

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

VOLUME 12 NO. 8
SEPTEMBER 2010

IN THE NEWS

“Astounding” Crime Results in Slap on Wrist

Something isn't right in the sentencing of former IBM senior vice president Robert Moffat who admitted to participating in the biggest insider trading fraud in US history.

That fraud, involving the massive New York hedge fund firm, Galleon Management, resulted in the apprehension of 21 defendants. Moffat pleaded guilty earlier this year to charges of conspiracy and securities fraud.

Incongruous: Manhattan federal court judge Deborah Batts, in imposing the sentence on Moffat, said he had committed “an outstanding breach of fiduciary duty” to IBM by providing insider financial information to Danielle Chiesi, a Galleon associate with whom he was having an extramarital affair.

Batts added insightfully, that “white-collar crime is just as destructive to the social fabric as drugs and violence.”

True indeed. Why then do individuals caught with a single ounce of crack cocaine get sentenced to a mandatory five years in prison? The only ones they're harming are themselves.

White-Collar Crime Fighter sources:

• *USA v. Moffat*, US District Court for the Southern District of New York, No. 10-00270.

• Media reports on the sentencing proceeding.

IN THIS ISSUE

- **CYBER-CRIME FIGHTER**
Protect against growing threat of insider attack..... 3
- **DOING THE RIGHT THING**
Corporate culture & anti-fraud... 4
- **ETHICS OR FRAUD?**
The confusing line between ethics and fraud 5
- **THE CON'S LATEST PLOY**
Law-enforcement successes from around the country..... 7

Paul McCormack, CFE, *Innovar Partners*

Essentials of a Highly Effective Organization-Wide Anti-Fraud Program



The good news is that, motivated by concern—even fear—of being victimized by fraudsters whose exploits have been gaining increasing media attention in recent years, many organizations are finally investing in the financial and human resources necessary to protect against this risk.

The bad news is that, despite these augmented anti-fraud initiatives, too many organizations are falling short of truly effective protection against the inexorable spread of economic crime.

Common reason: Often, several of the essential elements of a fraud program exist but management fails to fully integrate these elements across the organization. It is not unusual to find fragmented detection and investigation procedures and policies spread throughout an organization with each area unable to make meaningful progress on its own.

Result: Without an integrated fraud program in place, the organization is forced to fight fraud in a reactive mode, rather than a preventive one, and is thus always one step behind the fraudsters.

BETTER WAY

With clearly defined roles and responsibilities in fraud detection and prevention, duplication of effort is eradicated and is replaced with an efficient and effective alignment of people, processes and technology. The organization can then implement specific detec-

tion analytics and carefully designed risk-based controls that “takes the fight” to the fraudsters, both internally and externally.

Such a high-impact fraud program typically contains these elements:

• **Detection.** Proactive fraud detection today requires a fine-tuned combination of automated and manual measures. Depending on the industry, there are a number of third-party fraud detection software tools that can analyze transaction data and identify anomalies or patterns that may be signs of fraudulent activity.

To gain maximum “bang for the buck,” it is also important to implement initial and ongoing training of your fraud detection staff that will be using the tool.

In addition, designating an internal fraud detection “point person” such as the chief internal auditor, controller or security manager and providing the necessary fraud detection training is increasingly unavoidable in today's climate of rampant fraud.

Important: Ongoing employee fraud training that addresses both internal and external fraud prevention. Employees are the organization's first line of defense against fraud because they have a direct view of red flags and hard evidence of fraud and are therefore in the best position to report suspicious activity via the organization's hotline.

Often several of the essential elements of a fraud program exist but management fails to fully integrate these elements across the organization

Key lesson: Taking the time to educate employees about the types of fraud threatening the organization and the red flags for spotting them can quickly pay dividends in uncovering ongoing fraud—as long as an effective employee hotline is in place for reporting incidents.

•**Investigation.** Once a fraud has been uncovered, employing a dedicated team of highly trained fraud investigators will result in better analysis that results in actionable intelligence the organization can use to improve its control environment, as well as potentially lower losses by way of faster, more effective recovery of fraud losses. To support the investigation process, implementing a robust case management system is essential.

Key: A well-designed case management system can not only house the results of an investigation, it can also be used to establish investigator performance metrics, provide data to support changes in

internal controls and facilitate the redesign of technology or services the organization offers to reduce fraud risk. In order to avoid duplication of effort, each department involved in the investigation process must have a clearly defined role and set of responsibilities.

