terrorist organization uses "clean" names to transfer money for its activities across borders. A terrorist group in Country X was found to be using wire transfers to move money to Country Y that was eventually used for paying rent for safe houses, buying and selling vehicles, and purchasing electronic components for building explosive devices. The organization used "bridge" or "conduit" accounts in Country X as a means of moving funds between countries. The accounts at both ends were opened in the names of people with no apparent association with any terrorist organiza-

tion, but who were linked to one another by family or similar ties.

These connections provided a cover of legitimacy for the transfers between them.

Result: Cash deposits were made by the terrorist into bank accounts from which the transfers were made. Once the money was received at the destination, the "holder," posing as a family member, either left it on deposit or invested it in mutual funds where it remained hidden and available for the group's future needs.

Sometimes the money was transferred to other bank accounts managed by the terrorist group's "financial manager" who also served as paymaster for the purchase of equipment and materials or to cover other expenses incurred by the group in its clandestine activities.

Case 3: Wire transfers used as part of a terrorist fundraising campaign. An investigation in Country A of Company Z, a company thought to be involved in smuggling and illegal distribution of pseudoephedrine, a chemical used in the production of methamphetamine, revealed that employees of Company Z were sending a large number of checks to Country B. Additional evidence revealed that the target business was acting as an unlicensed money remitter.

Search warrants were obtained for the Company Z premises and two residences. Analysis of the documents and bank records seized indicated that the suspects had wire transferred money to an individual with suspected ties to a terrorist group. 

White-Collar Crime Fighter source: *Financial Action Task Force on Money Laundering*, the international anti-money laundering arm of the Organization for Economic Cooperation and Development (OECD), www.fatf-gafi.org.

Continued from page 3

check kits that include special software and safety paper.

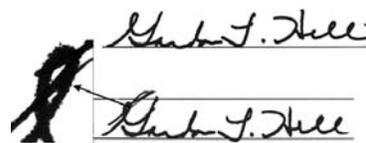
Problem: Genuine documents cannot be distinguished from phony ones when the same method is being used to create both kinds of documents.

Fraudsters will scan complete documents into their computers, then alter them in literally any way they want. In other situations, they scan signatures onto contracts fraudulently committing the victim to large payments.

Challenge: Since the perpetrator is using an original, genuine signature, the victim is always puzzled by the appearance of his/her legitimate-looking signature on the phony document. Only high-tech magnification will prove that the writing is a copy.

CASE STUDY

Gordon Hill was the victim of a forger who scanned and printed Gordon's signature onto a promissory note for \$50,000. The forger placed the signature onto the contract in two places. He was unable to avoid slight alterations to the signature, but wasn't concerned, knowing that no one's signature is exactly the same every time they write it. His efforts were uncovered when a document examiner studied the signatures under magnification and discovered tiny dots along the edge of the signature—the product of a computer printer, not an ink pen, as shown in the illustration below.



Added high-tech challenge: Today's low-end color photocopiers are good enough for forgers to duplicate their handiwork or make high-quality copies of legitimate financial documents. Color copies can often be identified by the different-colored dots under magnification, but copier technology is improving, making it increasingly difficult to differentiate an original from a copy.

LATEST DEFENSIVE MEASURES

How can you and your employees spot a computer forgery before it's too late? *Effective...*

• **Compare documents.** It's often easy to flag a bogus document when you have the original for comparison. If you suspect a forgery, examine the

Continued on page 5

Continued from page 4

alignment of the print. Genuine documents are professionally typeset, while counterfeits are not.

- **Do the “flake test”.** To determine if a questionable document is a phony laser copy, make a sharp fold over some of the type and scrape the edge of the ink line. If it flakes, it may be toner from a laser printer instead of ink. While this is not always a sure sign of counterfeiting, genuine, negotiable instruments are created on offset printers and are not computer-generated.

- **Use non-standard safety paper.** The US Bureau of Engraving and Printing has introduced polyester threads in the paper used for printing currency, to prevent color copiers from simply running off photocopies of authentic cash.

Though this is very costly, large companies can come close to this

Fraudsters will scan complete documents into their computers and then alter them in literally any way they want

level of security by ordering non-standard safety paper and restricting the supplier’s right to use the same pattern elsewhere.

