

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

VOLUME 9 NO. 8
AUGUST 2007

YOUR SECRET WEAPON IN THE WAR ON FRAUD

IN THE NEWS

Sarbanes-Oxley from the Sarbanes/Oxley Viewpoint

To those who argue that the Sarbanes-Oxley Act has driven up the costs of raising capital in US financial markets, thereby threatening to undermine the global supremacy of those markets, the authors of the law point out that the main purpose of the Act was—and is—to restore confidence in those markets by eliminating opportunities for dishonest executives to compromise the standards of conduct that made those markets great in the first place.

It is such standards, suggest former Senator Paul Sarbanes and former Representative Michael Oxley that, when adhered to, ensure that companies committed to honest risk-taking are rewarded with long-term success.

Similarly, say the authors, “integrity and transparency of our capital markets is an exceedingly significant economic asset for companies going public. We must continue to restore the high business standards of the past because in the end, it is those standards that will guarantee the long-term competitiveness of US capital markets.”

White-Collar Crime Fighter source:

Senator Paul Sarbanes and Representative Michael Oxley, speaking at the 18th Annual Association of Certified Fraud Examiners Fraud Conference, July 17, 2007.

IN THIS ISSUE

•INTERVIEWING INSIGHTS

Catching fraud suspects in a lie is not always a sign of guilt... 3

•KNOW YOUR NUMBERS

*Tell-tale signs of potential earnings manipulation.....*4

•CYBER-CRIME FIGHTER

*Lessons from the TJX crisis ...*5

•THE CON'S LATEST PLOY

Law-enforcement successes from around the country..... 7

Joseph B. Nelson, CPA, CFE, FCPA
Marks, Paneth & Shron, LLP

Preparing for a Fraud Investigation

A View from The Trenches



Case study: New York Corp (NYC), a Manhattan-based maker of household products, such as tableware, cookware and flatware, manufactured all of its goods in a New Jersey plant for over 100 years. A year ago management decided that, to remain competitive, the company would move its manufacturing operations to Tijuana, Mexico.

The new Tijuana plant is a wholly-owned subsidiary of NYC. *Key characteristics:*

- A small back-office staff handles all local accounting. The plant's financial results are consolidated using a monthly spreadsheet-based reporting application.

- NYC is listed on the NYSE. It reported revenues of \$110 million in its last fiscal year, and net income of \$8 million. It has been in full compliance with Sarbanes-Oxley since the initial deadline and has received unqualified audit opinions from its external auditors every year since.

- The new Tijuana facility also functions as a distribution center for the West Coast of the United States, and has been expanding into Latin America through a growing network of distributors. The new facility's sales growth has been solid in its first year and the financial markets have regarded this favorably.

Key event:

Two weeks before the latest external audit was to be completed, NYC's general counsel received an anonymous complaint on the company's whistleblower hotline. The caller stated that in recent weeks a “large distributor” in Mexico City returned a large quantity of goods to the Tijuana subsidiary because they “didn't sell.” The distributor was permit-

ted to do this under an agreement made with NYC's country manager in Tijuana.

Problem: The returns strained the capacity of the company's Tijuana warehouse, so local management found another distributor who was willing to “hold” the merchandise for a “fee” of \$25,000.

The whistleblower stated that, when asking about the \$25,000 fee, she was told by local management that it was a “good deal,” because the waiver on the environmental permit for the new factory had cost twice as much.

The GC has informed the Board of these events and has directed the Board to retain independent counsel to investigate.

POTENTIAL FRAUD FACTORS

The events reported by the whistleblower imply potential legal trouble in a number of ways...

- Potential violation of the Foreign Corrupt Practices Act (FCPA) by payment of the \$25,000 “fee”.

- Possible illegal channel stuffing by paying a distributor to “hold” goods that wouldn't sell.

- Possible accounting fraud in the Mexican back-office due to lax internal controls.

- Potential collusion between NYC's Mexican executives and local authorities.

TAKING THE RIGHT STEPS

NYC's management had numerous options for handling these events after learning of them from the whistleblower.

