

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

VOLUME 6 NO. 9
SEPTEMBER 2004

IN THE NEWS

Reconstructing Iraq: Not Without Fraud

The Coalition Provisional Administration (CPA) in Iraq, which was dissolved after the handover of sovereignty in June, and was responsible for overseeing multi-million US-sponsored reconstruction projects, reported fraud in several of the awarded contracts.

Details: In the less than six months of its operation, the CPA's Office of Inspector General opened 69 cases of fraud, waste or abuse by contract recipients doing reconstruction work in Iraq. Several remain unresolved.

Examples: One case involved a senior CPA advisor who manipulated the contract-award system to have a \$7.2 million security contract awarded without going through the required bid process. The award contained an "advance payment" of \$2.3 million.

In a less brazen, albeit more amusing case, the Iraqi Ministry of Interior appointed a DoD civilian as a coach for an Iraqi amateur sports team. The Ministry advanced the coach \$40,000 to take the team to competitions in other countries, and the coach gave the funds to his military assistant. While at a sporting event, the assistant gambled and lost some the money, which was then written off as a legitimate loss.

White-Collar Crime Fighter source:

Quarterly Report of the Office of the Inspector General, Coalition Provisional Authority, US www.cpa-oig.org

IN THIS ISSUE

- **INTERNAL FRAUD ALERT**
Strategies for growing economy... 3
- **CASE STUDY**
Why fraud awareness works... 4
- **SECURE OUTSOURCING**
Trusting management companies... 5
- **THE CON'S LATEST PLOY**
Law-enforcement successes from around the country... 7

George Heuston

Hillsboro (OR) Police Department

GEEKS WITHOUT GUNS

How High-Tech Security Whizzes Help Law Enforcement Fight Cyber-Crime



The majority of American police officers are unprepared to deal with crimes involving either the direct or indirect use of computers. No one in particular is to blame for that. It's just an unfortunate fact of high-tech life.

Current situation: The average state or municipal police officer receives little or no instruction in computer forensics during his or her time at the Police Academy.

The few existing local digital forensics labs are staffed by detectives who have been assigned to a high-tech crime unit with only limited specialized training.

Our solution: We recruit local private-sector high-tech security experts to support the local police with computer/Internet crime and digital forensics training. It sounds simple and it is. And it works.

Main reason: The local private sector professionals are eager to help the cops learn how to use computers to catch cyber-thieves, con artists, hackers and saboteurs.

THE "GEEKS-WITHOUT-GUNS" MODEL

We came up with a concept called Police Reserve Specialists (PRS)...a group of volunteers from the private sector with computer and high-tech security and forensics skills with two main functions...

- Train local law enforcement officers in computer forensics techniques...and raise awareness about the many kinds of high-tech crime that can and are committed by dishonest or malicious individuals armed with formidable computer skills.

- Actively assist police officers in investigating high-tech crimes.

This involves assisting police investiga-

tors in the entire investigative cycle—from preparation and execution of search warrants to preserving and analyzing digital evidence as well as providing expert testimony in court.

Where they come from: Being located near Intel Corporation, with six local campuses and 30,000 employees, we are fortunate to have a large pool of potential volunteers with state-of-the-art know-how about computer and Internet crime...digital forensics...information security and other information-age security matters.

LEGAL DETAILS

The PRSs serve as non-sworn agents of our local police department. They have clearly limited authority, defining when and where their specialized skills are needed. Specifically, all reservists work under the direction of a case officer—usually the detective in charge of the investigation. As agents of the police, PRSs act under the Fourth Amendment and all other statutory mandates governing police conduct and the search and seizure of digital evidence.

Important: For our private-sector technology volunteers, the goal is to use any and all available technologies to collect the evidence needed to nail the bad guys. However, not all technically feasible techniques can be legally used to collect evidence. For instance, it may not be legal to trace Internet connections to machines not specified in a warrant... even though it is possible to do so. That's why we have detectives manage our PRSs on actual cases...and why we train them to use "least intrusive means" to obtain evidence

within the scope of a warrant.

