

## **Biometrics & Fraud Mitigation Following SOX**

**The old days of external auditors claiming that they are not responsible for detecting fraud and of managements depending upon management letters from external auditors for learning about weaknesses in their internal control systems have changed with the enactment of the Sarbanes-Oxley Act (SOX). Following SOX, external auditors, corporate attorneys, directors, and managements of large companies have legal obligations to mitigate fraud. Just as it is smart to use seat belts in automobiles regardless of local legal requirements, it is smart to use biometrics to improve internal controls and to mitigate fraud regardless of whether companies are large enough to be subject to SOX or to other mandatory laws, regulations, standards, or to codes. Laws represent minimum standards. Companies may still suffer large losses from frauds even if their internal control systems meet minimum standards.**

*By Paul Sheldon Foote and Reena Hora*

Biometrics  
& Fraud Mitigation  
Following

SOX



## Accounting Frauds and Scandals

In the United States, the numbers and sizes of major accounting frauds and scandals became so excessive that Congress passed and President George W. Bush signed the Sarbanes-Oxley Act (SOX) of 2002.

## Lawsuits and Criminal Cases

Investors and other third parties who have relied upon managements' representations and certified financial statements have sought to recover their losses in the courts. As experience with SOX and court cases develop, there will be a better understanding of who will be held responsible for accounting frauds, scandals, and internal control failures. Lawsuits against external auditors, corporate attorneys, directors, and managements will provide evidence of what needs to be done to correct these failures. There can be several legal cases related to the same loss because parties may file cross complaints against each other.

However, there are steps corporations should be taking now to mitigate future frauds.

## Lawsuits against External Auditors

Over time, court decisions have expanded the types of third party users of certified financial statements.

- In *Ultramares v. Touche & Co.* (1931), the court held that auditors may be held liable for ordinary negligence to a third party -- provided that the auditors were aware that their certified financial statements would be used for a particular purpose by known parties.
- More recent cases have moved from the known user approach to a foreseen user approach. For example, in *Williams Controls v. Parente, Randolph, Orlando & Associates*, 39 F. Supp. 2d 517 (1999), the court held that auditors could be

liable to a purchaser of a client's business even if the auditor did not know at the start of the audit who the purchaser would be.

- In New Jersey, in *Rosenblum v. Adler* (1983), the court extended the liability of auditors to any third parties the auditors could "reasonably foresee" as recipients of certified financial statements for routine business purposes. [Whittington, O. Ray, and Kurt Pany, *Principles of Auditing & Other Assurance Services*, Sixteenth Edition, McGraw-Hill Irwin, 2008]

Certified public accountants will not be able to continue to accept financial audit engagements unless corporate managements mitigate the possibilities of frauds.

### No Insurance Coverage

It is not realistic to expect that companies will be able to make no improvements in their internal control systems and to buy enough insurance to cover all possible losses in legal cases. For example, one international public accounting firm paid US\$6 million to defend successfully a lawsuit involving a client with US\$20,000 annual audit fees. At least one major insurance company has responded by refusing to insure accounting firms for legal liabilities. [Whittington, O. Ray, and Kurt Pany, *Principles of Auditing & Other Assurance Services*, Sixteenth Edition, McGraw-Hill Irwin, 2008]

Directors and officers have relied upon the availability of errors and omissions (professional liability) insurance.

# SOX

## Compliance Requirements for Management

1. Assess risk and design controls.
2. Segregate duties.
3. Place internal controls for processes and system access.
4. Monitor controls and follow up to check if controls are in place.
5. Document and test the controls.
6. Management has to provide a report on its internal controls.
7. An independent auditor has to evaluate management's assessment of its internal controls and provide a report.

### Sarbanes-Oxley Act (SOX)

For a long time, external auditors attempted to defend themselves in fraud cases by claiming that the purpose of a financial audit (as opposed to a fraud audit) is not to detect fraud. Sections 302, 404 and 906 of the Sarbanes Oxley changed the responsibilities of corporate managements and of auditors with respect to fraud mitigation.

- Section 302 mandates corporate responsibility for financial reporting and internal controls. It requires the CEO and CFO to certify that they have reviewed the report for the periodic filing and that the financial statements and disclosures in all material aspects truly represent the operational results and financial conditions of the company. [Sarbanes-Oxley Act Section 302. Retrieved September 2007 from [http://www.sox-online.com/act\\_section\\_302.html](http://www.sox-online.com/act_section_302.html)]
- Section 404 requires management's assessment of internal controls. It requires each annual report filed with SEC to contain a report on its internal controls. This report should state management's responsibility to establish and maintain internal control procedures for financial reporting and also assess the effectiveness of these internal controls. A registered public accounting firm

needs to evaluate management's assessment of their internal controls.

