

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

VOLUME 6 NO. 2
FEBRUARY 2004

IN THE NEWS

For Once: Good News About Fraud-Fighting

Insurance fraud, while representing just one portion of the country's overall fraud problem, is in the news because of its startling success in recent years in convicting the bad guys.

Insurance fraud bureaus from 43 states responded to the Coalition Against Insurance Fraud's (CAIF) recent survey of bureau performance. Together, the bureaus reported a total of 2,535 criminal convictions in 2002—up 31% from the 1,931 figure for 2001.

Biggest gains: Florida, New York, New Jersey, Pennsylvania.

Also impressive: This gain was achieved in the context of flat or shrinking bureau budgets. The average annual insurance fraud bureau budget was \$3.5 million in 2002, down slightly from the year before.

Outlook: To maintain this impressive growth level in convictions, state insurance bureaus say that they will need to be prepared for the growing size and complexity of fraud—especially staged accidents and fake health insurance. As always, money, staff and computers lead the budget wish list of bureau directors.

White-Collar Crime Fighter source: Dennis Jay, Executive Director, Coalition Against Insurance Fraud, www.insurance-fraud.org. Dennis is author of the above-referenced survey, *A Statistical Study of State Insurance Fraud Bureaus*.

IN THIS ISSUE

- **STOP SUPPLIER STEALING**
How to keep them honest.....3
- **TERRORIST UPDATE**
Why they're still in business....4
- **GOVERNANCE GUIDANCE**
SOA for private companies.....5
- **THE CON'S LATEST PLOY**
Law-enforcement successes from around the country.....7

Martin Biegelman
Microsoft Corporation

FRAUD FORECAST

Internal Threat Faces Tougher Preventive Strategies



Accounting giant KPMG recently released its *KPMG Fraud Survey 2003* which analyzes the impact of fraud on American businesses.

Participants: Over 450 executives in medium- and large-sized US businesses across industries, as well as government agencies.

Important: While the results may not be surprising to fraud prevention professionals, the survey's conclusions can be used to guide the fine-tuning of your existing fraud prevention programs...or to develop such a program from the start.

INFORMATIVE FINDINGS

The KPMG Fraud Survey found that:

- Awareness of financial fraud and fraud prevention is on the rise in the post-Sarbanes world.

- Organizations are applying greater focus on fraud prevention than in previous years.

- Sarbanes-Oxley has had a dramatic effect on American business. Three-quarters of KPMG survey respondents reported that they will implement anti-fraud programs as a result of this legislation.

- Companies are finally accepting that well-conceived and professionally managed fraud prevention programs do work.

- Seventy-six percent of companies now immediately terminate employees who commit fraud.

Key question: Why isn't this number 100%? This statistic proves that much more needs to be done in the areas of fraud awareness and prevention.

- Two-thirds of KPMG's respondents now take legal action after discovering

frauds, usually including contacting law enforcement authorities.

Significance: Legal action against fraudsters not only addresses the immediate problem, but also serves as a psychological tool by sending a strong message to other employees. The potential of being caught in a fraud scheme, and getting fired and prosecuted is a strong deterrent for those who consider a move to the dark side.

Lesson for management: Continually educate employees about fraud and the damaging effect it can have on the company and on their future employment.

Important: Begin fraud prevention training at the time of hire...and continually reinforce the lessons on a year-round basis.

Effective: A special training program for financial, procurement and management personnel including top executives.

THE FRAUD PREVENTION GOSPEL

As part of this training, consider adopting an "evangelistic" approach to fraud detection and prevention.

Example: Expose employees to scenarios based on actual incidents of internal fraud. Representatives of human resources and legal should then discuss the impact of scenarios with employees and enthusiastically promote the company's mission and vision for fighting these crimes.

Objective: To get employees emotionally committed to learning about the specific types of frauds and abuse that affect your business and about learning how to

detect and report these incidents before damage is done.

THE INTERNAL FRAUD PLAGUE

In the KPMG survey, instances of employee fraud far outstripped other frauds such as consumer fraud and computer crime.