Result: By balancing the technological know-how of our volunteers about how to gather digital evidence...with the legal/procedural guidance of experienced law enforcement investigators, the PRS team can be extremely effective.

CASE STUDY

Recently two reservists were assigned to a felony fraud and forgery investigation. Our Hillsboro PD detective received authorization from the District Attorney's Office for PRS reservists to assist in the investigation.

Key detail: Because representatives from the DA's Office had participated in the PRS policing/legal training, they were confident the reservists would contribute to the case in a meaningful way.

The case began with a briefing attended by the detectives assigned to the investi-

gation, two PRS volunteers and the PRS management coordinator for the HPD.

The limits of the warrant and types of evidence the detectives were expected to find on the computer systems were outlined. After the briefing, both reservists went to the HPD Forensics Lab, where computers seized earlier in the case were being held.

The reservists, who had special skills in computer forensics, imaged the hard drives and with the guidance of the detectives, examined the drives in accordance with the terms of the search warrant.

The examination turned up forged documents and the programs that produced them. The police-reservist team's findings were documented—including a log of their procedures—in a report to the case detectives for use in prosecution.

The case was subsequently scheduled for trial.

GETTING STARTED

The concept of the PRS program was first presented by the Hillsboro Chief of Police at a meeting of a local organization called Computer-Related Investigations, Management, and Education (CRIME).

Founded in 1998, CRIME is made up of people from law enforcement, industry and academia who share an interest in computer security and digital forensics.

After the meeting, PRS program applications, resumes and letters of intent were solicited.

Twelve applicants were ultimately selected out of an initial group of 40. The group consisted of eight people from the computer/software industry...two with extensive legal backgrounds (one was in fact a former deputy district attorney)...three computer science academicians...and one retired business executive.

Acceptance criteria: The initial recruits were selected based on their technical expertise and their willingness to participate in formation of the program. Successful applicants had to be skilled in specific areas pertinent to fighting high-tech crime—such as hardware and software engineering, programming, systems networking and telecommunications.

Our PRSs commit to a minimum term of two years of service. Most spend some time in the forensics lab, especially as they become more involved in the program. Others, however, may only need to be available for a quick consultation or in crisis situations depending on their area of expertise

Over a 10-week period, the partici-

Three Cs of Financial Statement Fraud

Fraudulent financial reporting occurs for many reasons, most of which can be grouped into three categories—conditions, corporate structure and choice...or the "Three Cs." *Definitions...*

•**Conditions.** The motivations and pressures to engage in financial statement fraud. Pressures to meet analysts', shareholders or bankers' earnings forecasts are common conditions motivating financial executives to cook the books.

•**Corporate structure.** A business's corporate structure can increase the likelihood that fraudulent financial reporting will occur.

Common fraud-conducive structure: Lax or non-existent corporate governance policies and procedures...and ineffective internal controls and monitoring. When accompanied by top management arrogance...low ethical standards and deceptiveness, the probability of financial wrongdoing is substantial.

•**Choice.** Management may choose to cook the books when personal wealth is linked to the company's performance through profit sharing, stock-based compensation and other bonuses...when the chances of getting caught are considered low...and the opportunities for doctoring the numbers are clear.

The presence of any one of the 3Cs can signal the possibility that fraud has occurred...or will.

White-Collar Crime Fighter source:

The Three Cs of Fraudulent Financial Reporting, by Abihollah Rezaee, CIA, CPA, CMA, CGFM, CFE, Thompson-Hill Chair of Excellence and Professor of Accountancy for the Fogelman College of Business and Economics at the University of Memphis, published on the Institute of Internal Auditors Web site, www.theiia.org.

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

R.W. (Andy) Wilson, Wilson & Turner Incorporated

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.

pants receive practical training on police procedure and law, including search and seizure, evidence handling, chain of custody, court testimony, privacy issues, conflict of interest, ethics and communication.

Main objectives of the training...


