WHITE-COLLAR CRIME FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

LUME 6 NO. 11
NOVEMBER 2004

IN THE NEWS

Latest Assaults on Phishing

The Financial Services Technology Consortium (FSTC) has attracted 11 major banks and 17 top technology vendors to form a new financial industry-wide anti-phishing initiative.

Mission: In collaboration with other industry groups, such as the Anti-Phishing Working Group, FSTC will define the technical and operating requirements of financial institutions for implementing strong anti-phishing measures.

FSTC is an industry research organization whose members include banks, financial service firms, national laboratories, universities and government agencies.

Separately, the Banking Information Technology Secretariat (BITS) formed the Phishing Prevention and Investigation Network (PPIN). *Objectives:*

- Help member financial institutions monitor and shut down phishing attacks faster and more effectively.
- Reduce financial institution manpower costs and losses related to fighting phishing.
- Step up phishing investigations and arrests of perpetrators.
- Improve anti-phishing communication among fraud specialists at financial institutions, service providers and law enforcement agencies.

***White-Collar Crime Fighter* sources:**

- Gene Neyer, Financial Services Technology Consortium, www.fs tc.org.
- Wilton Dolloff, Executive Vice President, Huntington Bancshares Incorporated and Member of the Executive Committee, BITS, www. bits.org.

IN THIS ISSUE

Gary D. Zeune, CPA, *The Pros and the Cons*

Does Your Compensation System Encourage ILLEGAL ACTIVITY?

Compensation systems are supposed to motivate people to work hard…but defective systems can inadvertently foster illegal or dangerous behavior that puts the company at risk of litigation and/or serious fraud losses.

Example: In the long-haul trucking industry many truckers drive far beyond the legal limits for speed and hours on the road. That's because they are typically paid by the mile, without additional pay for hours spent waiting for shippers and receivers to load and unload their trucks.

It is estimated that 80% or more of drivers comply with the federal regulations. But, it's also an open secret in the trucking industry that many drivers maximize their incomes by consistently ignoring speed limits and driving more hours than permitted by law.

The risk: If such illegal activity results in an accident, the driver, the trucking company and, in some circumstances even the receiver, could face multi-million dollar liability lawsuits….*and lose,* if a jury is sympathetic to the plaintiffs.

A SYSTEM THAT DIDN'T WORK

In another example, about 10 years ago Domino's Pizza, Inc. used the marketing ploy of a 30-minute delivery guarantee. To encourage drivers to get to customers on time, some stores reportedly paid drivers a bonus of 1% for making a minimum number of on-time deliveries.

Unfortunately, the compensation system backfired. In one case, the company reached a $2.8 million settlement with the family of an Indiana woman killed by a delivery vehicle allegedly speeding to meet the 30-minute guarantee.

DEFECTIVE COMPENSATION SYSTEMS ARE COMMON

At the white-collar level, there are many compensation arrangements that, while aiming to boost productivity, inadvertently create strong temptation for employees to break the law.

It is widely recognized that the illegal and unethical financial reporting activities at WorldCom, Xerox and others was fueled, at least in part, by outlandish bonus plans and stock options.

Problem: Many companies have what I call "goal-discongruent" systems. This unpleasant-sounding term describes situations where, when a decision is made in a particular way, it benefits top executives or the company but harms the rank-and-file employees.

That's what happens when bonus and stock option compensation plans go too far.

Example: Fannie Mae, where executives allegedly manipulated the system to "smooth" income in order to receive huge bonuses.

Meanwhile, the company's actual financial condition may be shaky, often leading to mass layoffs. Or, as in the case of WorldCom, things can get so bad that the only choice is to file for bankruptcy protection.

MORE LEGAL TRAPS…

These are the kinds of situations that make it absolutely critical that corporate boards establish systems of checks and balances to prevent discongruent com-

pensation structures from harming the company's financial wellbeing.

Fortunately, the Sarbanes-Oxley Act of 2002 is creating a legal environment that requires companies to come up with accounting procedures that impose tough sanctions for failing to maintain "clean" financial reporting.

Challenge: Defective compensation systems are not illegal in and of themselves. But, as Domino's, WorldCom and others learned the hard way, the company can face devastating legal consequences for illegal conduct that the compensation system fosters.