•**Prevention.** Prevention starts with a rigorous new-hire screening process and a code of conduct that is frequently circulated and referenced by executives. The code of conduct must include a policy detailing the organization's "zero tolerance" stance toward both internal and external fraud as well as policies for investigating, disciplining and/or prosecuting offenders.

Note: Obvious as it may sound, prevention hinges critically on a system of scenario-specific and continuously updated anti-fraud controls. For companies subject to Sarbanes-Oxley compliance, a framework of anti-fraud internal controls is mandatory. For others, though, such a framework is equally critical.

Caution: Implementing controls is not enough. Management has a tendency to become complacent about its anti-fraud controls once they are in place. As soon as fraudsters sense that controls are neither enforced nor updated, they will begin exploiting the resulting weaknesses in such controls to commit fraud.

Problem: Implementing changes in the internal control environment often encounters employee resistance. However, focusing on detection and investigation at the expense of remediating weaknesses in internal controls is potentially costly.

A well-defined development and deployment program that is supported by quantitative and qualitative information will result in a stronger internal control environment that ultimately prevents more fraud.

Key: Such information is best gathered by conducting a thorough fraud risk assessment (FRA). Depending on changes taking place in the organization's operating environment, the frequency with which risk assessments are conducted will vary.

However, the essential outcome of all FRAs is a complete understanding of new or ongoing vulnerabilities to specific fraud scenarios so that continuous refine-

Employees are the organization's first line of defense against fraud because they have a direct view of red flags and hard evidence of fraud

WHITE-COLLAR CRIME FIGHTER

Editor
Peter Goldmann, MSc, CFE
Consulting Editor
Jane Y. Kusic
Managing Editor
Juliann Lutinski
Senior Contributing Editor
David Simpson
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.A. (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 © 2010 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 law 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.

"DETECTING AND PREVENTING FRAUD IN TODAY'S HIGH-CRIME CLIMATE"

A SPECIAL "HOW-TO" LEARNING SERIES FROM AUDITNET AND FRAUDAWARE

Get Expert Advice on how to stay a step ahead of fraudsters with proven tactics and techniques.

After completing this carefully designed series of 12 high-impact Webinars featuring the anti-fraud profession's top experts, your auditors, investigators, accounting staff, financial personnel, compliance officers and senior management teams will have a unique body of knowledge, skills and abilities to launch highly effective initiatives that beat fraudsters at their own games—affordably and efficiently.

Sign up now for this unique series of learning sessions that gets right to the brass tacks of using your organization's resources to safeguard its financial, intellectual and physical assets from the growing army of fraudsters.

For full details, dates, CPE credits and registration options, **PLUS VALUABLE FREE BONUSES** please visit <http://www.auditnet.org/FASTPACKdm.htm>

ment and adaptation of internal controls can be accomplished. 

White-Collar Crime Fighter source:

Paul McCormack, CFE, a partner at Innovar Partners where he leads the firms' fraud practice. Paul is also former vice president of Fraud Detection for SunTrust Banks in Georgia. He can be reached at pmccormack@innovarpartners.com.

McCormack On: Overcoming Resistance

As your anti-fraud team continuously identifies fraud risks, their objections will inevitably be raised to any proposed changes in the organization's internal controls. The objections will vary depending on the pertinent manager's area of responsibility and previous experience in fraud prevention.

Helpful: Before implementing changes to your anti-fraud controls, hear out objections and formulate workable responses with the cooperation of line management.

Also consider designating an executive sponsor to champion the effort. In addition, there should be a clearly documented project charter that details the specific goals of the initiative as well as key stakeholders in the process. Finally, there should be regular status reporting to ensure that changes are consistent with the goals previously agreed to by the sponsor and key stakeholders.

Mini case study: For each purchase made by customers of a major European retailer, the patrons earned loyalty points that could be redeemed for gift certificates at the company stores.

The retailer began hearing from customers—often ones who had not made use of their accounts in several months—that their points had been redeemed without approval.

Action steps: Management assembled an anti-fraud team comprising internal audit, corporate security, human resources and loyalty program management. The steps needed to combat the fraud were thus quickly identified and agreed upon. This led to implementation of fraud detection reporting focused on uncovering the guilty employees, improvement of internal controls associated with the loyalty program and improved use of technology to protect dormant loyalty accounts.