[Sarbanes-Oxley Act Section 404. Retrieved September, 2007 from [http://www.sox-online.com/act\\_section\\_404.html](http://www.sox-online.com/act_section_404.html)]

- Section 906 increases corporate responsibility for financial reporting by requiring the chief executive officer and the chief financial officer to certify financial statements filed with SEC. These certifications must state compliance with Securities Exchange Act and also state that all material aspects truly represent the operational results and financial conditions of the company. [The Sarbanes-Oxley Act of 2002. Retrieved September, 2007 from <http://www.sox-online.com/soxact.html#sec906>]

To comply with the Sarbanes-Oxley Act, corporations need to improve documentation and internal controls for financial reporting. These internal controls need to be tested and monitored to make financial reporting transparent. Management is required to provide a report on its internal controls. An independent auditor has to evaluate management's assessment of its internal controls and provide a report. Thus, the external auditors now have added responsibility for fraud mitigation.

#### Public Company Accounting Oversight Board (PCAOB)

The Sarbanes Oxley Act of 2002 created the Public Company Accounting Oversight Board (PCAOB) for setting auditing standards for public companies. Smaller companies continue to use Statements on Auditing Standards from the American Institute of Certified Public Accountants (AICPA). On July 25 2007, the SEC approved PCAOB's Accounting Standard No 5 "An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements" ["PCAOB's New Audit Standard for Internal Control over Financial Reporting is approved by the SEC". Date: July 25, 2007. Retrieved September, 2007 from [http://www.pcaobus.org/News\\_and\\_Events/News/2007/07-25.aspx](http://www.pcaobus.org/News_and_Events/News/2007/07-25.aspx)].

All registered audit firms will be required to use this standard for their audits of internal controls.

## Statements on Auditing Standards (SAS)

In November 2002, in the wake of the accounting scandals, the Auditing Standards Board issued SAS 99 "Consideration of Fraud in a Financial Statement Audit". SAS 99 supersedes SAS 82. It gives the auditor more guidance to detect material misstatements due to fraud in financial statements. [CPAs' "Perceptions of the Impact of SAS 99" Authors: Donald C. Marczewski and Michael D. Akers. Source: The CPA Journal.

June 2005 issue. Pg 38. Retrieved September 2007 from <http://www.nysscpa.org/cpajournal/2005/605/essentials/p38.htm>]

## Biometrics: The Solution

Accounting frauds perpetrated by high-level managers of major companies prompted the passage of the Sarbanes-Oxley Act. These accounting frauds were possible because of weak internal control systems and of external auditors claiming that financial audits were not designed to detect frauds. The DuPont case shows that there are reasons beyond accounting frauds for strengthening internal control systems. A single employee accessing trade secrets can cause hundreds of millions of dollars of losses for a company, lawsuits, and declines in the value of a company's stock.

According to a 2006 study by Association of Certified Fraud Examiners, 25% of internal frauds caused at least US\$1 million in losses per incident. The first single incident median loss was US\$159,000 and in over 9 cases the internal fraud cost the company over US\$1 billion.

[ACFE (Association of certified Fraud examiners) 2006 Report to the nation on Occupational Fraud.

Retrieved September 2007 from [http://www .acfe.com/documents/2006-rttn.pdf](http://www.acfe.com/documents/2006-rttn.pdf)]

Frauds cannot be completely eliminated, but controls can be put in place to minimize frauds. A company has to have tighter controls over the user's system access rights, limit access to sensitive data based on user role, and monitor who tried to access

sensitive data. Instead of using a weak password control system, companies need to be using a user access authentication system with these characteristics: unique identification of each user and controls extending to the transaction and field levels.

## **Biometrics**

Biometrics can provide this solution. Biometrics uses certain characteristics of a person such as fingerprints, retinal pattern, or even speech pattern to uniquely identify a person, grant access for an authorized user and clearly reject unauthorized users. Biometrics for computer authentication is different than biometrics for law enforcement. For law enforcement an “open system” is used where law enforcement authorities scan a finger with an optical sensor and store an entire image of the finger (mostly all fingers) in the national IDENT or AFIS database. This enables all law enforcement authorities to check fingerprints against those templates.

Biometrics for computer authentication can protect the privacy of users of the system while still identifying uniquely the users. A proprietary binary template (01110101010) consisting of a unique set of numbers is created, not an optical scan of the fingerprint. While a few laptop computers had fingerprint sensors already in the late 1990s, every major laptop manufacturer offers now at least one model with a built-in fingerprint sensor. With the astonishing improvements in the sensor technology, manufacturers have switched from a larger touch sensor to a smaller and much more secure swipe sensor. Built-in fingerprint sensors, together with hard drive encryption, were the top 2 requirements from corporate America for laptop manufacturers.