- Teach the reservists enough about law enforcement procedures and technique so they know when to ask questions of the investigators while working a case.
- Train the reservists to provide the investigators with enough technical knowledge to ask the right questions of subjects and witnesses in the course of their investigations.
- Teach the law enforcement officers enough about technology so they are able to make best use of the reservists' high-tech skills.

- Maintain a two-way training process that raises the level of knowledge on both sides.

Important: In addition to actual investigative support, our PRSs participate in what we call a P2B Program—where they assist Hillsboro police personnel in conducting awareness and training sessions for businesses on the major high-tech crime threats facing business...and how to reduce risk.

SECRETS OF SUCCESS

From our experience, it is clear that the essential ingredients for successful creation of a PRS program include...

- Existence of an active group of people from industry and academia (such as our CRIME organization) with an existing line of communication with the local law enforcement community.
- Police department leadership committed to extending the department's activities and effectiveness beyond the traditional boundaries.
- Existence of ample local private sector technology talent. Intel's 30,000-employee operation in Portland has been an invaluable source of PRS talent for us. But you don't need an Intel in your backyard to build a PRS program. Virtually every community has some high-tech experts willing to volunteer time to fighting the new forms of fraud and cyber-crime threatening business and individuals. 

White-Collar Crime Fighter source:

George Heuston, JD, Project Manager, Hillsboro Police Department, Hillsboro, OR. Founder of the Hillsboro PRS program, George is a retired FBI Special Agent, with more than 15 years of experience in high-tech crime and investigations. He worked for 10 years in Silicon Valley, where he specialized in high-tech investigations related to foreign counterintelligence and industrial espionage. George can be reached at georgeh@ci.hillsboro.or.us.

INTERNAL FRAUD ALERT

Jonathan Turner, CFE, CII
Wilson & Turner, Incorporated

THE FRAUD CYCLE

Tighten Controls as the Economy Continues to Grow



Though the mega-frauds at Enron, Tyco, Worldcom and Adelphia didn't make the headlines until after the turn of the millennium, the schemes behind them were hatched long before then—during the late 1990s. It was a time of robust economic growth and prosperity following on the heels of recession—much like the economic climate today.

Significance: Because the incidence of embezzlement, inventory theft, vendor/employee schemes and other internal frauds tend to spike during good economic times, now is an especially important time to screen for red flags of fraud taking place in your organization.

WHERE TO START

Rule of thumb: Avoid the tendency to focus exclusively on segments of the business that are doing especially well during an economic upswing at the expense of other operations. The stress of trying to meet increasing customer demands can result in insufficient management oversight of other operations, making it easier for dishonest employees to steal without drawing attention from co-workers or bosses.

Example: One of our clients that was in a growth mode focused all of its attention on its \$400 million business unit—which had the most to gain from the current economic expansion...and let its \$10 million units run themselves. A small-group embezzlement scheme was perpetrated in one of the company's \$10 million units while management was looking the other way, and \$3.75 million was stolen.

SCHEMES HEATING UP

Depending on your company's stage

in its economic cycle, the fraud schemes you're looking for are either about six months old or are just getting underway. In other words, if your company has been in a strong growth phase for the last two or three quarters, chances are that opportunistic employees have been planning ways to rip you off for several months now. If you're just now beginning to undergo a business upswing, the internal scheming may be just beginning.

Detecting these schemes early is key: There's no such thing as a "small" fraud...schemes detected in their infancy are just big frauds that haven't been allowed to "grow up." *Now's the time to screen for...*

• **Fraudsters for hire.** Today's job-seekers are yesterday's laid-off workers. In a tight labor market, you may be interviewing candidates with leftover animosity from a previous job, grudges, feelings of entitlement...and financial pressures in the form of old bills that have been accruing interest.

Self-defense: Go beyond the standard background check, resume verification and reference check...and get into the applicant's head.

Example: Call his or her former employer and ask about the circumstances of his or her termination. Ask, "Was she angry?" "Did she make any threats?" "Did your company do anything to help her get a new job?" "Did she receive any severance pay?"