Also risky: Employers can face liability for actions by an employee or an independent contractor, because either way, that person is acting as an agent of the company. If a plaintiff can identify a pattern of illegal behavior, a compensation system that clearly encourages that behavior might raise the stakes from negligence to deliberate disregard and therefore trigger punitive damages.

Example: If a company is put on notice by regulators that a policy is being interpreted by employees in ways that could result in fraudulent activity, and the company fails to change the policy, punitive damages could result…in addition to any criminal punishment.

Critical lesson: You can't blame employees for not following the rules when you knew…or should have known…that your compensation system directly causes illegal behavior.

COMPENSATION FLAWS ON THE FRONT LINE

Fortunately, not all ill-conceived compensation systems result in the kinds of mega-frauds like WorldCom, Xerox and Tyco. However, too many companies have compensation policies that they think are good for the company, but that backfire by fostering fraudulent behavior on the part of employees.

Scenario: You assign one of your employees to work on a project out of town for several weeks. One evening, she's flipping through the TV channels, and watches a pay-per-view movie. Your accounts payable clerk crosses the $5 movie off the hotel bill that she submits later for reimbursement.

Resenting being "nickled and dimed," the employee records a fake $15 or $20 charge on the following week's T&E expense report.

What did you do in that two-week period? You "taught" the employee that in order to be fairly compensated; she has to cheat—to embezzle. The second week's expense report complied with the company policy—there were no pay-per-view movies on the hotel bill—but the policy "drove" the employee to commit fraud against the company.

Worse: Not only does the employee resent the way she was treated, her productivity drops while she's plotting how to get repaid.

Result: Your total loss in embezzled funds and lost productivity is much greater than $5 the employee originally (and honestly) sought reimbursement for.

***White-Collar Crime Fighter* source:**

Gary D. Zeune, CPA, founder of The Pros & The Cons, a speaker's bureau for former white-collar criminals, www.theprosandthecons.com. Gary has more than 30 years of experience in auditing, corporate finance and investment banking and teaches a variety of courses in fraud and performance measurement. He can be reached at gzfraud@bigfoot.com.

Case History: How a Single Case of Insider Computer Crime Can Bring Down a Company

A manufacturing company had a secret formula for a new adhesive product stolen by an employee. The employee sold the formula to an Asian competitor. *The results…*

- An estimated $600 million in sales was immediately lost by the US company.
- 2,600 jobs were immediately lost.
- 9,542 jobs were lost over the following 14 years.
- The Asian competitor secured the entire world market for the new adhesive product.
- $129 million in tax revenue was lost.
- The US company ultimately went out of business.

All from the theft of a single trade secret by a single employee.

Lesson for all: If you think your intellectual property is secure, look again. Fortunately, there are defensive measures that can be taken to minimize the risk of devastating insider crimes—starting with a "no exceptions" in-depth background checking policy covering all existing and prospective employees. But if your company's success hinges on the security of proprietary information, the first step is to stop underestimating the chances that someone will steal that information and turn it against your organization.

***White-Collar Crime Fighter* source:**

Yalkin Demirkaya, Director of IT Security Services, CSS-Group, a New Canaan, CT-based private investigation and security firm, www.css-group.com. Yalkin is also an experienced police investigator, serving as Commanding Officer of the Computer Crimes Investigation Unit of a major metropolitan law enforcement agency.

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

White-Collar Crime Fighter (ISSN 1523-0821) is published monthly by White-Collar Crime 101, LLC, 213 Ramapoo Rd., Ridgefield, CT 06877. www.wccfighter.com. Subscription cost: $275/yr. Canada, $299.

Mission Statement

White-Collar Crime Fighter provides information of maximum practical value to organizations and individuals involved in all facets of investigating, detecting and prosecuting economic crime.

This community includes law enforcement officers…regulatory officials…corporate security professionals…business owners and managers…private investigators…and many more.

The editors of *White-Collar Crime Fighter* strive to gather and compile the most useful and timely information on economic crime issues.

Comments, suggestions and questions are welcome. Please fax us at 203-431-6054, or E-mail us at editor@wccfighter.com. Visit us on the Internet at www.wccfighter.com.