

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

VOLUME 11 NO. 5
MAY 2009

YOUR SECRET WEAPON IN THE WAR ON FRAUD

IN THE NEWS

Fraud Factors in the Financial Fiasco Under Review

The Fraud Enforcement and Recovery Act of 2009, (FERA), was signed by President Obama on May 20. In addition to appropriating funds for stepped up investigation of corporate crime and tightening the laws against mortgage fraud, FERA establishes a special commission to investigate the causes of the 2007-2009 financial meltdown.

Specifics: FERA establishes the Financial Crisis Inquiry Commission with broad authority to investigate the financial and economic crisis.

The Commission will have until December 15, 2010, to complete its investigation of the circumstances that led to the financial crisis and report its findings and recommendations to Congress. The Commission will have broad investigative authority, including subpoena power, and the ability to refer any evidence of criminal activity to the U.S. Attorney General and state attorneys general.

The Commission is mandated to investigate 22 areas contributing to the crisis, with "fraud and abuse in the financial sector, including fraud and abuse towards consumers in the mortgage sector" topping the list.

It remains to be seen how deeply the panel digs for hard answers that will play a role in preventing future meltdowns.

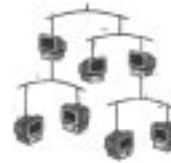
White-Collar Crime Fighter source: Cady North, Manager of Government Relations, Financial Executives International, www.fe.i.org.

IN THIS ISSUE

- **DOING MORE WITH LESS**
Fraud-fighting on a tight budget... 3
- **AUDITOR INDEPENDENCE**
Essential to detecting fraud..... 4
- **PAYABLES PLOYS**
AP book-cooking—how it happens and how to stop it..... 5
- **THE CON'S LATEST PLOY**
Law-enforcement successes from around the country..... 7

Toby J. F Bishop and Frank E. Hydoski, *Deloitte*

Essentials of Fraud Detection Monitoring



It is common sense that any policy, procedure, technique or automated solution designed to prevent fraud is only as effective as its implementation and sustainment, and still is likely to be imperfect.

Logically, then, some form of fraud detection monitoring is desirable to determine if your organization's efforts to reduce fraudulent activity are working and to help catch those frauds that are not prevented.

Important: There are two key forms of fraud monitoring. One involves monitoring the effectiveness of anti-fraud controls. That is the subject of another article. This article addresses the monitoring of business activities and transactions for potential fraud.

Caution: Though there have been impressive strides in the area of transaction monitoring software, none are perfect. Moreover, since monitoring for fraud should be the responsibility of everyone in the organization, relying on machines to do all this important work could cause red flags of fraud that are best caught by people "in the trenches" to be missed.

That is why management should consider strongly encouraging employees to assist in monitoring for signs of potential fraud. This is not to say that you and your employees should not trust anyone you work with. However, since the Association of Certified Fraud Examiners found in its 2008 study of 959 frauds reported by its members that the number one way in which internal frauds are detected is through

tips—mainly from employees—it is extremely valuable for employees to adopt a constructive attitude of skepticism about red flags of potential fraud.

MONITORING MOS

Some key ways in which organizations may be able to improve their fraud detection effectiveness include:

• **Enhancing whistle-blower hotlines.** Under Sarbanes Oxley, publicly traded companies are required to have a confidential reporting mechanism such as a whistle-blower hotline in place for employees to report fraud.

However, in the Deloitte Forensic Center's 2007 study, *Ten Things About Fraud Control*, which surveyed executives involved with fraud control, only 32% of the 277 respondents felt that their hotlines were "very effective." This suggests that an opportunity exists to raise hotline performance at many organizations.

Potential problems: Companies may be under-communicating to employees the existence and purpose of their hotline or neglecting to train employees to recognize red flags of fraud that can be reported via the hotline.

Another problem may be failure to convince employees that by using the hotline they will not incur retaliation.

Bottom line: In many cases, the elements of a whistle-blower hotline program may not be performing as well as they could be, particularly if employees were trained to detect and report potential fraud.

•**Expanding internal audits for fraud.** The internal audit function might increase its focus on detecting fraud where significant fraud risks are identified in the organization's risk assessment.