Useful measure: Take hiring personally: Don't hire someone you wouldn't leave alone with your children.

Also key: Think "location, location, location." Consider where you're putting new hires' desks. Are they near

Continued on pg. 4

CASE STUDY

Why Fraud Awareness Works



A construction company's project manager engineered a simple scam that earned him about \$250,000 before he was caught.

His story underscores an essential truth about white-collar crime: Fraudsters almost always slip up. *Details:*

- The project manager opened a bank account using a name similar to that of the construction project he was managing. He told the bank that the account would be used for miscellaneous field purchases and related activity, since his company was located in a distant city. He submitted phony authorization letters from his company as support for the application.

- He contacted three major suppliers and requested cash rebates. In exchange, he guaranteed each would be the sole source for their respective products.

- He promised that they would be paid promptly for all materials delivered.

- He told the suppliers that rebates were due on the first of each month for all transactions of the preceding month. The checks were to be made payable to the name which appeared on the bogus bank account and sent directly to the bank.

Not surprising: The suppliers agreed to the unusual terms in order to win the business. None questioned the name on the checks because it was the same as the actual project name.

Result: The arrangement worked smoothly for several months. After the rebate checks cleared, the project manager withdrew most of the funds using cashier's checks.

Slip-up: A supervisor in the construction company's accounts payable department noticed that the three suppliers were being paid unusually fast. She wondered why they weren't offering prompt payment discounts.

Key: She had just attended a fraud

awareness seminar and remembered that an unusual arrangement like the one with the three suppliers could be an indicator of fraud.

Shrewd move: Instead of confronting the project manager or the suppliers, she referred the matter to the corporate audit department for investigation.

After reviewing internal records to gather background information, the auditors made simultaneous unannounced visits to all three suppliers. Two wouldn't talk, but the third—believing that the transactions had


been approved by the construction company—explained the relationship and provided copies of the cancelled rebate checks.

Lessons learned:

- It is too easy for dishonest people to open fraudulent bank accounts. Despite new-account screening procedures, there is nothing to prevent an informed, motivated fraudster from opening an account that the bank believes is legitimate.

- Schemes that involve relationships with suppliers are particularly hard to prevent and detect.

- When contracting with suppliers, secure the right to review all appropriate records. While this "right to audit" is extremely common in the contracting environment, it should also be more widely used in *any* business relationship where purchase orders are used.

- When financial transactions look strange, never let them slide. They often indicate a fraudster's mistake... and can deliver the key to the bust. Always refer suspicious activity to designated individuals for follow-up. 

White-Collar Crime Fighter source:

John Hall, CPA, Hall Consulting, Inc., a Chicago-based fraud prevention training and consulting firm, www.hallconsulting.biz. John can be reached at jhall@hallconsulting.biz.

Continued from page 3

the cash drawer or the computer room?

Related imperative: Avoid prematurely handing over responsibilities to new employees. Trust is still a vital part of successful business management. When an employee has been with the company for six or 12 months and has begun to earn management's respect and trust, that's the time to consider granting him or her access to secure assets and/or confidential information....*but not before.* Too many companies are willing to assume that an employee is honest, because they need the person to assume responsibilities based on trust. Big mistake!

- **"Ghost" employee schemes.** As hiring picks up and growing compa-

Now is an especially important time to screen for red flags of fraud taking place in your organization

nies struggle to meet customer demand, opportunities emerge for "ghost employees" to get added to the corporate payroll—particularly in organizations in which department managers, rather than HR, are in charge of hiring, scheduling and firing.

Example: A manager responsible for all personnel tasks related to his construction crew added 20 "employees" to his payroll. The only problem was that they were all friends of his who worked at other companies. He filled out time sheets for the fictitious employees, authorized them and took the paychecks generated to the real individuals, who cashed them and split the proceeds with him.

Self-defense: Verify that background checks are conducted for all new hires in all departments—no exceptions. Maintain complete and up-to-date files on the background checks.