Top forms of internal fraud:

Expense account abuse, financial reporting fraud, theft of company assets, check fraud.

EFFECTIVE COUNTERMEASURES

- To reduce expense account abuse, require and *enforce* rigorous management oversight and review. Require all expense reports to be thoroughly reviewed and approved by the employee's manager. Then hold the manager accountable if fraud or abuse is missed.

- To reduce financial reporting fraud, conduct a full and accurate implementation of the Sarbanes-Oxley requirements including...

- CEO/CFO certifications that hold chief executives accountable for their actions and for any fraud detected in the financial statements filed with government agencies.

- Reviewing and enhancing internal controls.

- A strong audit committee.

- A truly independent external auditor.

- A code of conduct communicated to all employees.

- Giving legitimate whistleblowers the opportunity to come forward without fear of retaliation.

MORE THREATS...MORE SOLUTIONS

- Internal-external collusion.** The KPMG study found that collusion between employees and third parties, such as vendors, is among the top M.O.s in internal fraud.

Effective: Directly involve vendors in your fraud prevention program. Earn "buy-in" from suppliers in stopping kickbacks and other vendor frauds by letting them know that you won't do business with any company that offers kickbacks and that you will report illegal activity to the authorities.

Also, include vendors in your training programs and tailor training specifically for them.

- Lax internal controls.** The survey determined that beefing up internal controls is the most widely used strategy

now for reducing fraud.

Increased vigilance by the internal audit function came in second, while tips from employees ranked third on the list of methods of uncovering fraud.

Significance: An earlier KPMG survey showed that employee reporting was the number one reporting method.

Possible explanation: Trends are shifting...and internal controls are finally working more effectively than they had in the past.

- Inadequate reporting.** Though tips from employees are still among the most common ways that fraud is detected, the increasing threat of fraud shows that more hotlines and better hotline policies are urgently needed.

Key: Under Sarbanes-Oxley, all public companies must have a

Begin fraud prevention training at the time of hire...and continually reinforce the lessons on a year-round basis

confidential and anonymous reporting mechanism for employees to report financial statement fraud. All companies, whether public or private, should have a hotline for employees and others to report fraud and abuse.

Essential: To ensure true independence, have a skilled professional third party administer the hotline.

THE BIBLE OF FRAUD PREVENTION: CODE OF CONDUCT

In addition to establishing a code of conduct for all employees, create specific codes for all finance and procurement employees. Implement another for all vendors. Have each employee and vendor sign the appropriate code, indicating that they have read, understand and will comply with the requirements. Conduct training for all employees so they fully understand the code's provisions. Provide each employee with a soft and hard copy of the code of conduct.

BETTER BACKGROUND CHECKS

Too many companies still refuse to accept that background checks should be conducted on all new hires. There should be no exceptions when it comes to conducting background checks.

The degree and level of the background checks should match the employee's position in the company. At the minimum, background checks

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.

Audit & Risk Management

Steven I. Adler, Senior Auditor, Health Net Inc.

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 Fraud

Raemarie Schmidt
Supervisory Computer Crime Specialist
National White-Collar Crime Center

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.

should include criminal and credit checks, prior employment verification, and educational degree and certifications received. (See box below.)

FUTURE OF CORPORATE FRAUD

There's no question that fraud is on the rise and it will take much more work by businesses and law enforcement to reverse the trend.

The good news: The many corporate scandals of the last few years have increased acceptance of the damaging effects of fraud and the need for greater fraud detection and prevention.

It finally looks like we are on the right path...but we must continually intensify and modify fraud-fighting efforts to keep up with the ever-nimble criminal minds that plague us. 🕒

White-Collar Crime Fighter source:

Martin T. Biegelman, CFE, Director of the Financial Integrity Unit, Microsoft Corporation, Redmond, WA. He is a former U.S. Postal Inspector and currently is a Fellow of the Association of Certified Fraud Examiners (ACFE). He can be reached at martinbi@microsoft.com.

Biegelman on...