Helpfully, earlier this year, the Institute of Internal Auditors disseminated its new International Professional Practices Framework with authoritative guidance including mandatory standards (the "Standards"). A new standard states that "The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk." The chief audit executive is also required to report periodically to senior management and the board on the organization's significant risks, including fraud risks. The Standards further require that internal auditors "consider the probability of significant errors, fraud, non-compliance and other exposures" when planning each internal audit engagement.

Key: Companies should consider taking substantive steps to monitor for fraudulent activity by applying the Standards and asking their internal auditors to assess and address fraud risks as part of their regular audit work.

Aim: To integrate active fraud detection into the day-to-day activities of your internal auditors.

Segregation of Duties in an Information-Intense Environment

The principles of segregation of duties in an information systems environment are critical as they ensure the separation of key computerized functions such as transaction entry, on-line approval of transactions, master file initiation, master file maintenance, user access rights and review of transactions.

Key: This means that one individual should not have computer system access rights which permit him or her to enter, approve and review transactions. Thus, assigning different security profiles to individuals supports the principle of segregation of duties.

White-Collar Crime-Fighter source:

Christine Doxey, vice president of business development, Business Strategy Inc., a Grand Rapids, Michigan-based transaction control and payment procurement consulting firm, www.businessstrategy.com.

•**Deploying technology-based fraud detection.** As mentioned above, there have been great strides in the effectiveness of computer-based fraud monitoring. These include continuous transaction monitoring for fraud (see below), data mining and data analytics.

Key: Commonly used data mining and analytics programs such as ACL and IDEA can be used to screen substantial volumes of your organization's transaction data for anomalies that may indicate potential frauds involving procurement, payroll, expenses, billing, money laundering and conflicts of interest, among others.

An ongoing challenge for the developers of fraud-monitoring software has

A new standard states that "The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk."

been the accuracy and variety of the data being used by these programs. So while these tools can greatly enhance fraud detection capabilities, they cannot detect all frauds and they may flag many items for manual follow-up, which can be time-consuming. A cost/benefit balance will likely have to be struck when using such tools, though the benefits include fraud deterrence and enhanced risk management as well as the value of frauds detected and stopped.

This brings us to the critical elements of...

•**Strengthening manual monitoring.** This method is an important complement to automated monitoring in many cases. It is especially cost-effective when transaction volume is low or the variety of transactions is high.

Example: Financial statement fraud. Progress toward automated screening for anomalies in accounting and financial reporting is being made, such as with automated journal entry testing tools. But an internal auditor's trained and skeptical eye is still valuable for monitoring for signs of improper revenue recognition, accounts payable fraud, kickback schemes, fictitious sales, channel stuffing and other types of record falsification.

•**Considering continuous fraud**

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

Tom Mahoney, Merchant 911.org

Forensic Accounting

Stephen A. Pedneault, Forensic Accounting Services, LLC

Fraud and Cyber-Law

Patricia S. Eyres, Esq., Litigation Management & Training Services Inc.

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, Deputy District Attorney Denver District Attorney's Office, Economic Crime Unit

Computer and Internet Investigation

Donald Allison, Senior Consultant, Stroz Friedberg LLC

Fraud Auditing

Tommie W. Singleton, PhD University of Alabama at Birmingham

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: \$295/yr. Canada, \$345. Copyright © 2009 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 preventing economic crime.

This community includes full internal auditors...fraud examiners...regulatory officials...corporate security professionals...senior executives...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.

monitoring (CFM). This variety of automated fraud monitoring differs from the data mining and analytics programs discussed above in that it is designed to screen for suspicious anomalies on a constant, transaction-by-transaction basis. The greatest advantage of this tool is that it offers near-real-time detection of potential fraud and can be programmed to flag transactions for analysis or cancel

The elements of a whistle-blower hotline program may not be performing as well as they could be

individual transactions before completion.

This can also help operations managers or the internal audit function to detect fraud much more quickly than when relying on periodic or random audits or sampling. It can also help reduce the risk of a fraudulent transaction being overlooked by traditional monitoring methods.

Drawbacks: Despite its estimable advantages, CFM may not be as cost-effective for smaller organizations because of the investment required. In addition, a CFM system is only as effective as the professionals who are responsible for reviewing flagged transactions and assessing them for fraud, so having a skilled anti-fraud or internal audit function is important. 