Require the payroll department to periodically cross-check its records with personnel records, organization-wide.

Revise hiring policies to prohibit individual managers from being solely responsible for hiring, scheduling, firing and authorizing time-sheets.

- **Purchasing frauds.** Increased spending goes hand-in-hand with business growth, so watch for dishonest employees making personal purchases

Continued on page 5

Continued from page 4

with company funds or credit cards... as well as false invoicing... altered purchase orders...returned merchandise for cash, etc.

Extreme example: According to a federal indictment, in the mid-to-late 1990s, Tyco CEO L. Dennis Kozlowski used corporate funds to buy more than \$11 million of antiques, art and other fancy furnishings for his New York apartment. He got away with it for years because no one thought to double-check his purchases or question his authority. *Red flags of purchasing fraud:*

- The company's purchasing, accounting and shipping/receiving operations are all handled by the same employee or group of employees.
- Personal visits, gifts and gratuities from vendors.

Schemes detected in their infancy are just big frauds that haven't been allowed to "grow up"

- Holding or splitting invoices.
- "Do Not Mail" checks.

•**Kickbacks.** These crimes are common during good times and bad...but for different reasons. During business downturns, vendors are likelier to offer purchasing agents a little "something extra" to get the job because they haven't been working for a while.

During growth periods, vendors often feel extra generous about offering gifts and special services...cash benefits...travel rewards...special discounts...and other bribes to "differentiate themselves" from competitors.

Red flags of possible kickback activity: A single vendor being used because "it's always been that way" or because "Sally says so"...a particular vendor's bid routinely comes in last...purchasing agents or those in receiving start taking expensive trips or buying things they haven't in the past been able to afford...an employee is suddenly especially generous with others in his or her department...orders for materials and supplies are more frequently placed than normal or necessary. 🚫

White-Collar Crime Fighter sources:

- Jonathan E. Turner, CFE, CII, Wilson & Turner Incorporated, Memphis, TN-based investigative consultants, www.wilson-turner.com.
- The Corporate Fraud Handbook: Prevention and Detection*, by Joseph T. Wells (John Wiley & Sons Inc./2004).

SECURE OUTSOURCING

Craig L. Greene, CFE, CPA
McGovern & Greene, LLP



MANAGEMENT COMPANIES

To Trust or Not to Trust?

The business of business management has for decades been most familiar in the hotel/motel/resort and residential real estate industries. But the use of outside management companies has spread rapidly—to such areas as information/network technology...medical practice administration...celebrity business management...to mention a few.

Problem: While business management outsourcing is a cost-effective option for many companies, vendors aren't always as honest and upstanding as they appear to be.

When business owners or top executives suspect their management agents of self-dealing, they usually first approach their internal auditor or accountant for an explanation. Because most audit and accounting professionals aren't adequately trained to detect fraud, top management may need to retain outside forensic investigators or accountants to determine if the management company is complying with the management contract.

The good news: This can sometimes lead to favorable renegotiation of the contract.

Example: An experienced real estate property developer hired Marriott International to run his big new hotel in Quincy, MA, and installed his own chief 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.

PURCHASING PRACTICES

Most lawsuits against outside management companies target purchasing practices.

Key: A forensic investigation, combined with the threat of a lawsuit, strengthens the owner's position should it wish to renegotiate a management contract on more favorable terms.

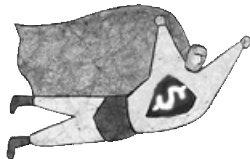
Example: An independent forensic expert discovered hundreds of a management company's contracts with manufacturers and suppliers, generating millions of dollars in undisclosed rebates to the management company. The investigation also uncovered hidden management company ownership interests in some of the vendors. The management contract restricted management company compensation to basic fees and cost-saving incentives.

Problem: When a management company fails to disclose rebates it receives from its vendors, it changes the character of those rebates to bribes.