Benefits of High-Level Background Checking

Executive level job applicants should be subjected to the most comprehensive and probing background check possible.

Example: "Chainsaw Al" Dunlap, the former CEO of Sunbeam Corporation, who was fired in 1998 shortly after the SEC launched a probe into the company's accounting practices, had a dubious background that was unknown to Sunbeam's senior management.

Dunlap was fired from a company in 1973 after less than two months on the job. In 1976, he was fired by another corporation based on allegations of financial fraud during his tenure. Dunlap failed to list these prior positions on the resume he submitted to Sunbeam and this adverse information was not discovered until *after* Sunbeam terminated him.

An in-depth background would have uncovered this incriminating information and possibly saved Sunbeam from SEC scrutiny and the media spotlight.

STOP SUPPLIER STEALING

Craig Greene, CFE, CPA, *McGovern & Greene LLP*

**VENDOR AUDITS:
Key to Keeping
Your Suppliers
Honest**



Though it's tempting to believe your vendors would never rip you off, do yourself a favor and never take anything for granted when it comes to doing business with suppliers.

Reason: Far too many suppliers—of all sizes and tenures in business—are defrauding unsuspecting clients...and not just through complex schemes, either.

Common forms of vendor fraud against customers...

...do yourself a favor and never take anything for granted when it comes to doing business with suppliers

- **Overcharging schemes.** In an overcharging scheme, the vendor may use prices that are higher than those you agreed to—or may bill you separately for items that should have been included in the contract price.

- **Inflating hours.** Billing for hours not worked on a consulting or time and materials contract or other type of service arrangement.

- **Short-shipping.** Deliberately billing you for goods that are below the quantity you contracted for—or not delivering goods at all while still billing you for them.

- **Substitution-of-materials fraud.** Billing for expensive, high-quality goods (possibly imported) and delivering cheaper, lower-quality, locally manufactured goods in their place.

FRAUD PREVENTION STRATEGY

The best way to protect against these and the many other forms of vendor fraud is to stop it before it starts.

Key to success: Make sure all of your vendor contracts and purchase orders contain a "Right-to-Audit" clause. In the same way that "good fences make good neighbors," the pres-

ence of a "Right-to-Audit" clause makes it more likely that your vendor relationships will always be open, honest and mutually beneficial.

How it works: The clause contains language that establishes your right to review a vendor's financial records in order to ensure that you're not being overcharged or charged for goods or services not delivered, and that no

other type of fraud is being perpetrated against you.

Who should manage the audit:

In large public companies, the director of internal audit is typically the best person to oversee audits of suppliers...unless an experienced director of corporate investigations is on staff. In smaller, privately held companies, the CEO is usually the only one who should handle this important function.

SPELLING IT OUT

Include an abbreviated version of the right-to-audit clause on every purchase order your company sends out. Use language that's authored by a committee consisting of legal, audit and procurement department personnel, and you'll cover all the bases.

Mistake to avoid: Applying your right-to-audit for too brief a period of time after your business with a vendor is concluded. Specify in each contract a right-to-audit window spanning three-to-four years from your last business transaction with a vendor.

Sample language: A clause included on a purchase order or other procurement document should contain language along these lines:

Continued on pg. 4

TERRORIST MONEY TRAIL

Why the Terrorists Are Still in Business

It was widely hoped that the war in Iraq and the concurrent battle against the Taliban and Al Qaeda in Afghanistan would cripple the international terrorist network enough to render it inoperable. Unfortunately, the recent holiday season jump in warnings about “real” plans to launch a major attack against the US proved otherwise.

Possible reasons: The terrorists are highly adaptable. While the US and its allies battle Hamas, Hizballah and al Qaeda, both militarily and financially, the terrorists are constantly devising new locations to hide in...new places to pick up ill-gotten cash...and creating new “businesses” to raise money for their dirty work.

Latest findings on how terrorists finance their operations...

• **Serious weaknesses in the USA PATRIOT Act.** The Act, signed shortly after the September 11, 2001, was written with the aim of strengthening US law enforcement’s authority to investigate and shut down terrorist-related money-laundering activities.