White-Collar Crime Fighter sources:

Toby J.F. Bishop, Director, Deloitte Forensic Center for Deloitte Financial Advisory Services LLP, and Frank E. Hydoski, Leader, Analytic and Forensic Technology practice at Deloitte Financial Advisory Services LLP. Toby and Frank are coauthors of *Corporate Resiliency: Managing the Growing Risk of Fraud and Corruption*, published by Wiley, www.wiley.com, on which this article is in part based. This article is based on the views of the book's coauthors and do not necessarily reflect those of Deloitte.

Preventing and Detecting Fraud in Accounts Payable

By Peter Goldmann

This book provides invaluable insight into how fraudsters exploit AP and how to stop them! Visit www.iappnet.org.

ONE STEP AHEAD

Sharie Brown, *DLA Piper*

DOING MORE WITH LESS

Effective Fraud Prevention in a Limited-Resources Environment



It has been widely reported in the press (including this publication) that financial fraud, though costly enough during good economic times, becomes a substantially greater threat when the economy is in recession.

Making matters riskier, in the wake of several high-profile criminal cases, the federal government—specifically the SEC and Department of Justice—have vowed to crack down on numerous varieties of securities fraud, financial crime and international corruption.

If you accept all of this, the critical next question is: How do you protect your organization from this growing dual threat of elevated fraud risk and increased risk of enforcement action when you are forced to slash costs to weather the downturn?

Fortunately, there are numerous ways of actually bolstering your anti-fraud defenses without added expense. Some of the most effective steps to take now...

- **Re-assess your greatest business unit fraud risks and reallocate detection and prevention resources accordingly.** Even if you've recently done a fraud risk assessment, this may be an ideal time to update it to pinpoint areas where your organization is most vulnerable to fraud or enforcement risk in the current economic climate.

These typically include...

- **Embezzlement.** Employees fearful of losing their jobs or who observe misconduct at senior levels of the organization are more likely to exploit internal controls.

- **Kickback schemes involving dishonest vendors.** Vendors are becoming increasingly aggressive about maintaining existing customers and winning new ones. Some sales reps will cut ethical corners by offering

your procurement staff financial “incentives” to channel business their way.

Example: One of your organization's senior purchasing managers is approached by a competitor of your current office supplies vendor with an offer to provide a sizeable discount on many of the products you purchase. The vendor also offers an “incentive” in the form of a monthly kickback of a portion of the savings that will result from the switch in vendors.

- **Financial statement fraud and intellectual property theft.** (See *White-Collar Crime Fighter*, April 2009, page 1.) When times are tough and financial performance is under pressure, the temptation for management to embellish financial reports increases.

- **Paying bribes to overseas officials** to obtain business or secure an improper advantage.

- **Travel and entertainment expense abuse.** Executives at home and abroad may abuse their expense privileges for personal gain or to secure business in illegal ways.

- **Allowing key controls to be circumvented,** ostensibly to save time and expense. This is a dilution of anti-fraud controls and can invite abuse by dishonest insiders.

Example: A payroll services employee, knowing that management has shifted its focus away from internal controls, may decide to use his access to the organization's payroll system without going through the normal due diligence and documentation procedures for approving new employees by adding a “ghost” employee to the payroll and having the “new” employee's paychecks deposited directly into his own account (knowing from previous

Continued on pg. 4

AUDITORS VERSUS FRAUD

Are Your Statements “Clean”?

Audited financial statements are essential because they reduce the end-user's cost of capital.

Reason: Audited statements reduce the end-user's assessed risk.

Example: A bank receives loan requests from two companies, identical in every respect, except that one has audited statements and the other doesn't. All things being equal, the bank will charge a lower rate of interest, and possibly impose less onerous covenants on the company with the audited statements.

So where does audited financial statement value come from? *There are two standards...*

- The numbers are fairly presented—not materially misstated. To most users this is synonymous with “accurate.”

- The numbers are “legitimate.” Even if the financial statements receive a “clean” opinion, if the bank loan officer or other end-user doesn't believe the numbers are legitimate, the statements have no value.

Critical: To establish “legitimacy” value, according to Statement of Accounting Standards (SAS) 107, “Audit Risk and Materiality in Conducting an Audit,” the key is *auditor independence*.

ESSENTIALS OF INDEPENDENCE

- Lack of bias.** Unfortunately, with respect to bias, our profession's model is fundamentally flawed. Who pays for the work? The client. What's the flaw? It is hard to be impartial about a paying client's financial records.

Challenge: Until the audit profession develops another payment mechanism, our independence will always be suspect.