- **Use tamper-proof paper and/or special ink to prevent forgeries.** Offset-printed forms are harder to duplicate than computer-generated forms. Papers are being manufactured with artificial watermarks that can be seen at an angle but cannot be copied by a scanner. Visit www.kantcopy.com.

- **Keep supplies and software in a secure environment to prevent employees from gaining access to the equipment needed to perpetrate document fraud.**

- **Split up job responsibilities.** One employee should write out the checks and a different person should reconcile the account. The same holds for all other functions involving the disbursement or receipt of checks or other financial instruments.

White-Collar Crime Fighter source:

Katherine M. Koppenhaver, President, Forensic Document Examiners, Joppa, MD, www.forensicdocumentexaminers.com. Katherine is one of the best-known forensic document examiners in the country, having provided services to many Fortune 500 companies and major government agencies. She also is President of the National Association of Document Examiners (NADE), www.documentexaminers.org. Katherine can be reached at ForDocExam@aol.com.

GUARDING THE GOODS

INVENTORY THEFT

Investigative Secrets for Accountants



When a company suspects that a current or former employee has stolen inventory, it can sometimes be difficult to determine whether the suspicions are valid, and if they are, to document and prove the theft.

Reasons:

- Companies often give too many employees access to inventory... and/or neglect to remedy their inadequate record keeping “systems.” The results can be an invitation to commit fraud...or just unchecked vulnerability to costly record-keeping errors.

- Some companies perform a complete inventory only once a year, or use haphazard methods if they count more often. Again the result can be theft or record-keeping blunders.

The bottom line: Management usually has no clue how much inventory the company should have at a given time. Or—if inventory is missing, executives are hard pressed to prove whether it was stolen...or whether their own neglect of internal controls was to blame.

THEFT VERSUS ILLUSION

Before assuming that theft has occurred, your accountant should always determine whether the assets were really stolen, because they may have been on the premises all along... shipped out to customers...or never delivered.

Example: Weak physical controls can cause big mistakes in recording items taken from storage. A company without a location assignment for each item, an effective method of keeping tabs on overflow stock or even a well-run returns system might have caused inventory to be misplaced.

Other conditions that can give the

appearance of inventory theft are short vendor shipments nobody notices because of lax receiving and inspection procedures...and unobserved vendor overcharges.

Even worse, some companies simply fail to bill customers for shipments because the shipping and billing functions don’t work in tandem.

IDENTIFYING THE PROBLEM

In cases where the missing inventory is not located or accounted for, many companies ask their accountants to start by checking their receiving and inspection procedures before concluding that a theft has taken place.

Key: If sifting through haphazard financial records doesn’t explain the inventory shortage, your accountant will usually look for signs that fraud is occurring.

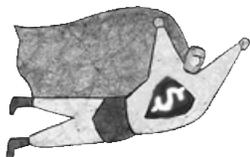
Example: Companies with poor purchasing, receiving and cash disbursement controls are at serious risk of inventory theft. One person performing multiple duties can both commit and conceal fraud.

If he or she believes that existing controls—or lack of them—led to theft, your accountant should begin combing the records for clues. Anything that doesn’t follow established inventory standards can raise a red flag. **Examples:**

- Odd journal entries posted to inventory.
- Unusually large declines in gross margin.
- Sudden problems with out-of-stock inventory.
- Unusually large account adjustments after staff performs a physical count.

Continued on page 6

**FRAUD-FIGHTERS'
NEED-TO-KNOW
HOT LINE**



The Flip Side of Insurance Claims Fraud

Corporate investigators, SIUs and law enforcement fraud specialists must be alert to a new trend in corporate insurance fraud: Workers' comp premium fraud. *How it works:*

- Misrepresenting that employees are working safer jobs than they actually are.

Examples:

- A roofing company said its roofers were clerical and sales employees.
- A construction firm dodged \$1 million in workers' comp premiums by classifying its roofers as "supply dealers."

• Keeping employees off the books. "Hiding" employees is a quick-and-easy way to engineer a lower worker's comp premium.

Example: A now-defunct painting company scammed its worker's comp insurer out of \$3 million by stating that more than 100 employees were independent contractors.