Key: The information that was supposed to be gained through submission by financial institutions of so-called Suspicious Transaction Reports (STR), was meant to be shared with law enforcement and intelligence analysts in their efforts to detect and deter terrorism.

Problem: For over a year, The Financial Crimes Enforcement Network (FinCEN) has been saying it lacks the resources to even draft regulations required under the Act...and as a result, it has been unable to prioritize the workload.

Added challenge: *The 2002 National Money Laundering Strategy*, issued by the Treasury and Justice Departments, now imposes regulations on businesses not previously subject to anti-money laundering regulations—such as automobile and boat dealers...pawn brokers...precious metals, stones and jewelry dealers. That has further increased FinCEN’s workload for collecting and managing the Act’s required STRs.

Result: Major loopholes for terrorist money-laundering are still available.

• **Trafficking in illegal cigarettes.** Much has been reported about terrorists’ dealing in illegal drugs and abuse of the international financial system to support their activities.


Less widely known is that terrorists have illegally generated millions of dollars through the black market for cigarettes—in the US.

ATF data: Hizballah, Hamas and al Qaeda have amassed assets through trafficking in contraband cigarettes or counterfeit cigarette tax stamps. As of August 20, 2003, ATF was investigating at least six such cases with

ties to terrorist groups.

• **Failure by the FBI to manage information about terrorist financing.** The FBI—which leads terrorist financing investigations—does not systematically collect and analyze data on terrorist financing outside the legitimate financial system.

Critical: Without this data—gathered and managed with the help of other government agencies—the Bureau can’t possibly perform the analysis of trends and patterns of terrorist financing which in turn prevents it from assessing specific terrorist financing risks and prioritizing anti-terrorist financing activities.

• **Failure by Departments of the Treasury and Justice to produce required terrorist-financing reports.** Under *The 2002 National Money Laundering Strategy*, the two federal agencies were required by March 2003 to complete a report on the links between terrorist financing and precious stone and commodity trading. Without this information, terrorists presumably still have those massive markets available to them. 

White-Collar Crime Fighter source:

Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists’ Use of Alternative Financing Mechanisms, US General Accounting Office, November 2003. For the full report, visit www.gao.gov. Search on report number GAO-04-163.

Continued from page 3

“Seller shall establish a reasonable accounting system which enables ready identification of seller’s cost of goods and use of funds. Buyer may audit seller’s records anytime before three years after the final payment to verify buyer’s payment obligation and use of buyer’s funds. This right to audit shall include subcontractors in which goods or services are subcontracted by seller. Seller shall insure buyer has these rights with subcontractor(s).”

Conduct routine audits of vendors with whom you have long-term relationships. Initiate a spot audit when you suspect fraudulent activity.

CONSISTENCY IS KEY

Best practice: Don’t wait until you have a reason to ask vendors to open their books. Routine audits send the message that you adhere to a strict code of ethics...that you require those who do business with you to do the same...and that you are on guard against irregularities at all times.

SURPRISE EQUALS SUCCESS

When dealing with a vendor you’ve never audited before, but which you suspect of ripping you off, don’t give the company too much time to prepare for your audit. Allowing more than a week to pass between the time you notify the vendor of your intent and the time you show up at his office increases his opportunity to sanitize the books.

AUDITING EXISTING SUPPLIERS...

• **Conduct behind-the-scenes preparation.** Before you meet with a vendor, prepare a written audit program that states your specific objective for conducting the audit.

Example: This audit is being done to ensure that invoices received from the vendor adhere to the compensation agreement outlined in the vendor contract, and that the vendor’s operating procedures are in compliance with our Business Conduct/Ethics Policy.

Key: Use this program to document each step of your investigation.

• **Carefully review all documents and information related to your current and past business** with the vendor, including invoices, contracts, agreements, bids, purchase orders, a list of disbursements, etc.