- Intellectual honesty.** Have you ever had a client who treats the organization as their own personal piggy bank? If your answer is “yes,” and you let your client charge personal expenses to the entity, it's a violation of SAS No. 1. Why? Because you've knowingly allowed your client to vio-

late his or her own internal controls. This represents intellectual dishonesty by the auditor.

Challenge: Auditors must resist the “easy way out” when it comes to confronting their clients' efforts to violate internal controls and tax laws.

Critical: Paragraph 10 of SAS 107 states, “When the auditor encounters evi-


Just because the deduction is immaterial for financial reporting does not mean it is legal

dence of potential fraud, regardless of its materiality, the auditor should consider the implications for the integrity of management or employees and the possible effect on other aspects of the audit.”

Key: Just because the deduction is immaterial for financial reporting does not mean it is legal. Legality and materiality are two different things. How can auditors render a clean and independent opinion knowing the financial statements are misstated by *any* illegal amount? Doing so is willful because you detect the deduction but do nothing about it.

- Avoid situations that lead others to question your independence.** SAS 107 defines materiality as “the magnitude of an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the omission or misstatement.”

Important: No percentage or amount is included in the definition. If end-users would make a different decision if the numbers were right, then the amount, transaction or event is material.

Lesson: If you aren't willing to walk away, lose a client, or refuse to let a client cheat, even if by only a small amount, how can you sign the opinion saying you're independent? 

White-Collar Crime Fighter source: Gary D. Zeune, CPA. Gary is a nationally recognized speaker and writer on fraud and auditing, and founder of The Pros & The Cons, the nation's only speakers' bureau for white-collar criminals. He has taught fraud classes for the FBI and more than 250 professional associations. He can be reached at gzfraud@bigfoot.com.

Continued from page 3

experience that his bank does not match employee names with account holder names).

- Instruct your internal audit team to re-prioritize its audit objectives** to more aggressively screen for red flags of these and other types of fraud that are most common to a particular business unit. Unfortunately, during economic downturns, there is an increase in the number and variety of frauds threatening organizations. This makes internal audit's job that much tougher during these periods.

Specifically, direct your internal audit team to concentrate its activities on the fraud risks listed above, and others that you identify which become especially pronounced during economic downturns.

REINFORCING COMPLIANCE AND CONTROLS

The message is that rather than cutting budgets for fraud prevention, now is the time to strengthen those defenses.

- Enhance due diligence with respect to potential new agents and business partnerships,** especially those involving overseas entities. During recessions it is tempting to cut back on costly examination of a prospective business partner's or vendor's background and business profile. However, during tough times, it is especially important to conduct this critical exercise. Think of the expense as an investment in insurance against potentially costly legal and regulatory trouble down the road.

Example: Some organizations cut costs during slowdowns by limiting due diligence to Internet-based resources. This creates the likelihood of missing as much as 50% of the critical background information about institutions that your organization has not done business with before. The obvious risk is that you'll miss facts that could result in legal problems down the road.

- Conduct more rigorous employee background checks.** This is the time when job-hunters are likelier than usual to embellish their resumes with false qualifications. It is also extremely important for your organization to ensure that it does not place an employee with a blemished background in a position of financial responsibility. This applies to existing employees as well. Spend the extra few dollars to do an updated back-

Continued on page 5

PAYABLES PLOYS

Continued from page 4


ground check on an employee who is being promoted to a position of enhanced financial responsibility. Look for negative changes in their credit history, legal claims on property or other red flags of trouble that could translate into financial pressure.

- **Train personnel outside of internal audit to assist in fraud detection and prevention.** Your legal team, tax team and security personnel can often be readily “deputized” to support internal audit in detecting fraud.

Example: Your legal department should be familiar with the key US anti-fraud, racketeering, corruption and civil legal standards that can be invoked when employees are caught committing illegal acts. If in-house attorneys lack familiarity with these laws, implement professional training to remedy this.

Another cost-free way to bolster your anti-fraud defenses is to train your physical security team to detect and investigate employee crime. This training should focus on improved surveillance methods for detecting cash larceny, theft of inventory, diversion of shipments, etc.

Finally, bring your tax and accounting department into the anti-fraud effort. Have them trained in the tax laws of countries in which the organization has business activities. Disputes over the tax aspects of alleged bribery, kickbacks, side payments to foreign revenue officials or other corrupt practices can present the need for such legal expertise which would otherwise have to be obtained from outside counsel.