Challenge: Accurately identifying the details of illegal or potentially illegal conduct in the Mexican operation—without increasing the risk of adverse

regulatory or legal repercussions.

What management should have done...

Step one: Verify the authenticity of the whistleblower's complaint. Most employees who use confidential hotlines do so for legitimate reasons, but there is always a certain amount of "junk" reporting—personal grievances or attempts at revenge against a co-worker or boss, etc.

To ascertain the validity of the fraud tip, start by documenting all immediately available evidence about the alleged fraud—such as product shipments, invoicing paper trails, etc. Next, have a senior internal auditor, member of the General

Computer Crime: The Looming Crisis

Antiforensics—an especially dangerous form of high-tech criminal attack—while not new, should nonetheless be making computer crime investigators and the organizations they work for tremble with anxiety.

Reason: Antiforensics has been best defined as a way for cyber-criminals to hack, sabotage, steal from and otherwise dangerously compromise an organization's computer system—without getting caught. It is a form of attack that not only makes it difficult to locate the perpetrators, but also impossible to prove that they have been discovered.

The threat: According to some of the best brains in the field of high-tech crime, the threat is rapidly reaching crisis proportions. That's because the technology used in antiforensics to commit high-tech crimes against corporations, government agencies and other institutions is no longer the domain of the technology elite. It has gradually become easier to obtain and easier to use, thereby causing a significant increase in the deployment of antiforensic tools in the past year.

According to some analysts, while some of the antiforensic tools are still not being used by criminals, it's only a matter of time before they are.

Countermeasures: High-tech investigators must rethink their approach to system security and forensic investigation. Some of the techniques for catching antiforensic attackers may be surprisingly low-tech in nature.

White-Collar Crime Fighter source:

- Scott Berinato, Senior Editor, CSOnline.com, sberinato@cxo.com.
- Bruce Schneier, founder and CTO of BT Counterpane, a leading protector of networked information and one of the foremost authorities on effective mitigation of emerging high-tech threats. He can be reached at schneier@schneier.com.

Counsel's office and other experienced investigative interviewer(s) question the whistleblower as well as other employees who might have knowledge about the alleged fraud.

If necessary, conduct surveillance or other forms of monitoring of the whistleblower's activities.

Aim: To determine the sincerity and integrity of the whistleblower...and to learn as much about the alleged fraud as possible at the earliest possible time.

Step two: Formulate a hypothesis about the fraud. With the evidence gathered so far, outline a general picture of the type(s) of fraud that could have occurred in the Mexican unit.

Important: With your initial gathering of evidence, consider frauds that may have occurred, but which the whistleblower didn't detect. List all potential frauds, based on the limited evidence you've collected so far.

Example: In the NYC Mexico case, your hypothesis might point to the payment of an illegal bribe to a local business to facilitate a channel-stuffing operation to enable management to "adjust" the accounting records to impress headquarters management with the Mexican subsidiary's financial performance.

Step three: Analyze the local business environment to determine the specific types of fraud that could have occurred.

Examples:

- Bribery in violation of the FCPA.
- Collusion with local distributors.
- "Bill and hold" or "channel stuffing" schemes involving the "second distributor."
- Accounting fraud to conceal the illegal payment.
- Fraudulent financial reporting to make the Mexican operation's performance appear healthier than it was.

Effective: Apply the elements of the Fraud Triangle (Opportunity, Pressure and Rationalization) to help in assessing the environment that could have given rise to the suspected fraud(s).

Example 1: With NYC in Mexico, the element of Opportunity proved to be key. Because the financial activities of the Mexican subsidiary were overseen by a small back-office accounting staff, internal controls were almost certainly lax, thereby creating ample opportunity to falsify financial reporting.

In addition, Latin American business "culture" is known to be conducive to loose financial oversight and in the NYC case, could have given rise to the \$25,000 bribe.

The same cultural characteristics may

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

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: \$295/yr. Canada, \$345.