Result: After several months, the level of loyalty account fraud had declined by 98%.

Lesson learned: Without creation of the anti-fraud program, changes needed to protect the loyalty accounts may not have been implemented.

CYBER-CRIME FIGHTER

Insider Cyber-Crime: How to Protect Against the Growing Threat



Definition of the “insider threat”: A current or former employee, contractor or business partner with access to your systems who commits fraud or causes other types of harm to the victim organization.

Three main types of insider cyber-criminals:

1. Insider IT saboteurs. These insiders wipe out data, bring down a system or use your system to harm an individual. Typical perpetrators include system administrators or database administrators with the know-how to cause high-tech crime.

Common characteristics: More than 90% are male, many of whom don't get along with others. This personality anomaly is a key psychological predisposition that motivates the individual to commit a crime if an unfavorable “precipitating” layoff or a similar event causes disgruntlement that triggers the malicious behavior. They are not responsive to normal discipline. Instead, they become increasingly disgruntled as time passes. This causes them to set up back-door access to your systems so they can commit sabotage whenever they want to.

2. Insider fraudsters. Employees who steal proprietary information—often personally identifiable information—or who use your system to manipulate payroll or vendor computer systems to embezzle funds. Insider fraud accounts for 40% of the insider cyber-crimes in the respected Carnegie Mellon Software Engineering Institute CERT incident database. Perpetrators are mostly lower-level employees who are easy to recruit by others or who are IT administrators with access to information that can be sold on the black market. Approximately one-half are male and one-half female.

Fifty percent are recruited by outsiders to commit collusive fraud or steal information for sale by the outsider such as customer credit card data.

3. Internal intellectual property thieves. These insiders engage in industrial espionage and steal customer lists, scientific formulas, marketing secrets and trade secrets.

Perpetrators typically include employees who work directly with the targeted information. They thus feel entitled to it when adverse events occur, such as downsizing or budget reductions.

Result: They look for a job with a competitor or plan their own businesses. Stealing the information occurs when they leave, rationalizing the crime by convincing themselves that the victim company “deserves” it.

Typical: Information is stolen within 30 days of announcing they are leaving the organization.

PREVENTIVE PRACTICES

Practice 1: Consider threats from insiders in enterprise-wide risk assessments. Insiders' access, combined with their knowledge of the organization's technical vulnerabilities and vulnerabilities introduced by gaps in business processes, gives them the opportunity to carry out malicious activity if properly motivated.

Solution: Determine the entire enterprise's critical assets, then define a risk management strategy for protecting the assets from insiders *and* outsiders.

Practice 2: Clearly document and consistently enforce technical and organizational policies and controls.

Key: In cases of insider cyber-crime studied by CERT, some employees felt they were being treated differently than

DOING THE RIGHT THING

David Gebler, *Skout Group LLC*

CORPORATE CULTURE

Pivotal to Anti-Fraud Efforts

While the link between an organization's ethics and its culture is well established, creating a corporate culture that both promotes and values ethical behavior is never easy.

Caution: While setting behavioral standards by distributing a well-written code of conduct and engaging in ongoing internal communications is necessary, to have employees adhere to ethical behavior, organizations must go beyond talking about the rules, and address the motives that drive good people to do bad things.

ETHICS VS. COMPLIANCE

Knowing the rules does not mean people will follow them. Do you always adhere to the speed limit when you drive? If you are inclined to speed, will seeing more "Speed Limit" signs make you slow down?

Stricter enforcement will deter some unethical or illegal behavior, but what kind of organization has ethics police parked at the end of every cubicle?

The key to running a fraud-proof organization is to look less at the rules and more at what keeps people from following them. *To do that, it is necessary to understand a few essential aspects of human nature:*

- People are basically good but they are all vulnerable to pressure and are prone to rationalize actions when given the chance.

- People are frequently torn between a desire to succeed and a desire to do the right thing. Management's focus should therefore be on training managers to create a corporate environment that encourages employees to do what they would like to do—but often feel pressured not to. *Creating this culture requires the following key steps:*

- **Move the cookie jar.** Humans have been vulnerable to temptation since Adam and Eve. By implementing anti-fraud controls and maintaining

clear ethics standards, your employees will more likely resist the temptation to cheat.