- **Build employee awareness about fraud.** Your employees should be the eyes and ears of the organization with respect to illegal conduct. But their effectiveness in this role is only as great as the level of knowledge they have. Training them in the red flags of common frauds and about how to use your whistle-blower hotline and other reporting channels (as well as their legal protections against retribution) is another low-cost but potentially high-impact method of reducing fraud risk in a tough economy. 

White-Collar Crime Fighter source:

Sharie Brown, Esq., chair of the Foreign Corrupt Practices Act (FCPA), Anti-Corruption and Corporate Compliance practice group and a partner in DLA Piper’s Litigation practice, based in Washington, DC. She can be reached at sharie.brown@dlapiper.com.

ACCOUNTS PAYABLE BOOK-COOKING

How it Happens and How to Stop It



In virtually every major corporate scandal, “cooking the books” has been a key element of the criminal charges against the company. Frequently, accounts payable (AP) records are manipulated to perpetrate these accounting schemes.

Example: The amount of accounts payable is falsely inflated for a specific accounting period to support similarly falsified increases in sales.

Key: Inflating revenues is among the most common forms of book-cooking, and when AP levels remain “normal” while sales are increasing, this can raise a red flag for astute auditors.

Additional AP book-cooking example:

- **Recording purchases in an accounting period other than the one in which the purchas-**

es were actually made can make the liability side of the balance sheet appear healthier than it really is.

- **Failing to record expenses altogether.** By simply neglecting to record expenses and “burying” vendor invoices, management can make it appear as though expenses for a particular reporting period are lower than they actually are, thereby making earnings appear greater than they are.

- **Classifying expenses as capital expenditures.** This results in converting liabilities into assets.

Example: The case of Buca Inc., which operates a chain of Italian restaurants called Buca di Beppo.

The company was investigated and ultimately sued by the SEC on charges of so-called earnings manipulation, which top management perpetrated in order to portray Buca as what the com-

mission called a “growth company in sound financial condition.”

According to federal court documents, the SEC charged, among other things, that:

“Beginning in 2000, [former Chief Financial Officer Greg] Gadel preliminarily assessed Buca’s financials at the close of each quarter to determine how much income he needed to “find” to meet Wall Street analysts’ earnings expectations. Gadel pressured Buca’s controller to “hit whatever earnings had been projected” by Wall Street. To fill any “gap,” [top management] concocted a scheme to reduce Buca’s costs through

By simply neglecting to record expenses and “burying” vendor invoices, management can make it appear as though expenses for a particular reporting period are lower than they actually are

improper capitalization of expenses. ... They merely took ordinary expenses, which are required to be expensed in the period in which they are incurred, and treated such expenses as capital expenses, which are expensed over extended financial reporting periods. The impact can be significant. For example, a \$25,000 expense capitalized over 10 years amounts to a cost of \$2,500 in the current year.

This scheme was effective. In 11 of 13 quarters, Buca either exactly met Wall Street estimates or exceeded them by a single penny. However, in its restatement, Buca admitted that this fraudulent scheme caused it to overstate earnings by \$12.6 million from fiscal year 2000 to 2003. The overstatement during this period was extraordinary—from 29% to 58% of earnings each fiscal year.”*

AP BOOK-COOKING RED FLAGS...

- **A pattern of unusually high expenses at the end of an account-**

**In re Buca, Inc. Securities Litigation*, case No. 05-ev-1762 Dwf1A, b.

Continued on page 6

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



Anti-Fraud Lessons from the Subprime Crisis

Recently, TV journalist Bill Moyers interviewed one of the most knowledgeable and experienced mortgage fraud experts in the country, William K. Black. Among his countless accomplishments is the famous book, *The Best Way to Rob a Bank Is to Own One* in which he meticulously chronicled the smorgasbord of frauds perpetrated by crooked bankers in the savings and loan crisis of the 1980s.

In his interview with Moyers, Black placed much of the blame for the subprime meltdown on outright fraud. In regard to the subprime crisis, Black told Moyers, "...the essence of fraud is, 'I create trust in you, and then I betray that trust, and get you to give me something of value.' And as a result, there's no more effective acid against trust than fraud, especially fraud by top elites, and that's what we have."