Effective: Select a sample of invoices from the time period of concern and check to see that they’re consistent with terms of the vendor agreement which

Continued on page 5

Continued from page 4

require, for example, clerical accuracy...approval for payment...and conformance with vendor time sheets, hourly rates, equipment costs, etc.

Make detailed notes concerning errors and/or irregularities.

•**Maintain a list of the vendor's employees you've dealt with over time**—those who've made deliveries, signed contracts, resolved conflicts/problems over the phone, etc.

Reason: If you must conduct further investigation of the vendor under the right-to-audit clause, these names will prove to be indispensable.

•**Conduct on-site investigations.**

If it becomes necessary to do a full internal investigation of a suspicious vendor, follow these basic steps...


□ Interview employees at the vendor's office who've done business with your company. Ask such questions as: What percentage of your business comes from our company...Who are your pri-

...the director of internal audit is typically the best person to oversee audits of suppliers

mary contacts at our company...Do any of our former employees work for you...Are you aware of our "Standards of Business Conduct/Ethics Policy"...In the course of doing business with us, have you encountered any difficulties—and, if so, how were those difficulties resolved?

□ Select a sample of vendor invoices from the vendor's records and review hours charged to your company...trace employees' "hours worked" from the posted schedule to time sheets to payroll roster...review the calculation of "amounts paid" to employees...examine rates charged for labor and equipment.

□ Review the petty cash fund, expense accounts, 1099 Forms, and canceled checks to screen for irregular gifts or payments made to your employees.

After you've conducted a vendor audit and found evidence—or red flags suggesting fraudulent activity, consider taking the next step by filing your audit results and damage estimates with your legal counsel or local authorities. 

White-Collar Crime Fighter source:

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

GOVERNANCE GUIDANCE

Sarbanes-Oxley for Private Companies?

ABSOLUTELY



While Sarbanes-Oxley Act (SOA) compliance is not mandatory for private companies, here are several compelling reasons for private company executives to live by the new law's core provisions anyway...

•**Some SOA rules do directly apply to both public and private companies.**

Examples: Document retention...tougher penalties for mail and wire fraud...liability for retaliating against whistleblowers...heavier criminal penalties for ERISA violations.

•**Deterring board misconduct.** Boards of directors of private companies often comprise large shareholders who, because of the "clubby" nature of their relationship, ignore the principles of governance and fiduciary duties.

Trap: Directors of private companies still have a fiduciary duty to creditors if their company gets into financial trouble. That means financial misconduct that occurs due to the absence of effective governance—as described in SOA—can backfire. Implementing key SOA rules on board and audit committee behavior can prevent this.

BENEFITS OF SOA COMPLIANCE

In addition to preventing legal hassles, there are potentially significant benefits for those that do use SOA as a guide to better corporate governance.

Examples:

•**Companies whose success hinges on the support of banks or venture capitalists** are prepared if they are faced with new, tough questions about financial disclosure or governance practices from their benefactors who seek comfort in knowing that their investments are in the hands of

honest people.

•**Improved chances of securing bank financing.** More and more bankers are asking for information about SOA compliance for new loan agreements.

•**Reduced insurance costs.** Because most insurance companies know that private company shareholders can sue the board of directors for breaches of fiduciary duty, heightened concern about governance is helping to push premiums higher for both public and private companies.

Major target: Directors and officers (D&O) coverage. Insurers are increasingly likely to ask about SOA compliance when the company renews its D&O policy.

•**Better buyouts.** Business owners trying to implement an exit strategy should know that prospective acquirers are impressed with companies that have enforced SOA compliance.

Important: This is true not only when selling the company outright, but also when preparing an initial public offering.

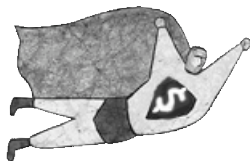
In either situation, buyer(s) in today's SOA environment want to know that the company is ethical from the top down. If the company implemented none of the SOA provisions, the sale could be delayed and/or the selling price could be pushed lower.

Bottom line: Businesses that are considering going public—or are being purchased by a public company—should have a good grasp of what is required of public companies and take similar steps toward compliance, so that they can meet requirements as soon as necessary.