Problem: The power of rationalization is so strong that most people can convince themselves that, for instance, taking what doesn't belong to them won't hurt anyone. Organizations can help diffuse rationalization by acknowledging the

People are basically good but they are all vulnerable to pressure and are prone to rationalize actions when given the chance

specific issues that tend to get people into trouble.

Effective:

Discuss the specific reasons individuals cut ethical or legal

corners or fudge reports. Open discussion often can be enough to deter many managers from engaging in that behavior.

- **Be fair.** Perception of unfairness is one of the major reasons why people rationalize unethical or illegal conduct. When someone feels they are being treated unfairly, they become defensive. Actions that would have been unthinkable before become acceptable because an "I deserve it" mindset emerges. Leaders must identify and rectify inconsistent applications of rules and policies. No one expects completely equal treatment. But people have a sophisticated ability to discern unfairness. And they will react—often emotionally—when those unwritten yet definitive lines are crossed.

- **Be open.** Most employees start out committed to their work and to their employers. They want to feel valued and important. Most are therefore sensitive to being left "out of the loop"—especially in terms of important information. Such "lack of engagement" can trigger the same kind of rationalization described above. The thinking is along the lines of "I don't matter so why should I care?". Committing fraud is often the "justified" next step. Managers must be taught to see open communication as critical to keeping employees engaged and committed.

White-Collar Crime Fighter source:

David Gebler, president of Skout Group LLC, ethics, governance and risk consultants, www.skoutgroup.com. David can be reached at dgebler@skoutgroup.com.

Continued from page 3

others, and retaliated against this perceived unfairness by attacking their employer's IT systems.

Other insiders were able to steal or modify information due to inconsistent or unenforced policies.

Practice 3: Institute security awareness training for all employees. A culture of security awareness must be instilled in the organization so that all employees understand the need for policies, procedures and controls. Employees must also be aware of potentially serious consequences of breaking the rules.

Practice 4: Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process. Research suspicious or disruptive behavior by employees before they are hired, and continue background checking after recruitment. Screen for repeated policy violations that may indicate or escalate into more serious criminal activity.

Practice 5: Anticipate and manage negative workplace issues. Clearly formulate employment agreements and conditions of employment. Responsibilities and constraints and consequences for violations must be clearly communicated and consistently enforced.

Practice 6: Secure the physical environment. Most employees and contractors do not need access to all areas of the workplace.

Essential: Log and audit all access attempts to identify violations or attempted violations of your physical space and equipment access policies. Also ensure that terminated employees and contractors do not have physical access to non-public areas.

Practice 7: Implement strict password and account management policies and practices. Password and account management policies and practices must apply to employees, contractors and business partners. They must ensure that all account activity is attributable to the person authorized to perform it.

Audit regularly to identify and disable unnecessary or expired accounts.

Practice 8: Enforce segregation of duties. If responsibilities for critical functions are divided among employees, the opportunities for one employee to commit fraud or sabotage without the cooperation of another is limited. Effective segregation of duties requires implementation of "least privilege"—authorizing insiders only for the

resources they need to do their jobs.

Practice 9: Use extra caution with system administrators and technical or privileged users. System administrators and privileged users such as database administrators have the ability and access to commit and conceal malicious activity including fraud.

Self-defense: Techniques such as segregation of duties or “two-man rule” for critical system administrator functions, non-repudiation of technical actions, encryption and disabling accounts upon termination.

Practice 10: Implement system change controls. A wide variety of insider crimes such as deploying keystroke loggers, logic bombs or other malicious programs result from unauthorized modifications to the organization’s systems.

Self-defense: Technical controls designed for early detection. Once baseline software and hardware configurations are characterized, comparison of current configuration can detect discrepancies.

Practice 11: Log, monitor and audit employee Internet activity. If account and password policies and procedures are enforced, the organization can associate online actions with the employee who performed them. Logging, periodic monitoring and auditing facilitate early discovery of suspicious insider actions.

Practice 12: Deactivate computer access following termination. This is an obvious defensive measure but one that is still too often overlooked.

Practice 13: Implement secure backup and recovery processes.

Practice 14: Prepare an insider incident response plan. This is critical because no matter how effective the organization’s preventive measures, insider cyber-fraud will occur.

Challenge: The same people assigned to a response team may be among the most likely to think about using their technical skills against the organization. Only those responsible for carrying out the plan need to understand and be trained on its execution. ☹

White-Collar Crime Fighter sources:

•“Understanding the Insider Threat,” podcast produced by SearchSecurity.com by Dawn Cappelli, Technical Manager, Threat and Incident Management, CERT Program, Software Engineering Institute, Carnegie Mellon University, August 4, 2010.