Asked by Moyers how fraud was perpetrated to create the subprime meltdown, Black put it very simply:

"...the way that you do it is to make really bad loans, because they pay better. Then you grow extremely rapidly, in other words, you're a Ponzi-like scheme. And the third thing you do is we call it leverage. That just means borrowing a lot of money, and the combination creates a situation where you have guaranteed record profits in the early years. That makes you rich, through the bonuses that modern executive compensation has produced. It also makes it inevitable that there's going to be a disaster down the road."

Asked by Moyers if he meant that bank executives deliberately set out to make bad loans in order to increase their own income, Black answered, "Yes." Moyers then wanted Black's take on how the bank bosses got away with this, to which Black clearly referenced *Tone at the Top*: "All of those checks and balances report to the CEO, so if the CEO goes bad, all of the checks and balances are easily overcome. And the art form is not simply to defeat those internal controls, but to suborn them, to turn them into your greatest allies. And the bonus programs are exactly how you do that."

"The Bush Administration essentially got rid of regulation, so if nobody was looking, you were able to do this with impunity."

Lesson: With poor *Tone at the Top* and no anti-fraud controls, the "acid" of fraud which Black references inevitably leaks into the system. This system does not have to be some mundane operations, logistics or human resources system. It can—and all too often is—the system of running an organization at the very top...

White-Collar Crime Fighter source: William K. Black, interviewed by Bill Moyers, April 3, 2009, on *The Bill Moyers Journal*, www.pbs.org/moyers/journal/i. Black is author of *The Best Way To Rob A Bank Is To Own One*, teaches economics and law at the University of Missouri—Kansas City (UMKC). He was the Executive Director of the Institute for Fraud Prevention from 2005–2007. Black was litigation director of the Federal Home Loan Bank Board, deputy director of the FSLIC, SVP and general counsel of the Federal Home Loan Bank of San Francisco, and senior deputy chief counsel, Office of Thrift Supervision.

Red Flags of a Potentially Bogus Social Security Number

- Issue date is inconsistent with the borrower's age.
- Three or more leading zeros.
- Zeros in positions 4 and 5.
- Numbers ending in 4 zeros.
- A leading number of 73 through 79.
- A leading number of 8 or 9.

White-Collar Crime Fighter source: *Fraud Prevention Strategies For Consumer, Commercial And Mortgage Loan Departments*, Report by BITS Fraud Reduction Steering Committee, BITS, financial services consortium, www.bits.org.

Continued from page 5

ing period. This could mean that management is trying to "get rid" of cash budgeted for a specific period even though it has no need for what is purchased.

• **New, strange-sounding vendors appear on the vendor master file.** This may signal the fraudulent addition of a sham vendor.

• **Sudden drops in days purchases in accounts payable.** This is another sign of potential falsification of expenses.

• **Unusually low costs for routine projects.** This may indicate falsification of expenses.

• **Unusual budget excess at the end of a budget period.** This could be another sign of misrepresentation of expenses and liabilities.

• **Sudden or abnormal increases develop in gross margins—**especially when compared with margins in the rest of the industry or those of direct competitors.

• **Accounts payable is declining** while competitors are experiencing growing AP as they stretch out payments to vendors.

• **Unusually low expenses and increased capital expenses.** This is a sign of expenses being fraudulently classified in the financial records as long-term capital expenditures. Low expenses may also be a red flag of failure to record expenses and "burying" or destroying the invoices to make the financial records falsely reflect higher earnings.

• **Clear existence of two sets of accounting records** and of earnings manipulation. This is most commonly found in privately owned businesses.

BOOK-COOKING CONTROLS...

• **Immediately document all purchasing databases** and shipping documents with details of goods received (billing/shell company schemes, inventory fraud, book-cooking).

• **Conduct detailed reviews of purchasing/procurement records** to detect unusual pricing for certain vendors—before payment is made (kickback/bribery schemes, billing schemes, shell companies).

• **Conduct surprise audits.** When dishonest employees are aware of scheduled audits, it's easy for them to conceal their fraudulent activities before the auditors arrive.

Solution: Unannounced audits by external auditors or fraud examiners.

Continued on page 7

Continued from page 6

Doing these once or twice a year and telling employees only that they can expect such an audit at any time puts a powerful anti-fraud deterrent into place.

•**Regular internal audits.** There is growing pressure on internal auditors to focus on the detection of illegal activity—with AP fraud ranking high on the list of such behaviors.