•**Reduced fraud losses.** In a very

Continued on page 6

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE



Internal Relay Calling: New Way for Fraudsters to Rip Off Merchants

T *True story:* A retail store owner received an Internet Relay Call from a person wanting to place an order with a credit card.

The call—the kind that allows Internet users to initiate real-time, cost-free computer-based conversations via a phone company operator—was from a woman named Kelly who wanted to order 30 computer hard drives and wanted to pay by credit card.

She gave her name, address and credit card number.

Fortunately, the retailer had experienced this before so, after taking the order, she checked with the “customer’s” issuing bank where she learned the card was stolen.

The retailer later learned that most Internet Relay Calls placed to retailers are fraudulent.

Self-defense: Have your phone company put a block on relay calls. That will stop many of the scammers, but you must still be on the lookout for con artists slick enough to get the operator to put the call through.

Also helpful: If you do get relay call orders, ask the caller for a phone number and address, as well as a name—to verify the order. Then call them back to confirm the legitimacy of the information. Nine times out of 10, the callers will hang up on you.

White-Collar Crime Fighter source:

“debh”, an Internet Relay Call operator, posting on the Loss Prevention Message Board at www.LPinformation.com

Better SAR Alternatives

As the federal government continues to lengthen the list of businesses required to file Suspicious Activity Reports (SAR) in the hope of bolstering its efforts to catch money-launderers—especially terrorist-related ones—more and more employees need to know how to file a SAR.

To the rescue: The Financial Crimes Enforcement Network (FinCEN) has published a useful and easy-to-follow set of guidelines on how to write a good SAR narrative. These narratives are required as part of every SAR filing and must cover a specific number of key information areas related to the suspicious incident.

To download the guidelines as well as a handy PowerPoint summary of the steps for writing a SAR narrative, visit: http://www.fincen.gov/narrativeguidance_webintro.pdf.

Preventing Auto Insurance Fraud Is No Accident

That’s the slogan for the Massachusetts Insurance Fraud Bureau’s (IFB) new reward program for tips on suspected car insurance fraudsters.

Details: In response to the death of a woman who was part of a staged-accident operation, the IFB launched its program offering a \$5,000 reward for information leading to the arrest and conviction of car insurance fraudsters in a particularly fraud-ridden portion of the state. The program is promoted with local newspaper ads which prominently display a special toll-free tip hotline.

The IFB is believed to be the only insurance investigative agency that is privately funded by a state’s insurance industry.

For more information visit: <http://www.ifb.org/Press%20Releases/lawrence%20reward%20ad.pdf>.

Continued from page 5

short time, SOA has become the benchmark against which every company’s financial reporting and disclosure and corporate governance practices are measured.

By willingly adopting what the business world now regards as best practices in corporate governance, private companies should see tangible results in terms of higher numbers of potential frauds prevented and reduced dollar losses from internal financial crime.

GETTING IT DONE

For private companies committed to governance driven by a culture of “doing the right thing,” these SOA-compliant practices offer a useful road map...

- **Adopt a formal code of ethics.** An ethics code not only sets the standard for corporate conduct by officers, it defines the culture of the company as one insistent upon honesty and integrity on the part of all employees.

- **Designate a compliance officer who reports to the company’s independent audit committee.** The officer can be either an internal employee or an outside consultant. But regardless of the option you choose, the officer must be fully empowered to run the compliance program and to address whistleblower issues independently.

- **Strengthen the internal audit function.** Internal auditors are essential for policing the adequacy and effectiveness of the company’s internal controls.

Effective: To set up tight controls in the short term, hire a consultant or temporary audit professional. This person can quickly perform a thorough review of your existing controls and provide you with a clear report on the risks the company currently faces...and the cost of implementing solutions.

Benefit: You can choose whether and where to take further action, based on the significance of the risks and the costs of addressing them.

- **Recruit one or more independent board members.** Independent board members with track records of business success and reputations of integrity can provide objective oversight and can actually become the foundation for an audit committee.