•“Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition—Version 3.1,” coauthored by Dawn Cappelli, Andrew Moore, Randall Trzeciak and Timothy J. Shimeall of CERT Program, Software Engineering Institute, Carnegie Mellon University.

ETHICS OR FRAUD?

Peter Goldmann, CFE, *White-Collar Crime Fighter*

The Confusing Line Between Ethics and Fraud



I recently received a copy of the *Compliance and Ethics Manual* published by the Society of Corporate Compliance and Ethics (www.scce.org). It is a very clearly written and well-structured volume of some 880 pages.

But it raises a question that’s been nagging me for years: What is Ethics/Compliance and What is Fraud? Or—to take it a step further, what is Compliance and what defines a Code of Conduct?

Frustratingly, these terms tend to be used interchangeably, thus perpetuating widespread confusion as to which guidelines for behavior an organization should publish and enforce in its Code of Whatever You Wish to Call It.

WORDING IS KEY

The *Compliance and Ethics Manual* emphasizes that despite the widely assumed synonymous meanings of “ethics” and “compliance,” there are important differences.

According to the *Manual*, “Ethics at the core is a philosophy of values, integrity and courage. What an individual chooses to do, defines his or her ethics.” “Compliance,” by comparison, is “...the requirement and act of conforming to a guideline or policy, regulation or law. It is a directive to follow and conform to a set of clearly defined rules.”

As to an organization’s code of conduct, the *Manual* suggests that “An effective compliance and ethics program provides ongoing training of employees and contractors, monitors their understanding of and compliance with the external rules and regulations, and provides the mechanisms to discipline those individuals who violate the company’s code of conduct.”

Problem #1: In companies required by Sarbanes-Oxley to implement codes and policies incorporating these definitions, the critical issue of fraud—more specifically, rules against committing it—become back-burnered. Specifically, if you review the codes of conduct for a random sample of *Fortune 500* companies, chances are that the word “fraud” appears at most once or twice and in many instances not at all.

Problem #2: In the *SCCE Manual* and other authoritative ethics documents, there are references to the importance of ethics and compliance policies in reducing fraud and abuse. But neither fraud in general nor any of its numerous specific varieties (embezzlement, kick-backs, financial statement schemes, etc.) is ever clearly defined.

IS IT RIGHT...OR WRONG—PERIOD

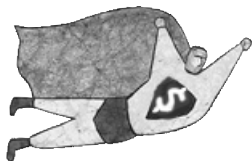
Key: Whenever someone commits a fraudulent act, they are acting unethically. But not all unethical acts are fraudulent...at least as far as the leading thinkers in the area of “Ethics and Compliance” are concerned.

Example: As the *Manual* clearly points out, conflicts of interest are not always fraudulent or even illegal. According to the *Manual*, “...unlike many areas of compliance law, the existence of a conflict of interest is not always wrong or evil. Indeed, it is certainly true that having personal interests and duties to others are simply aspects of the human condition.

According to the *Manual*, it is not the existence of a conflict that is necessarily problematic, but instead how management responds to it. According to

Continued on page 6

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE



Boards and Fraud: Where the Focus Should Be

At the 2010 Annual Conference of the Association of Certified Fraud Examiners, Deloitte Financial Advisory Services' Forensic Center director, Toby Bishop, participated in a lively panel session on the role of boards, auditors and management in deterring and detecting financial statement fraud. *His comments included some very practical advice for board members...*

- Study the ratings from employee survey questions about how well management walks the talk on the organization's ethics and code of conduct.

Important: By taking the pulse of employees throughout the organization, boards may identify an overall fraud issue or find individual business units in which the opinion of management's commitment to ethics and integrity is weak.

- Evaluate the number and types of violations of ethics and compliance policies over a year. This can provide insights about management's effectiveness in creating a workplace of integrity. Comparing the results against those of preceding years can show if ethics and compliance are improving or deteriorating. It may turn out that despite having the best code of conduct in the world, management may need to do more in terms of communication and enforcement.

- Assess the degree to which employees use anonymity in making ethics or fraud hotline calls. A pattern of low and diminishing anonymity can be an indicator of good and improving Tone at the Top where employee confidence in non-retaliation policies and management's commitment to act on employee tips is strong. The opposite may apply to high and growing insistence on anonymity.