Specific AP fraud audit measures are numerous, but internal auditors should start by adopting the widely recognized mindset of “professional skepticism” in determining the existence and seriousness of fraud risks in their regular internal audits.

This approach will serve auditors well as they move on to perform the following fraud detection activities:

•**Ratio analysis of the organization’s AP-related financial records.** This involves quantifying the relationship between two different financial statement amounts.

Key: When anomalies are found from one accounting period to the next in any of the following basic financial ratios, there is reason to dig deeper for evidence of fraud...

□ **Current ratio.** This is the ratio of current assets compared to current liabilities. A check fraud embezzlement scheme or other internal theft usually will create an unusual drop in the ratio.

□ **Inventory turnover,** or cost of goods sold compared with average inventory. If an employee is stealing inventory, the ratio will jump, as missing inventory is written off and the resulting cost of goods sold increases.

□ **Debt-to-equity ratio**—total liabilities compared with total equity. If this ratio is increasing, along with a comparable increase in accounts payable, it may mean phony invoicing or another fraud is causing total liabilities to spike.

□ **Margin analysis**—sales minus cost of goods sold. If embezzlement or another form of AP fraud is in progress, cost of goods sold will rise, which, in turn, will reduce the margin to an unusual level.

•**Horizontal analysis.** This involves assessment of patterns in specific accounts such as sales and expenses. If sales are increasing unusually rapidly while expenses are declining, there is a possibility that a fraud or book-cooking scheme is going on. 📌

White-Collar Crime Fighter source:

Peter Goldmann, Editor, White-Collar Crime Fighter, Ridgefield, CT. He is author of *Preventing and Detecting Fraud in Accounts Payable*, International Accounts Payable Professionals, (IAPP), 2009, www.iappnet.org. This article is based in part on excerpts from the book.



THE CON'S LATEST PLOY...

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

Baltimore, MD

Bank teller's routine cash thefts total over \$1 million over five years. Karen L. Baer, age 46, of Westminster, MD, pleaded guilty to bank fraud in connection with a scheme to steal at least \$400,000 from the bank where she worked.

According to United States Attorney for the District of Maryland Rod J. Rosenstein, Baer stole more than \$1 million in the course of her scheme.

According to her guilty plea, from 1998 until her termination on October 25, 2007, Baer was a teller at PNC Bank or one of two banks, Westminster Union Bank and Mercantile Bank that PNC was acquiring. She was the teller supervisor of the 140 Village Shopping Center branch in a Baltimore suburb at the time of her termination.

Beginning in June 2002, Baer allegedly stole cash from the branch, usually \$10,000 at a time. To conceal her thefts, Baer made false entries in a “Due from Mercantile” account, creating false debit and credit tickets purporting to reflect cash shipments sent from the 140 Village branch to the Federal Reserve, and cash shipments received by the 140 Village branch from the Federal Reserve. In fact no cash shipments were made.

Baer reportedly made at least several hundred fraudulent debits and corresponding credits to make her initial theft difficult to detect and to hide additional thefts. In total, the scheme resulted in losses to PNC of \$1,050,000.

Baer's fraud was uncovered when PNC began an audit in September 2007 in connection with its acquisition of Mercantile Bank. PNC's auditors discovered \$1,050,000 in unaccounted funds. Further investigation revealed the pattern of suspect debit and credit tickets signed by Baer.

In October 2007 when a PNC inves-

tigator confronted Baer concerning these allegations, she admitted that she had been stealing money from the bank since 2002. She told FBI agents in subsequent interviews that she took \$10,000 from her teller drawer on at least a monthly basis. She said that she used the stolen funds for living expenses, vacations and college tuition for her children. She also admitted that she forged another bank employee's name on several of the credit tickets.

As part of her plea agreement, Baer agreed to forfeit her interest in a home, nine bank accounts, a 2004 Hummer H2, a Chevrolet Corvette, several snowmobiles and all terrain vehicles.

Baer faces a maximum sentence of 30 years in prison and a \$1 million fine.

Miami, FL

International card gang went to town to the tune of \$75 million. Four members of a South Florida-based criminal gang generated \$75 million in credit card fraud losses were arrested by the U.S. Secret Service.

More than 200,000 credit card account numbers, two pickup trucks, about \$10,000 in cash and one handgun were also recovered in connection with the gang's activity, according to a Secret Service statement.