Continued on page 7


Continued from page 6

An audit committee can contribute useful guidance on development and implementation of better controls and financial management...which is especially useful for companies preoccupied with operations.

Critical: Bringing on independent directors and establishing an audit committee can only be successful if they have the unqualified support of top management. Board directors should be compensated for their contributions and they must be given full independence in learning about the company's financial operations. Most importantly, executives must be willing to act on board recommendations for improved controls.

- **Segregate internal audit and outside accounting and audit services.** Sarbanes-Oxley requires companies to use a firm other than their external auditor for key services, such as internal accounting and auditing. Though private companies are not bound by this provision they can boost their image as well-governed and ethical businesses by separating audit services from other accounting or consulting services.

- **Require official certifications of financial information.** Public company CEOs must now certify that all financial statements are in compliance with financial reporting laws and rules and "fairly present a company's financial condition and results of operations."

Private companies can substantially improve their chances of obtaining bank financing, venture capital and other benefits by doing the same. 

White-Collar Crime Fighter sources:

- Cheryl de Mesa Graziano, CPA, Director of Research at the Financial Executives Research Foundation (FERF), a unit of the Financial Executives International (FEI) www.feio.org. (cgraziano@feio.org). Portions based with permission on material published in FEI's *Financial Executive Magazine*.

- *The Impact of SOA on Private Business*, study by Robert Half International (RHI), world leaders in business accounting staffing and professional recruiting, www.rhi.com.

- Peter Goldmann, Editor, *White-Collar Crime Fighter*.

COMING SOON IN

White-Collar Crime Fighter...

- **Technology's role in Sarbanes-Oxley compliance**
- **Avoid new traps in payables fraud**
- **Secrets of international fraud investigations**
- **New identity theft threat: Gay gangs**



THE CON'S LATEST PLOY...

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

New Haven, CT

Latest cyber-crime targets: Gullible older gay men. In an example of how easy it is for cyber-fraudsters to prey on demographic "niches", Steven Smith pleaded guilty to one count of mail fraud for a crime involving the placement of Internet ads that fraudulently induced older gay men to mail him in excess of \$64,000.

Details: Smith placed an ad on several gay Web sites, include a gay dating site, "GaySweetHeartz.com." Using the screen name of "Stevenyounger," the 43-year-old Smith posed as a 21-year-old gay male who had been rejected by his parents, was in prison and was seeking guidance from an older man.

When victims replied to the ads, Smith corresponded with them through the mail and on the phone. During this correspondence, he indicated that he was in jail and needed money to secure his release. At least 28 of Smith's victims from across the country and in Canada collectively mailed Smith \$64,615.

The mail fraud count to which Smith could get him up to 20 years' imprisonment, a \$250,000 fine, a three-year period of supervised release and a \$100 special assessment. The plea agreement requires Smith to make full restitution to all of his victims.

The case was investigated by United States Postal Inspectors.

Seattle, WA

Big-time internal fraud hurts Even the most security-conscious. Kori Brown, an administrative assistant for X-Box at Microsoft, used her office computer to place 17 orders for high-end business soft-

ware, known to cyber-security experts as "Sequel Server" software. The orders had a retail value of more than \$6 million.

Upon receiving the orders, ClientLogic, which provides warehouse facilities to Microsoft, shipped the software from its facility in Columbus, OH, to an address in Washington State. They went either to Brown directly at Microsoft, or to two phony organizations identified by Brown as charities.

Problem: Brown had fabricated the order to deceive ClientLogic into believing that the software was for Microsoft business use or was to be distributed by Microsoft for charitable purposes.

Brown actually sold the misappropriated software to a third party for an unconfirmed amount between \$50,000 and \$100,000.

The case was investigated by the FBI and the US Postal Inspection Service.

Charleston, WV

Strong-arm debt-collection fraud Costs victims thousands in losses. A Utah law firm, Bennett & DeLoney, called Eugene Blake of Eleanor, WV to demand payment of \$145.42 for a \$17.42 bad check he had allegedly written to a local discount store.