White-Collar Crime Fighter source: Toby J.F. Bishop, CFE, CPA, FCA, speaking during panel session, "The Role of Auditors, Corporate Management, Boards and Audit Committees in Deterring and Detecting Financial Statement Fraud" at the 2010 ACFE Annual Conference, July 2010.

Are Your Company's Internal Control Weaknesses Being Properly Reported?

Sarbanes-Oxley Section 404 requires all large public companies to detect and report any weaknesses in their internal controls over financial reporting (ICFR).

Disturbing finding: According to recent research, only 28% of all ICFR weaknesses are actually disclosed when misstated financial reports are restated.

Key patterns to be aware of...

- Large public companies are less likely to disclose existing weaknesses than others, often because capital market pressures are greater for larger firms.

- Firms that recently changed audit firms are more likely to disclose existing weaknesses, which is consistent with new auditors being more likely to push for disclosure when the problems can be attributed to a predecessor.

Lesson for management and auditors: Despite the onerous costs associated with SOX 404 compliance, the resulting financial reports are successful in identifying accounting problems *less than half the time*, suggesting that substantial room for process improvement remains. Auditor change and other factors associated with the disclosure of existing weaknesses should be an important input in future deliberations to that end. Moreover, auditors should be aware that capital market-based pressures appear to represent a significant risk factor to be considered in their audits of internal controls and operations.

White-Collar Crime Fighter source: "How Reliable is Internal Control Reporting Under SOX 404? Determinants of the (Non-) Disclosure of Existing Material Weaknesses," by Sarah Rice, PhD, assistant professor of accounting, University of Connecticut, David P. Weber, PhD, assistant professor of accounting, University of Connecticut, dweber@business.uconn.edu.

Continued from page 5

the *Manual*, "This is one reason that compliance regimens are so essential in effectively dealing with conflicts. They create the infrastructure and systems that allow individuals to act ethically and appropriately in the face of conflicting interests, which are often inevitable."

Lesson: Conflicts of interest (and other potentially improper acts) can be unethical but aren't necessarily fraudulent. As the *Manual* continues, "While having a conflict need not necessarily be inappropriate or wrong, conflicts nonetheless have the potential for creating enormous harm to organizations and to society at large."

Contrast: There is no such thing as an ethical fraud. Period. Which may explain, at least in part, why so many companies choose to evade the fraud issue in writing their codes of ethics or conduct.

Conflicts of interest can be unethical but aren't necessarily fraudulent

Result: More and more anti-fraud experts are recommending that management supplement the organization's code of ethics or code of conduct with an Anti-Fraud Policy.

Example: When I recently spoke with the chief auditor of a small West Coast bank, she told me that while they had an ethics policy in place and all employees were required to read it, the bank still badly needed a formal anti-fraud policy. The auditor explained that the bank's ethics policy simply didn't incorporate definitions of such threats as loan fraud, mortgage fraud, check fraud and other costly financial crimes that most banks are constantly being hammered with.

Lesson: That this particular executive focused on the need for an anti-fraud policy may indicate that companies are finally beginning to realize that the ethics and compliance policies put into place after the 2002 enactment of SOX aren't doing the job when it comes to protecting the organization against fraud.

MANAGEMENT SETS THE TONE

Helpful insight: Microsoft Corp.'s director of financial integrity Martin Biegelman says, "A code of conduct must include written standards that

Continued on page 7

Continued from page 6

are reasonably designed to deter wrongdoing. It must promote honest and ethical conduct by all employees no matter their positions within the company. It should advise employees what they can and cannot do and reinforce compliance with government laws, rules and regulations. Consider writing specific codes for finance and procurement employees, and vendors.


Key: Each organization should formulate a specific anti-fraud code addressing specific fraud types that may be encountered in specific functional areas of the organization.

Helpful: Start by reviewing the Association of Certified Fraud Examiners' sample "Code of Conduct and Business Ethics." In contrast to the *Manual* and to most actual corporate codes of business conduct the ACFE document does not use the words "ethics" or "compliance" even once.

Instead, it lays out specifics of what constitutes *fraud*—and what doesn't.

Example: The document's section on conflicts of interest meticulously describes different kinds of conflicts and how they should be managed so as not to run afoul of the definition of fraud.