• Creating convoluted premium scams. A security firm perpetrated a double-whammy scam. First, it reduced comp premiums by lowballing the number of guards posted at public housing buildings in its contract with the city housing authority. They then inflated the number of guards for which they billed the city... though many buildings had no guards at all. The company not only cut its comp premium, it *profited* from the second part of the fraud.

Self-defense: Internal awareness. One large insurer has introduced an on-line training course in worker's comp premium fraud for all employees involved in underwriting. The course will include actual scenarios of premium frauds as well as awareness training for detecting suspicious signs of possible premium fraud.

White-Collar Crime Fighter source: James Quiggle, Director of Communications, Coalition Against Insurance Fraud, www.insurancefraud.org. Jim can be reached at jamesq@insurancefraud.org.

Who's Supposed to Be Doing What In Fighting Corporate Malfeasance

Confusion about the proper roles of a corporation's top management, its board of directors and its independent auditor in combating fraud is, unfortunately, a common syndrome in the era of corporate mega-wrongdoing.

To help define anti-fraud roles and responsibilities for key executives, PriceWaterhouseCoopers analyzed numerous scandals and determined that the dizzying varieties of business fraud can actually be segmented into six distinct categories...

- Fraudulent financial reporting, comprising frauds arising from improper revenue recognition... overstatement of assets or understatement of liabilities.
- Misappropriation of assets, including embezzlement... payroll fraud... external theft... procurement fraud... counterfeiting or product diversion.
- Improper expenditures or liabilities, such as commercial or public-sector bribery.
- Fraudulent acquisition of revenues or assets, defined as overbilling or product substitution against third parties... or employer fraud against employees.
- Fraudulent avoidance of taxes.
- Financial misconduct by senior management, encompassing the endless varieties of big-dollar misconduct as defined by PCAOB Auditing Standard No. 2.

Who does what: Professional auditing standards (SAS 99) now require independent auditors to examine two of these six areas—fraudulent financial reporting and misappropriation of assets.

Senior management and the audit committee, by contrast, are responsible for *all* six categories.

White-Collar Crime Fighter source: *The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks*, report by Internal Audit Services, PriceWaterhouseCoopers, http://pwc.com/images/gx/en_g/about/sv_cs/grm_s/TheEmergingRole.pdf.

Continued from page 5

Next step: Having found one or more red flags of inventory theft, your accountant will most likely try to establish sufficient evidence to prove that fraud is in fact the explanation for the shrinkage.

SEARCHING FOR EVIDENCE

Inventory fraud often leaves a paper trail, which enables forensic accountants to screen journal entries for unusual patterns.

Example: An entry recording a physical count adjustment made during a period when no count was taken obviously is cause for suspicion.

Your accountant should probe further by tracing all unusual entries to supporting documents (assuming they exist).

Important: Financial records

Management usually has no clue how much inventory the company should have at a given time

aren't the only "paper" evidence. Vendor lists sometimes reveal suspicious patterns, such as post office box addresses substituting for street addresses... vendors with multiple addresses ... and names closely resembling those of known vendors.

Key: Even if he or she has found no evidence of bogus vendors, your accountant should look at all vendor invoices and purchase orders for anomalies.

Examples:

- Unusually large invoices or alleged purchases with no record of delivery of goods.
- Discrepancies between the amounts due per invoice, the purchase order and the amount actually paid.

Your accountant should also fully analyze the cost, timing and purpose of routine purchases and flag any that deviate from the norm.

WATCH WHAT'S GOING ON

Whether employees or an outside firm counts inventory, an accountant, auditor or inventory expert should carefully observe warehouse activity once employees realize a count is imminent.

What to watch for: Fraudsters may make frenzied attempts to shift inventory from another location to

Continued on page 7

Continued from page 6

substitute for missing items they know will be discovered.

Inventory at remote locations also can disappear, so your accountant should confirm quantities with the storage facility or go with someone from your company to personally inspect them. In pinning down suspected theft, it's best to do the count in person rather than delegate the job to a possible fraudster. **WJ**

White-Collar Crime Fighter source:

Craig L. Greene, CFE, CPA, partner in charge of financial investigative services for McGovern & Greene LLP, Certified Public Accountants and financial fraud prevention consultants, Chicago, IL. www.mcgovernandgreene.com. Craig can be reached at craig.greene@mcgovernandgreene.com.