Turning nasty: When Blake questioned the excessive fees, the caller warned him that he would be sued and face \$800 in additional fees if he didn't pay the \$135.42.

Problem for the Utah firm: Eugene Blake was not the first victim to complain to the West Virginia Attorney General's office about this strong-arm fraud scheme.

The AG's office began an investiga-

tion of Bennett & DeLoney's "debt collection" practices, and found that about 555 West Virginia consumers had been illegally charged the \$128 fee in connection with allegedly uncollected checks.

"Minor" details:

- It is illegal to charge more than \$25 in fees for collecting on bad checks in the state of West Virginia.

- Bennett & DeLoney was not licensed or bonded to conduct debt collection business in West Virginia.

The good news: Following the investigation, Bennett & DeLoney agreed to refund the entire \$53,929 to the victims.

Background for investigators:

There are numerous unscrupulous entities like Bennett & DeLoney that either purchase large batches of supposedly bad checks from—or act as third party collectors on behalf of—other collection companies.

They use overly aggressive, often illegal tactics such as threats of added fees or even legal action to intimidate unwitting victims into paying their extortionate fees.

Often, the checks involved aren't even written by the victims, because they were stolen and forged. In other instances, when targeted individuals are called for payment, and they ask for a copy of the check, the "collector" refuses to send the copy and sim-

ply intensifies the pressure to get the victim to pay.

Lansing, MI

Unemployment fraudsters use own money in convoluted scheme to cheat the system. Ronald Paul, Wayne Mulka and Eugene R. Grulke were caught trying to fraudulently collect unemployment compensation benefits.

Paul and Grulke pleaded guilty and each paid \$7,800 after pleading guilty to making false statements in order to fraudulently obtain unemployment compensation benefits. Mulka failed to appear for his arraignment.

The scheme: The men paid a business owner in Presque Isle County, MI to put them on his payroll. They were then "paid" for two weeks of "work" for the company with their own money. After the two-week period, they were "laid off."

The men then applied for unemployment compensation, which each of them received in the amount of \$7,800.

The case was ultimately referred to the Michigan Attorney General's office by the local prosecutor to avoid any conflict of interest because the prosecutor knew each of the men charged in the case. ☹

Fiduciary Relationships: What They Are and How to Manage Them

What is a fiduciary relationship? According to Black's Law Dictionary, a person has a fiduciary relationship exists when "the business which he transacts, or the money or property which he handles, is not for his own benefit, but for another person, as to whom he stands in a relation implying and necessitating great confidence and trust on the one part and a high degree of good faith on the other part".

In English: A fiduciary relationship exists when an employee—regardless of rank in the hierarchy—handles his or her employer's assets and is expected to do so with honesty, reliability and integrity.

This applies to a convenience store cashier as much as it does to a top executive of a multi-billion dollar corporation.

What it means for employers: If someone in your organization steals small amounts of cash...inflates an expense report...forges and cashes a company check...masterminds a multi-million dollar financial fraud—to name just a few examples—he or she breaches the fiduciary relationship with your organization.

Key lesson: Your organization should consider using the legal standard of fiduciary relationship to formulate a clearly worded section in its fraud prevention policy stating the consequences of any breach of fiduciary relationship. It can be immediate termination...disciplinary action...prosecution...or any combination of these and other consequences.

Bottom line: A fiduciary relationship is something that all employees must take seriously. If they don't know what it is, explain it and emphasize that your organization takes this relationship extremely seriously.

White-Collar Crime Fighter source:

R.A. (Andy) Wilson, CFE, CPP founder and managing director with Wilson & Turner Incorporated, an investigative consulting firm, where he specializes in the prevention, identification and resolution of employee crime. This article is based in part on *Employees Dishonesty: A National Survey of Risk Managers on Crime*, a research project completed as part of Andy's work toward a Master of Science in Economic Crime Management at Utica College. Andy can be reached at raw@wilson-turner.com.



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**—FOUR Special Reports on preventing, detecting and investigating latest computer and Internet frauds.

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