Because a management company serves as an agent for the business owner, agency law applies, with its prohibitions of agent self-dealing without disclosure to, and approval by, principals. But some business management operators hide rebates...charge extra

Continued on page 6

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



**USA Patriot Act:
Benefits Beyond Busting Terrorists**

As part of its vigorous effort to overcome opposition in Congress to renew controversial provisions of the USA PATRIOT Act, the US Justice Department submitted to Congress a lengthy list of examples of how the Act has been used to catch terrorists and seize their assets.

Important: The Act has also proved useful in apprehending *non-terrorist* financial criminals.

Example from the DOJ report: Section 319 of the Act authorizes the US government to seize money targeted for forfeiture as a result of a fraud investigation, but which is located in a foreign bank account...by allowing the seizure of foreign banks' funds that are held in a correspondent U.S. account.

The rule holds, regardless of whether the money in the correspondent account is directly traceable to the money being held in the foreign bank account. *Useful example:*

An important model case for investigators involved in international anti-money laundering work involved attorney James Gibson who was indicted prior to passage of the USA PATRIOT Act on charges of conspiracy to commit money laundering and mail and wire fraud by stealing from his personal injury clients, including widows, orphans and severely ill patients.

Gibson and his wife fled to Belize, depositing some of the proceeds from their scheme in two Belizean banks. The Department of Justice's efforts to seize the cash were initially unsuccessful.

Though Belize's government first agreed to freeze the money, a Belizean court lifted the freeze and prohibited the government from further assisting American law enforcement agencies. Efforts to break the impasse failed, while the Gibsons drained their accounts in Belize by purchasing luxury items.

After enactment of the USA PATRIOT Act, DOJ served a seizure warrant on the Belizean bank's correspondent account in the US—pursuant to section 319. About \$1.7 million of remaining cash belonging to Gibson's victims was promptly recovered and earmarked for restitution.

White-Collar Crime Fighter source:

Report From The Field: The USA PATRIOT Act At Work, US Department of Justice, www.usdoj.gov.

Health-Care Fraud: Dangerous Trend

The 41 Blue Cross and Blue Shield companies increased savings and hard dollar recovery from fraud by 52% in 2003...to \$240 million. Unfortunately, the fraud problem weighs in at about \$85 billion, or 5% of the approximately \$1.7 trillion spent on health care every year, so the challenge for investigators, prosecutors and insured organizations remains enormous.

Important for fraud fighters: One area where the fraud losses are piling up fastest is in unnecessary surgical procedures. The Blue Cross/Blue Shield providers report a disturbing increase in the number of unnecessary cosmetic surgeries...colonoscopies...sweat gland removal procedures and other services being performed. Most of the fraudulent surgery cases involve dishonest providers paying insured individuals to undergo the unnecessary procedures at "clinics" whose business practices the FBI and other agencies now have under the investigative microscope.

White-Collar Crime Fighter source:

Byron Hollis, National Anti-Fraud Director, Blue Cross Blue Shield Association, Washington, DC, www.bcbs.org.

Continued from page 5—
fees...and conceal falsified documents from owners.

Examples:

•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 had received vendor payments that were, in fact, rebates rightfully belonging to the owner.

PROTECTING YOURSELF

If the purchasing clause in your management contract specifies that the only compensation for purchas-

Most lawsuits against outside management companies target purchasing practices

ing 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 of financial irregularities can also help you negotiate new purchasing agreements that provide you—not the management agent—substantial proceeds from rebates or discounts.

Important: In addition to rebates, be alert to other frequently overlooked costs, such as unexplained extra fees, which can significantly increase the charges specified in the management contract.

Example: The Quincy, MA hotel owner alleged in his lawsuit that independent agents who completed a Marriott training program received 10% commissions when they booked guests into Marriott hotels, compared with 8% commissions paid to other agents.

Adding insult to injury, the management company charged the property owner a heavy surcharge, despite the fact that the basic management fee covered commission costs.

LESSONS LEARNED

Tempting as it may be, business owners and executives simply cannot

Continued on page 7

Continued from page 6

operate with blind trust in management companies. To ensure a decent rate of return on their investment, you must evaluate the true costs of hiring management companies—including the underhanded ones.