Copyright © 2007 by White Collar Crime

101, LLC. No part may be reproduced with-

out 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.

have helped local NYC management decide to sidestep the laws against collusion in order to execute the channel stuffing scheme.

Example 2: The Fraud Triangle's component of Pressure may have led the Mexican management team to feel the need to impress the bosses in New York.

In addition, the financial markets' favorable reaction to the Mexican subsidiary's early "success" may have added pressure on the local Mexican executives to continue generating impressive financial results.

Example 3: Rationalization may have come into play when the local Mexican management team convinced themselves that the \$25,000 "fee" was not for their benefit, but was instead for the "greater good" of NYC's globalization strategy.

If necessary, conduct surveillance or other forms of monitoring of the whistleblower's activities

Step four: Prepare and conduct a thorough fraud investigation. With the hypothetical fraud scenario in mind, supported by your assessment of the local business environment and the Fraud Triangle-based analysis of what could have occurred, structure your investigation to gather evidence of all suspected illegal activities.

Essential: Investigate every potential illegal activity in your pre-investigation assessment. This is important because with a probe such as this in a business environment that your legal and audit teams are unfamiliar with, the Mexican facility may

be guilty of frauds that even your initial hypothesis and environmental analysis didn't initially anticipate.

The last thing you want is to spend substantial resources on an investigation that, once concluded, proves to have been inadequate by revelations of additional unexpected fraud.

White-Collar Crime Fighter source:

Joseph B. Nelson, CPA, CFE, FCPA, Director, Litigation Services Group, Marks, Paneth & Shron LLP, Certified Public Accountants and Consultants, New York, www.markspaneth.com. Joe has earned a reputation as an "internal control and anti-fraud troubleshooter" with special expertise in investigating and preventing corporate fraud. His areas of specialty include complex financial reporting and compliance, fraud investigation and forensic accounting, commercial damages, lost profits and intellectual property damages. He can be reached at jnelson@markspaneth.com.

WHY SETTLE FOR JUST A PIECE OF THE PIE WHEN YOU CAN HAVE IT ALL?

FraudAware Picks up Where Ethics Training Leaves Off

The Government Says Compliance and Ethics Training Should be Designed to "Prevent and Detect Criminal Conduct" DOES YOURS DO THAT?

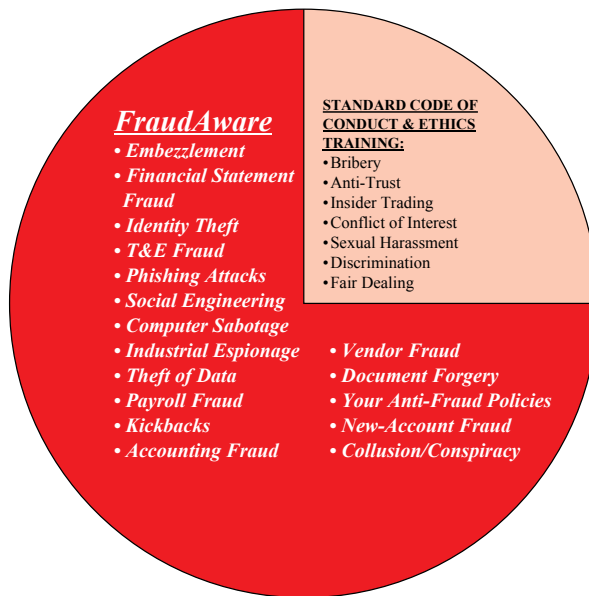
Sarbanes-Oxley and the Federal Sentencing Guidelines and other laws and regulations have pushed companies to adopt costly "Compliance & Ethics" training programs.

Question: Why were SOX and FSG put into effect in the first place?

Answer: To stop corporate FRAUD. So—Why do compliance & ethics programs teach employees virtually NOTHING about Fraud?

We don't know the answer. But we DO know that to prevent and detect fraud against your company, your employees must be trained to recognize the telltale signs of countless types of Fraud and how to report it.

The ONLY training program that does that is *FraudAware*...



FraudAware

1-800-440-2261

Email: info@fraudaware.com