Additionally, the ACFE's Code specifies that employees who handle the organization's money are strictly prohibited from "obtaining or creating 'false' invoices or other misleading documentation or the invention or use of fictitious sales, purchases, services, loans, entities or other financial arrangements."

This type of unambiguous, unalterable description of specific fraudulent acts is what should constitute any organization's Anti-Fraud Policy. Leave the "soft stuff" about ethics to your mandatory "Code of Ethics and Compliance." To really lay the groundwork for preventing fraud, formulate and continuously communicate the definitions of fraudulent conduct, the strict prohibition against it and the consequences for violating the prohibition in a clear and succinct Anti-Fraud Policy. 

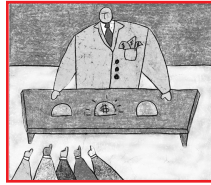
White-Collar Crime Fighter sources:

•Peter Goldmann, MSc, CFE, Editor, *White-Collar Crime Fighter*, www.wccfighter.com.

•*Compliance and Ethics Manual* published by the Society of Corporate Compliance and Ethics (www.scce.org).

•"Code of Conduct and Business Ethics," Association of Certified Fraud Examiners, www.acfe.com.

Note: A version of this article originally appeared in *The Fraud Examiner* newsletter, a publication of The Association of Certified Fraud Examiners, www.acfe.com.



THE CON'S LATEST PLOY...

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

Washington, DC

Deceptive subprime derivatives sales tactics finally coming under legal scrutiny. The Financial Industry Regulatory Authority (FINRA) fined Deutsche Bank Securities Inc. (DBS) \$7.5 million for misrepresenting delinquency data in connection with the issuance of subprime securities.

Details: FINRA found that DBS misrepresented and underreported the percentages of delinquent mortgages contained in the prospectus supplements of six subprime residential mortgage backed securities (MBS) issued in 2006. The firm also failed to correct errors by a third-party vendor and servicers, which underreported the historical delinquency rates of the mortgages in connection with its sale of 16 additional subprime MBS issued in 2007. DBS also failed to establish a system to supervise its reporting of required delinquency information.

Critical background: Delinquency rates constitute essential information for MBS investments because that data affects the investor's ability to evaluate the fair market value, the yields on the certificates and the anticipated holding periods of the securitizations. Institutional investors often consider this information in assessing the profitability of these securitizations and in determining whether future returns would be disrupted by mortgage holders who fail to make loan payments.

Case details: During 2006 and 2007, DBS underwrote subprime MBS and sold them to institutional investors. FINRA found that in the prospectus supplements of six subprime securitizations worth approximately \$2.2 billion offered in March 2006, the firm described a method of calculating delinquencies that was different from the method it actually used.

The result: Delinquencies were

underreported.

Example: In one MBS deal, DBS reported that under its described method of calculation, 8.75% of the loans were between 30 to 59 days delinquent, corresponding to \$14 million in delinquent loans. But the *actual* delinquency numbers computed under the method (DBS) disclosed were much higher—with 24.02% of the loans between 30 to 59 days delinquent, corresponding to \$38.5 million in delinquent loans.

Additional violation: FINRA also found that DBS underreported historical delinquency rates on a Web site the firm maintained that was referenced in prospectus materials in connection with the sale of 16 MBS.

Background: Issuers of subprime MBS are required to disclose historical performance information for prior securitizations that contain similar mortgage loans as collateral. That information, which includes historical delinquency rates, is called "static pool" information. It is one of the key disclosure requirements for asset-backed securities under a federal regulation that became effective in December 2005. After the rule came into effect, DBS prospectus supplements for new subprime MBS offerings informed investors they could view static pool information on the firm's special Web site.

Honest errors become deception issues: In January 2007, DBS learned that the outside vendor it retained to post content to the Web site was underreporting delinquencies as a result of errors made by the servicers responsible for tracking delinquencies. DBS determined that these errors affected 16 securitizations and provided corrected delinquency data for 13 of them to the vendor to use going forward. But the vendor failed to use the corrected data. Moreover, DBS never ensured that the vendor posted the corrected static pool information and continued to refer investors to the inaccuracies about these 13 securiti-

zations on the Web site.

Though DBS was unable to determine the extent to which delinquency rates were underreported in the remaining three affected securitizations, the firm continued to use this data without indicating on the Web site that the information was inaccurate.

In settling the matter, Deutsche Bank Securities neither admitted nor denied the charges, but consented to the entry of FINRA's findings.