Your internal auditor, accountant or an outside forensic accountant or fraud investigation firm are your best resources for safeguarding your hard-earned assets from dishonest management companies. 🚫

White-Collar Crime Fighter sources:

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.mcgoverngreene.com. Craig can be reached at craig.greene@mcgoverngreene.com.

The Fraudster's Smile...

A forced or insincere smile is often a disguise for discomfort or anxiety in a fraud interview.

Example: An investigator is about to enter an interview room to assess the credibility of a suspect accused of selling secret documents to a foreign government. As the investigator enters the room the suspect gets out of the chair and vigorously shakes his hand. While smiling ear-to-ear he says, "It's a real pleasure to meet you Mr. Jones. You have such a neat job and, by the way, that's a really nice suit you're wearing."

Message: Instantly the interviewer knows that he has just shaken the hand of a liar. No person—innocent or guilty—enjoys coming to an investigation-related interview enough to be that jovial.

Variation: In the context of an interrogation, the investigator may see a guilty suspect give a partial smile... a kind of smirk, indicated by closed lips twisting in an upward turn.

Caution: The investigator should avoid reading defiance and cockiness into the smile and responding with aggressive language such as, "Wipe that smile off your face when I'm talking to you." **Reason:** The suspect is unaware that he or she is forming the slight smile and may be simply subconsciously expressing guilt in response to the investigator's accurate assertions.

In fact, a smirk is often a sign that the suspect is getting close to making the first admission of guilt, and the investigator should recognize it as such.

White-Collar Crime Fighter source:

Brian Jayne, John E. Reid Associates, loss prevention and corporate security consultants, www.reid.com.



THE CON'S LATEST PLOY...

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

Milwaukee, WI

Voucher program abuse destroys school, costing taxpayers big bucks. David A. Seppeh, founder and principal of Milwaukee's Mandella School of Science and Math, was indicted in county court on charges of stealing \$330,000 of state funds earmarked for the state's pioneering school choice program.

Details: Seppeh, allegedly cashed 234 school voucher checks—many of which were made out to families whose children were never enrolled at the school.

Under the Milwaukee school choice program, parents could choose to send their children to accredited private schools and receive cash vouchers to defray part of the tuition cost.

According to the complaint against Seppeh, enrollment applications were filed on behalf of parents who never intended to enroll their kids at Mandella. Checks were received by Seppeh and allegedly cashed illegally.

Adding insult to injury, Mandella used \$65,000 of state voucher money to purchase two Mercedes-Benz automobiles.

The Mandella school was shut down by the state earlier this year after it had failed to pay more than \$40,000 in back rent and other operating expenses.

An investigation into the school's finances and education activities was initiated by the Milwaukee District Attorney's office, culminating in the latest court action against Seppeh. Seppeh faces up to 10 years in jail.

Birmingham, AL

Medicaid fraud supreme: New program to reduce infant mortality targeted for brazen bid-rigging scheme originating in gov-

ernor's office. Former Alabama Governor, Don Siegelman, his former chief of staff, Paul Hamrick and a local businessman and Seligman benefactor, Phillip Bobo were indicted on a variety of counts including conspiracy, health-care fraud, witness tampering, wire fraud, making false statements to the FBI and making false statements to the court, in connection with a major bid-rigging scheme aimed at ripping off a new Medicaid maternity care program.

While Siegelman was Governor, he and Hamrick allegedly helped Bobo, owner of a company called Neighborhood Health Services, a local health-care services provider, to rig the bidding process for a new federal maternity services program.

The Maternity Care Program was created by the Alabama Medicaid Agency to provide medical services to poor pregnant women...with the aim of lowering the unusually high infant mortality rate in Alabama.

The scheme: Siegelman and Hamrick allegedly transferred \$550,000 from Alabama's Special Education Trust Fund budget to the State Fire College in Tuscaloosa so that Bobo could use the money to issue fraudulent contracts, to pay off a competitor who was also participating in the Maternity Care Program bid process.