Fraud-Finding Clues: New Report Shows Most Internal Fraudsters Are "Loyal" Male Employees

An assessment of 100 fraud cases that KPMG investigated in the past two years showed that most perpetrators are male employees, often with long periods of service with their companies.

Details: One-third of internal fraudsters studied had been working for their companies for between 10 and 25 years. And—72% of the total were male.

Important: Contrary to common belief, most internal fraudsters commit their dirty work with accomplices rather than alone. In more than one-half of all the cases analyzed, two to five parties were involved in the fraud, compared with only one in three cases carried out solo.

Lesson: The often surprising number of people involved in some of the cases indicates that fraud can be endemic within some departments with especially weak controls...and consequently more difficult for outsiders to detect. One case involved 207 co-conspirators.

Key finding: Corporate finance departments appear to be the most commonly targeted business areas...with procurement coming in second.

The age factor: The largest age group of ringleaders in the cases analyzed was 36 to 45 (41% of cases) Another 29% of cases involved perpetrators aged 46 to 55. Young employees (under 25) accounted for only 1% of total fraudsters.

Information: KPMG LLP, UK member firm of KPMG International, www.kpmg.co.uk.



THE CON'S LATEST PLOY...

From *White-Collar Crime Fighter's* files of new scam, scheme and rip-off reports

New Haven, CT

Doing nothing about a known fraud can be hazardous to your freedom and your wallet. A. Robert Palmer, former CEO of Eastern Coloring Printing, an Avon, CT-based commercial printing firm, pleaded guilty to a one-count federal Information charging him with misprision (neglect) of a felony.

The case: Palmer confessed that he was aware of, but failed to report to law enforcement, a check kiting scheme being perpetrated by David Lackenby, the company's chief financial officer.

Palmer acknowledged that he knew that thousands of worthless Eastern Color Printing checks were being exchanged between the company's operating and draft accounts, and that the balance in those accounts was not sufficient to cover the face value of the checks.

The former executive also acknowledged that he had tried to conceal the scheme by delaying financial auditors from gaining access to the company's books and records, and that he neglected to notify law enforcement as soon as he became aware of the crime. The company's bank reported losses of approximately \$2.2 million as a result of the scheme.

Palmer faces up to three years in prison, a term of supervised release of up to one year and a fine of up to \$250,000.

Fort Wayne, IN

Could this have been a terrorist financing operation? A federal judge sentenced Khaled Al Raffai, a Jordanian national, to 21 months in prison and payment of \$61,615 in restitution for his role in embezzling \$1 mil-

lion from Western Union.

Details: Raffei is the first of five Jordanians charged in a scheme to open Western Union franchises in small convenience stores in northern Indiana and Illinois ...and to wire more than \$1 million in bogus money orders to other Western Union locations without having deposited the cash to complete the transactions.

Khaled and his four co-conspirators had individuals pick up and cash the fraudulent money wires before the illegal transactions were discovered. The money reportedly disappeared in Germany, Jordan, Lebanon and Turkey over the past two years.

The government presented evidence that Raffai had opened a Western Union franchise in Burbank, IL, to perpetrate the bogus money order scheme.

There are no confirmed reports that Raffei and his co-conspirators have ties to terrorist organizations. But Raffai's lawyer, Charles Stewart Jr., in a plea for leniency, claimed in court that there is evidence Raffai had helped federal agents before and after the September 11 terrorist attacks to develop information on other Middle Eastern individuals living in the United States.

Co-defendants Yousef Zriakat and Kefah Makamreh pleaded guilty earlier and are awaiting sentencing. Two additional co-defendants are still at large...more than 12 months after their indictments.

Montgomery, AL

Case indicates connection between depression and fraud. Bobbie Jean Grant, the former city clerk of Moulton, AL, was sentenced to three years in prison and ordered to receive treatment for

depression following her guilty plea in a check forgery case. She was also ordered to pay \$66,193 in restitution to the town.

Details: Grant forged the town Mayor's signature on an extra pay-check she fraudulently made out to herself.

Though she pleaded guilty specifically to that single forgery, the restitution ordered covers the total amount of money related to earlier charges that were dismissed concerning 11 other alleged check forgeries from the clerk's office over three years.