Alexandria, VA

Mortgage lending executive indicted for role in \$1.9 billion fraud that contributed to major bank failure. Lee Bentley Farkas, former chairman of private mortgage lending company, Taylor, Bean & Whitaker (TBW), was arrested in Ocala, FL, and charged in a 16-count indictment for his alleged role in a more than \$1.9 billion fraud scheme that contributed to the failures of Colonial Bank, one of the 50 largest banks in the United States in 2009, and TBW, one of the largest privately held mortgage lending companies in the United States in 2009.

Background: TBW's principal source of income was servicing mortgage loans it sold to Freddie Mac and that it sold as part of securities guaranteed by Ginnie Mae. TBW's loan servicing responsibilities required it to, among other things, collect principal

and interest payments on mortgage loans from borrowers and disburse those "pass-through" payments to the third-party loan buyers.

Colonial Bank's Mortgage Warehouse Lending Division (MWLD), based in Orlando, FL, provided short-term, secured funding to mortgage lending companies. MWLD's largest customer was TBW.

MWLD accounted for at least 20% of Colonial Bank's pre-tax income from 2005 through 2009, and in 2008 and 2009 was one of Colonial Bank's few banking segments that reported a profit.

According to the indictment, Farkas and his co-conspirators at TBW and Colonial Bank stole more than \$400 million from Colonial Bank's MWLD and approximately \$1.5 billion from Ocala Funding, a mortgage lending firm controlled by TBW. Farkas and his co-conspirators allegedly stole this money in order to cover TBW's operating losses.

The indictment further alleges that Farkas and his co-conspirators committed wire and securities fraud in connection with their attempt to convince the United States government to provide Colonial Bank with approximately \$553 million in TARP funds.

Origins and evolution of the fraud:


Court documents allege that the scheme began in 2002, when Farkas and his co-conspirators ran overdrafts in TBW bank accounts at Colonial Bank in order to cover TBW's cash shortfalls. Farkas and his co-conspirators at TBW and Colonial Bank allegedly transferred

money between accounts at Colonial Bank to hide the overdrafts. After the overdrafts grew to tens of millions of dollars, Farkas and his co-conspirators allegedly covered up the overdrafts and operating losses by having Colonial Bank purchase from TBW more than \$400 million in what amounted to fake mortgage loan assets, including loans that TBW had already sold to other investors and fake interests in pools of loans. Farkas and his co-conspirators allegedly caused Colonial Bank to hold these bogus assets on its books at their face value when in fact the mortgage loan assets were worthless.

Ocala funding fraud: Ocala Funding sold asset-backed commercial paper to financial institution investors, including Deutsche Bank and BNP Paribas Bank. Ocala Funding, in turn, was required to maintain collateral in the form of cash and/or mortgage loans at least equal to the value of outstanding commercial paper.

The court documents allege that Farkas and his co-conspirators diverted cash from Ocala Funding to TBW to cover its operating losses, and as a result, created major deficits in the amount of collateral Ocala Funding possessed to back the outstanding commercial paper. To cover up the diversions, the conspirators allegedly sent false information to Deutsche Bank, BNP Paribas Bank and other financial institution investors to deceive them into believing that they had sufficient collateral backing the commercial paper they had purchased.

Result: Deutsche Bank and BNP Paribas Bank held approximately \$1.68 billion in Ocala Funding commercial paper that had only approximately \$150 million in cash and mortgage loans collateralizing it. When TBW failed in August 2009, the banks were unable to redeem their commercial paper for full value.

In August 2009, the Alabama State Banking Department, Colonial Bank's state regulator, seized the bank and appointed the FDIC as receiver. Colonial BancGroup also filed for bankruptcy in August 2009. 



YES! I want to save \$100 on a one-year subscription to **WHITE-COLLAR CRIME FIGHTER!** By subscribing now, I'll get the money-saving introductory subscription rate of \$150. *That's \$100 off the regular subscription price of \$250!*
Plus, send me—for **FREE**—The new book, *Detecting and Preventing Fraud in Accounts Payable*. This is a \$50 value—yours absolutely **FREE** with your subscription to *White-Collar Crime Fighter!*

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...

- **Detecting and preventing management override of internal controls**
- **Lessons from growing retail industry fraud**
- **Information security strategies for non-technical decision-makers**
- **Practical anti-fraud lessons from the financial crisis**