The gang was discovered through an earlier investigation by the Secret Service's Miami and Nashville field offices which targeted an individual named Julio Lopez, who used the screen name “Blinky” to traffic in counterfeit credit cards and stolen IDs.

Lopez, based in Hialeah, FL, and his girlfriend, Anett Villar, were arrested earlier, and an investigation into their activities led to the discovery of an

organized fraud ring comprising Cuban nationals operating in South Florida.

The Secret Service reported that the gang sent “large amounts” of money using E-gold accounts to cyber-criminals in Eastern Europe in exchange for “tens of thousands” of stolen credit card numbers. The numbers were then used to create counterfeit cards in several “plants” throughout Florida. (E-Gold is an illegal form of on-line currency).

Disturbing: Christopher Pierson, a partner at the law firm Lewis and Roca LLP in Phoenix and a board member in the local chapter of the FBI’s InfraGard security information-sharing program, said that the arrests show how cyber-crime is becoming more profitable than the illegal drug trade.

“What this shows is the transnational nature of the crime,” Pierson said. “This is a crime that moves across borders and is worldwide and is hitting the U.S. very hard.” It also highlights the highly decentralized way cybercriminals work with different gangs responsible for various aspects of the operation, he said.

Additional perspective: In light of the sophisticated supply chain that exists today for the creation and distribution of malware, some observers like said Andrew Jaquith, an analyst at Yankee Group Research Inc. in Boston say it is no surprise that some elements profit from it. “The fact that they found 200,000 cards doesn’t surprise me,” Jaquith said. “What surprises me is that

they didn’t find more.”

Orem, UT

Technology in the wrong hands is a costly weapon. Zeldon Morris was the controlling partner in the computer consulting firm, Lee & Morris. Morris, who took on Eunyoung Lee as a partner in April 2008, Morris had been retained as an independent contractor by Provo, UT-based Open Solutions Inc., to repair and maintain the data processing systems or Family First Credit Union in Orem.

Morris proceeded to use his estimable technical skills to plunder more than \$1 million from the credit union over a period of about 10 months ending in January 2009 when his crimes were discovered.

Details: According to the indictment, Morris was given passwords by Open Solutions to access the credit union’s computer system at its Orem office and via remote location. For about six months, he accessed the credit union system and executed fraudulent electronic funds transfers, depositing more than \$1 million into his personal accounts and into a business account of Lee & Morris.

An investigation by credit union officials reportedly found that Morris made the fraudulent transfers either by using bogus trace numbers—numbers that, according to banking officials, are “serial number[s] for ACH transaction[s], similar to a check number, that identifies the payment”—or, according

to court documents, by “duplicating other legitimate trace numbers but using fictitious amounts, or by remotely accessing the bank’s system through the ‘E-teller’ system and overriding it to accept deposits” to Morris’s own accounts.

Added details: The sources of the stolen funds were internal general ledger accounts. According to the indictment, Morris transferred the stolen funds to his personal accounts at other financial institutions, and to other businesses or individuals, as well as to a Family First account in the name of his wife.


Among the red flags was the fact that several cashiers’ checks were purchased with the stolen funds, which included the phrase “Re: Zeldon Thomas Morris” on the face of the checks. The endorsements on the checks were either to Morris, or to an account that required his signature.

The bust: Court documents indicate that Family First would not have discovered the fraud scheme if Eunyoung Lee didn’t blow the whistle after investigating odd details in the company’s accounts in October.

Lee initially suspected Morris of embezzling funds from the company after he made suspicious withdrawals and failed to pay Lee for his work.

When he reviewed Morris’s accounts at the credit union, he found several very large deposits that appeared to be “real estate-related.” Morris, who confided in Lee of his financial difficulties, reportedly told Lee that the deposits were proceeds of mortgage refinancings. But Lee said he found no recorded real estate transactions on Utah County online property records, and also found Morris’s original mortgage loans were still outstanding.

Lee informed credit union officials of the suspicious deposits to Morris’s accounts in March 2009 and asked Morris to buy out his interest.

Family First vice president, Jason Craddock said that the institution’s losses were covered by the National Credit Union Association. 



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 \$245. **That’s \$50 off the regular subscription price of \$295!**
Plus, send me—for **FREE**—THREE 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...

- **How to do employee background checks right**
- **Check fraud: Latest prevention methods**
- **Bank loan fraud: Still going strong**
- **Fighting accounts receivable fraud**