

AUDITOR JAILED FOR SOX VIOLATION AFTER ALTERING AUDIT PAPERS

A former audit partner of Ernst & Young, a Big 4 accounting firm, was sentenced this past January to a year in jail and \$5,000 in fines after pleading guilty to violating rules under the Sarbanes-Oxley Act of 2002 against obstructing a federal investigation of a public company. Section 802 of SOX provides for jail terms and fines for altering or destroying records and for failing to retain accurate audit records.

The 42-year old former partner had been involved in the audit of San Francisco-based NextCard, a public company that issued credit cards through its wholly-owned banking subsidiary, NextBank. NextCard declared bankruptcy in 2002 after its Internet-only credit card strategy produced higher than average loan losses. Beginning in October 2001, after the partner heard that the Office of the Comptroller of the Currency (which regulated NextBank) might want to review Ernst & Young's audit

workpapers, he had his subordinates alter E&Y's workpapers on the NextCard/NextBank audit to show earlier dates. He also had electronic records - such as e-mails and other workpapers - destroyed if they had information conflicting with the changed dates.

These altered documents were provided to the OCC in March and April 2002. When questioned in April 2003 by the SEC about his role in producing those workpapers for the OCC, the partner concealed his actions. It was this obstruction of a federal investigation, occurring after



IN THIS ISSUE:

- Auditor Jailed for SOX Violation After Altering Audit Papers ..1
- Vast Majority of Identity Theft Begins at Work.....1
- Riggs Faces the Costs of Non-Compliance2
- Protection from "Naked" Short-Sellers2

the adoption of the Sarbanes-Oxley Act, that led to the partner's arrest by the FBI in September 2003. He eventually pled guilty in October 2004.

The prospect of jail time, SEC sanctions and bank regulatory lawsuits has caused accounting firms to increase their diligence. However, it has also led to their reduced interaction with clients so as to avoid the possibility of any involvement in a company's accounting misconduct. ▣

VAST MAJORITY OF IDENTITY THEFT BEGINS AT WORK

A recent report from Michigan State University found that 50% to 70% of identity theft begins with the theft of personal data from a company by an employee. In one instance, a temporary data-entry clerk stole the identities of 2,000 corporate executives. In another case, a help-desk technician who only briefly worked at a company was able to orchestrate identity theft that resulted in over \$50 million in losses.

Two pending bills in Congress

would require companies to be proactive against identity theft. Under S 1350, a company that owns or licenses electronic data containing personal information must notify those persons residing in the U.S. whose personal data may have been compromised because of a security breach in its systems. HR 818 is similar to S 1350, but it focuses on financial institutions and is broader in its scope and obligations.

Companies can act to fight identity theft right now in their workplace:

- Do not use Social Security Numbers (SSN) as employee numbers and do not print SSNs on anything that can readily be seen by others, including timecards, etc.
- Store sensitive personal information in secure computer systems with restricted access, and implement electronic audit trail procedures to monitor any access or transmission of that

data.

- Place any confidential documents with sensitive personal information in locked storage.
- Dispose of any confidential information by cross-shredding it and depositing it in a locked dumpster.
- Conduct regular background checks on ALL employees with access to classified information, including mailroom staff, cleaning crews, temporary workers, and computer technicians.

Most at risk, according to the Michigan State report, are financial and health care companies. In fact, the OCC has warned that organized crime has begun planting new tellers at banks in order to obtain information that is later used to commit identity theft.

Identity theft beginning at a company can tarnish that company's reputation and lead to claims of negligence. ▣

"IT USED TO BE THAT SHRINKAGE WAS THE BIGGEST COST TO EMPLOYERS AFTER PAYROLL AND HEALTHCARE. TODAY WHAT WE HAVE TO THINK ABOUT IN THE INFORMATION AGE IS EMPLOYEES STEALING INFORMATION."

- JUDITH COLLINS, DIRECTOR OF MICHIGAN STATE UNIVERSITY IDENTITY THEFT PARTNERSHIPS IN PREVENTION AND RESEARCH LAB

RIGGS FACES THE COSTS OF NON-COMPLIANCE

A recent failed merger highlights the significant impact of a Bank Secrecy Act violation on a company.

On Feb. 7, 2005, a proposed merger between Riggs National Corporation (Riggs) and PNC Financial Services Group, Inc. (PNC) was called off, and Riggs sued PNC for damages relating to the now-defunct deal. Riggs' subsidiary, Riggs Bank, has a 168-year history in Washington D.C., serving as the bank of choice for US presidents and foreign embassies and for significant transactions such as the purchase of Alaska.

Initially, PNC agreed in July 2004 to pay \$779 million to acquire Riggs, or about \$24.25 per share. This followed payment by Riggs of a record \$25 million fine for its

involvement in a money-laundering scheme. A provision allowing PNC to back out of the deal if a "material adverse change" occurred to Riggs before finalization in April 2005 was included in the merger agreement.

Following the signing of the merger agreement in July 2004, Riggs was fined an additional \$16 million and pleaded guilty to a felony



charge of violating bank-secrecy laws. This was in addition to over \$13 million in legal fees in the third quarter of 2004.

In response, PNC argued that a material adverse change had occurred and lowered its offering price to \$19.32 per share, with possible downward adjustments, and made additional demands.

Riggs' board unanimously refused to accept the changes and sued PNC, citing damages arising from preparing for the merger and taking various actions at PNC's insistence.

Strong compliance programs, especially with heightened scrutiny under the Bank Secrecy Act, can help a company avoid significant fines and successfully execute profitable business strategies. ■

PROTECTION FROM "NAKED" SHORT-SELLERS

Steven Amen of our Omaha office writes:

To protect thinly-capitalized companies and their investors from possible price manipulation of their stock, the SEC recently adopted rules - Regulation SHO - designed to curtail increased instances of "naked" short-selling (i.e., selling short without borrowing the necessary securities to make delivery).

Regulation SHO prohibits broker-dealers from executing short sales unless they first have borrowed the securities or have reasonable grounds to believe they could borrow the security in time to deliver it when due. The regulation also prohibits investors and their broker-dealers from engaging in further short sales of a stock if they have previously failed to deliver on a short sale for that stock.

Brokers have had since last fall to prepare for this new requirement,

which applies to investors beginning on January 3, 2005.

"Naked short-selling" can have a downward pricing effect if the investor fails to deliver the shares when due. Also, it allows a short seller to exert significant downward price pressure on a stock without having any stock at risk. This then may cause other

SHORT-SELLING IS AN INVESTMENT STRATEGY IN WHICH AN INVESTOR BORROWS STOCK AND SELLS IT IN THE MARKET, HOPING TO REPURCHASE IT LATER AT A LOWER PRICE, THEREBY MAKING A PROFIT

investors to abandon their long-standing positions, driving the company's stock price to even lower levels. As its stock price plummets, the

company finds that it becomes impractical to raise additional capital or use its shares to complete acquisitions. Equity-based compensation arrangements also lose their value.

Companies anticipating or experiencing short-selling should determine whether the short-seller is complying with this new SEC regulation. ■

Kutak Rock LLP is a national law firm with 16 offices located throughout the United States. Our practice areas include:

- Corporate Governance
- Banking Law
- SEC Reporting and Compliance
- Mergers and Acquisitions
- Employment / Employee Benefits Law
- Stock Offerings

Please visit our website www.kutakrock.com to learn more, or contact:

Paul Borja.....202-828-2310
paul.borja@kutakrock.com

Jeremy Johnson....202-828-2463
jeremy.johnson@kutakrock.com

Editor:

Justa Schmidt202-828-2305
justa.schmidt@kutakrock.com