The dismissal was conditional upon Grant's guilty plea and agreement to pay the full restitution.

Hillsboro, OR

HHealth-care fraud of the very dangerous kind. Dr. Steven Moos, a medical doctor of "lifestyle" medicine, and Dr. Thomas Holeman, an employee at Moos's Frontier Medical Clinic, were sued by the Oregon Department of Justice (DOJ) on a variety of charges relating to illegal medical practices.

Background: In 2000 the Oregon Board of Medical Examiners (BME) placed Dr. Moos on 10 years of probation for illegally advertising and selling prescription drugs over the Internet.

The BME later learned of Moos's ear-

lier indictment for illegal drug use and a criminal investigation in California related to practicing medicine without a license.

Moos' Oregon medical license was suspended by the BME in early 2003.

When the BME referred the Moos case to the Oregon DOJ, a joint investigation with the US Food and Drug Administration's Office of Criminal Investigation was initiated.

Key: Oregon and the FDA along with other state and federal agencies are members of the International Interagency Health Products Fraud Steering Committee that promotes multi-agency cooperation in the prosecution of health-care fraud.

During the Moos investigation, DOJ was informed that the FDA was already conducting a parallel investigation of both Moos and Holeman. The two agencies then collaborated in a joint probe of the two suspects' activities.

Results: The state's prosecution of the doctors states that they violated state and federal laws by advertising and selling "Viaglide," a female arousal cream, over the Internet, when the "product" actually contained nothing even close to Viagra. The doctors were also charged with illegally selling the bogus drug without a prescription and without taking a medical history of prospective users, as required by law.

It gets worse: The MDs were also charged with prescribing, promoting and selling Human Growth Hormone

(HGH) by misrepresenting that it was a harmless panacea for the effects of aging.

Little Rock, AR

Collect calling scheme draws ire of state attorneys general. The State of Arkansas joined Minnesota and Illinois in suing a company called 00 Operation, or "Double-O Operator" for trying to scam businesses through fraudulent bills and threats.

Details: Investigators in Arkansas Attorney General Mike Beebe's office discovered that the Sarasota, FL-based company had a contract to sell Internet marketing services by phone for another company, American Directory Services of Nevada. Under the agreement, 00 Operator would place collect calls to businesses, then offer the services once the collect-call charges were accepted.

Businesses then received bills for \$22.42 (\$28.84 in Illinois, Minnesota, Iowa and Texas) purportedly to cover the cost of the sales calls. The bills were marked "Final Notice," and the company threatened to shut off phone service to the businesses if the bills were not paid.

According to 00 Operator's own records, at least 69 Arkansas companies paid these bills. But in Minnesota, 9,200 attempted calls to businesses resulted in 900 companies being billed. In Illinois, the collective damage was even greater, with more than 3,000 businesses getting fraudulently billed for a total of more than \$80,000.

Arkansas, along with Illinois and Minnesota, filed formal suits against 00 Operator, while Montana, Wyoming and others issued alerts to businesses.

COMING SOON IN

White-Collar Crime Fighter...

- Procurement fraud: Expert preventative advice
- Whistleblowers: How to encourage honest employees to speak up
- New anti-fraud tool: Unofficial task forces
- Forensic accounting: How to stop earnings manipulation before it's too late



YES! I want to save \$50 on a one-year subscription to **WHITE-COLLAR CRIME FIGHTER!** By subscribing now, I'll get the money-saving introductory subscription rate of \$225. **That's \$50 off the regular subscription price of \$275!**

Plus, send me—for **FREE**—FIVE Special Reports on preventing, detecting and investigating fraud threatening MY organization.

Payment enclosed (or) Charge my Visa Mastercard AMEX Discover Bill me

Card # _____ Expiration date _____

Signature _____

Name _____

Affiliation _____

Address _____

City _____ State _____ Zip _____

Call 1-800-440-2261...Or Fax this order form to: 203-431-6054

Or subscribe on-line at www.wccfighter.com.

Or mail this form and your check to: White-Collar Crime Fighter, 213 Ramapoo Rd., Ridgefield, CT 06877. You can contact White-Collar Crime Fighter by E-Mail: subscribe@wccfighter.com