Details: In addition to running Neighborhood Health Services, Bobo served as the Medical Director of the Emergency Medical Services training program at the Alabama State Fire College.

At one point during the pre-bidding period, Bobo allegedly asked the Fire College's Executive Director, Bill Langston, "about the possibility of" the Fire College contracting with Capstone Health Services Foundation, P.C., an affiliate of Alabama Health Network, another

health-care services consortium which was also competing for the Maternity Care Program contract.

According to the indictment, Bobo received cooperation from senior officials in Seligman's office to use the transferred \$550,000 to issue the fraudulent contracts to Alabama Health Network in exchange for Alabama Health Network's agreement not to participate in the Maternity Care Program bidding process.

According to the indictment, the Maternity Care Program contracts for the entire state were worth more than \$100 million per year.

The case was jointly investigated by the FBI, the Alabama Attorney General's Office and the U.S. Department of Health and Human Services, Office of Inspector General.

Denver, CO

Bogus grant program cons hundreds into giving up Social Security numbers and more. Carlotta Wilson promoted herself as a philanthropist until Colorado authorities got the goods on her phony consumer grant scheme.

Details: Carlotta and her company, SSS Organization Nine, Inc., promoted a free "grant" program which claimed to have access to \$900 billion in government and non-government funding

to help needy people start businesses...repair bad credit histories...obtain scholarships...pay for prescription drugs...cover child support and other expenses.

Problem: The 400 or so unsuspecting victims who lined up at Wilson's door to fill out applications for the grants got nothing. But by completing the applications, the victims gave Carlotta their Social Security numbers, dates of birth and other personal identifying information that constitute the essential ingredient for committing identity theft and fraud.

Carlotta was sued by the Colorado Attorney General and upon failure to respond to the suit, was issued a default judgment ordering her to pay \$50,000 for violation of the state's Consumer Protection Act by making up the phony story about her ability to obtain grant money.

Richmond, VA

Virginia's tough anti-spam law results in multi-jurisdictional bust. Virginia's eagerness to play a leadership role in the battle against spam has borne fruit ... at least in one small way with the arrest and indictment of Jennifer Murray.

It seems Jennifer is one of the "unfortunate" few, among legions of illegal E-mail mass marketers, to have

fallen victim to Virginia's tough anti-spam law.


Operating from Texas, Murray allegedly orchestrated a spam campaign to promote sales of human growth hormone (HGH). As a part of the illegal campaign, Murray was accused of altering the headers of the spam E-mails to conceal her identity.

As home to America Online, Virginia has been aggressive in enacting anti-spam legislation which prohibits the sending of unsolicited bulk E-mails by fraudulent means—such as by changing the header or routing information in order to obscure the sender's true identity.

Under the Virginia statute, this activity constitutes a felony if it involves sending 10,000 or more E-mail messages in a single 24-hour period...or if the amount of revenue generated by a specific spam message exceeds \$1,000, or if the total revenue from all spam messages transmitted to any Virginia-based ISP exceeds \$50,000.

Jennifer Murray's HGH campaign was investigated by AOL and by the Attorney General's Computer Crime Unit. Under the anti-spam law, the AG's office is permitted to investigate and prosecute spammers who use computers or networks located anywhere in the state.

Thanks to the cooperation of local Texas law enforcement officials, Jennifer was picked up in Fort Worth and subsequently indicted in absentia in Loudon County, VA.

She will be extradited and tried in Virginia where she faces five felony charges, each of which carries a sentence of one- to five-years in prison, a fine of up to \$2,500 or both...and subjects her to seizure of assets that may have been obtained by committing the crimes. 



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

COMING SOON IN

White-Collar Crime Fighter...

- **Anti-identity theft success strategies**
- **Electronic evidence: Legal traps to avoid**
- **Practical health-care fraud prevention insights**
- **New technology for busting forgers and counterfeiters**