[Notebook with a built-in fingerprint sensor”. Author: Jean Francois Manguet. Retrieved September 2007 from

[http://perso.orange.fr/fingerchip/biometrics/types/fingerprint\\_products\\_notebooks.htm](http://perso.orange.fr/fingerchip/biometrics/types/fingerprint_products_notebooks.htm)]

### CASE STUDY

## **DuPont Fraud**

In the DuPont fraud case, Gary Min, a former employee who worked as a research chemist at DuPont stole trade secrets from DuPont valued at US\$400 million. He had accepted employment with rival firm Victrex in 2005. After accepting the employment, he continued

to work with DuPont for a few months and downloaded 180 confidential papers and thousands of abstracts from the DuPont server and intended to use this confidential data in his new post. Most of this data was unrelated to his work. When he resigned from DuPont, his unusually high usage of the server hosting DuPont's technical documentation was detected. Victrex cooperated with DuPont and seized Min's laptop and handed it over to the FBI for investigation.

Min later admitted to misusing DuPont's trade secrets.

["DuPont chemist pleads guilty to IP theft." Computer Fraud & Security. Volume 2007 issue 3

March 2007, pg 3 Retrieved online from Science Direct database in September 2007

[http://www.sciencedirect.com/lib-proxy.fullerton.edu/science?\\_ob=ArticleURL&\\_udi=B6VNT-4NGKDYC-3&\\_user=521375&\\_coverDate=03%2F31%2F2007&\\_alid=615118925&\\_rdoc=1&\\_fmt=full&\\_orig=search&\\_cdi=6187&\\_sort=d&\\_docanchor=&view=c&\\_ct=1&\\_acct=C000059558&\\_version=1&\\_urlVersion=0&\\_userid=521375&md5=ee6baf3188afeb123fd6c395b75b07f2](http://www.sciencedirect.com/lib-proxy.fullerton.edu/science?_ob=ArticleURL&_udi=B6VNT-4NGKDYC-3&_user=521375&_coverDate=03%2F31%2F2007&_alid=615118925&_rdoc=1&_fmt=full&_orig=search&_cdi=6187&_sort=d&_docanchor=&view=c&_ct=1&_acct=C000059558&_version=1&_urlVersion=0&_userid=521375&md5=ee6baf3188afeb123fd6c395b75b07f2)]

### **Sarbanes-Oxley Compliant yet Exposed to Fraud**

DuPont's 10-K report filed in 2005, 2006 & 2007 includes CEO & CFO's certifications of the financial statements filed with SEC stating compliance with Section 13 (a) of Securities Exchange Act of 1934 and also stating that the report fairly represents in all material aspects the financial condition and results of operations of the company. Their 10 k reports also include

Management's Reports on Responsibility for Financial Statements and Internal Control over Financial Reporting. These show DuPont's corporate responsibility for financial reporting and their

internal controls. These were assessed and certified by public accounting firm

PricewaterhouseCoopers LLC as seen in their 10-k report. Thus, **DuPont complied with SOX.**

**This compliance did not eliminate their exposure to fraud by internal security threats.**

This fraud could have been mitigated if biometrics were used at DuPont for internal controls. The confidential data access should have been restricted to certain users by using biometric computer authentication instead of passwords for computer authentication. Min should have had access after biometric authentication to only data related to his research.

DuPont could have used various levels of biometrics authentication to grant access to users accessing the confidential data. As this was unrelated to Min's work, Min would not have access to this confidential data. This would prevent unauthorized users from accessing the trade secrets. The report of who accessed or tried to access this server would have shown that Min tried to access this data and would have authorities at DuPont investigate Min's intentions. Biometrics authentication could have saved DuPont the risk of losing confidential data to rival firms and also have saved them the expense of going through a court case to protect their intellectual property.

*Paul Sheldon Foote is Professor of Accounting at California State University, Fullerton and Reena Hora is Independent Information Technology and Services Professional and Master of Science Information Technology at California State University, Fullerton.*

For more information, please send your e-mails to [swm@infothe.com](mailto:swm@infothe.com).

©2007 [www.SecurityWorldMag.com](http://www.SecurityWorldMag.com). All rights reserved.

[http://www.securityworldmag.com/head/weekly\\_view.asp?idx=1227](http://www.securityworldmag.com/head/weekly_view.asp?idx=1227)