

Fraud Mitigation and Biometrics following Sarbanes-Oxley

“Your company might be compliant, but you are still exposed to fraud!”

Paul Sheldon Foote

Reena Hora

California State University, Fullerton

pfoote@fullerton.edu

The authors acknowledge with thanks the contributions of realtime North America, Inc. and of its Chief Operating Officer and Director for Biometric Solutions, Thomas Neudenberger, of content for this article.

Abstract

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.

Accounting Frauds and Scandals

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. For general summaries of SOX, see:

<http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/Summary+of+the+Provisions+of+the+Sarbanes-Oxley+Act+of+2002.htm>

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. [1]

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 \$6 million to defend ***successfully*** a lawsuit involving a client with \$20,000 annual audit fees. At least one major insurance company has responded by refusing to insure accounting firms for legal liabilities. [1]

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

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. [2]

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. [3]

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. [4]

CRIMINAL PENALTIES. - Whoever -

"(1) certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the

requirements set forth in this section shall be fined not more than \$1,000,000 or imprisoned not more than 10 years, or both; or

"(2) willfully certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than \$5,000,000, or imprisoned not more than 20 years, or both."

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.

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.

Appendices A, B and C show DuPont's management reports on its internal controls for financial reporting for SOX compliance. Appendices A-1, B-1 and C-2 are independent auditor PricewaterhouseCoopers LLP's report on their evaluation of management's assessment of their internal controls.

These certifications are examples of SOX compliance.

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*" [5]

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. [6]

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 \$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. [7]

Sarbanes-Oxley compliant yet exposed to fraud:

Appendices A, B and C 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 by Appendix A-1, B-1 and C-2. 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.

Biometrics: an Identity Management and Fraud Mitigation 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 \$1 million in losses per incident. The first single incident median loss was \$159,000 and in over 9 cases the internal fraud cost the company over \$1 billion. [8]

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 1990's, 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. They favor the proven swipe sensor from biometric leader UPEK. Built-in fingerprint sensors, together with hard drive encryption, were the top 2 requirements from corporate America for laptop manufacturers. [9]

A company does not need to wait until the next round of computer purchases to implement biometrics solutions. Inexpensive USB add-ons using UPEK sensors are available from UPEK, The Cherry Corporation and other vendors.



<http://www.upek.com/>

<http://www.cherrycorp.com/>

Fraud mitigation in an SAP Environment using bioLock

Security risks

A major reason for the popularity of SAP R/3 with corporations is the fact that SAP integrated most of the data of a company across most or all of the departments. While corporations need integrated data, individual users of computer systems should not be able to access data for which they lack authorizations. Internal control systems must have segregation of duties. The Sarbanes-Oxley Act formalized the legal requirements for corporations and for external auditors.

SAP is all about business processes and roles assigned to users for these processes. This ensures segregation of duties. SAP has a report-generating feature which generates reports of who performed which transaction when. So, this does seem like it is complying with SOX. Is this enough, however, to mitigate fraud?

1. The system gives access to users with passwords which match the approved user profile. Anyone having access to this password can basically log on to SAP and perform the desired transaction.
2. SOX requires segregation of duties. SAP provides that with allowing access to certain transactions to restricted users with predefined roles having their passwords. Is this really secure? Anyone who has access to the username and password can easily perform the transaction. This defies segregation of duties. Basically, a user can log on to the SAP system perform a transaction and use another password and username to perform another transaction. It is very easy for User A to get access to a username and password of User B and perform a Sales transaction and then to get User.C's username and password and perform a financial transaction. The SAP report would show that User B and User C have

performed the transaction when User A has performed the transaction. User B and User C are completely innocent. Another scenario would be that User B logs on to SAP and leaves his desk to make a few photocopies. Meanwhile, User A goes to User B's desk and performs a financial transaction before User B returns. Poor User B has no idea what just happened, but the transaction report would report User B as having performed that transaction. It is impossible to track, which "actual" person accesses or changes critical information

3. Business partners and outsourced companies have access to SAP. Many processes and audits are being outsourced. This would give the users from an outsourced company or external consultants access to company data. Sometimes, business partners and vendors also have access to the company SAP system. This makes the system more vulnerable to security threats. With increasing globalization, many employees access critical information from different parts of the world.

All of the above shows that the SAP system, or any other ERP system using only passwords, does not provide adequate fraud mitigation or possibly even compliance with SOX sections 302 and 404. The historically accepted flaws in security completely defy the internal controls and segregation of duties required by SOX. Everything has changed since the invention of computers including programming languages and platforms, but one thing which has not changed is the most critical factor: security. We still use the same old way of usernames and passwords for security. This is just an illusion of security. There are many ways to discover passwords, ranging from casual coffee conversation to more sophisticated software which grabs passwords. If the password requirements get more complex, to increase security people usually write down this password someplace so that they do not forget the complex password. Whoever has access to this written password is a security threat. [10]

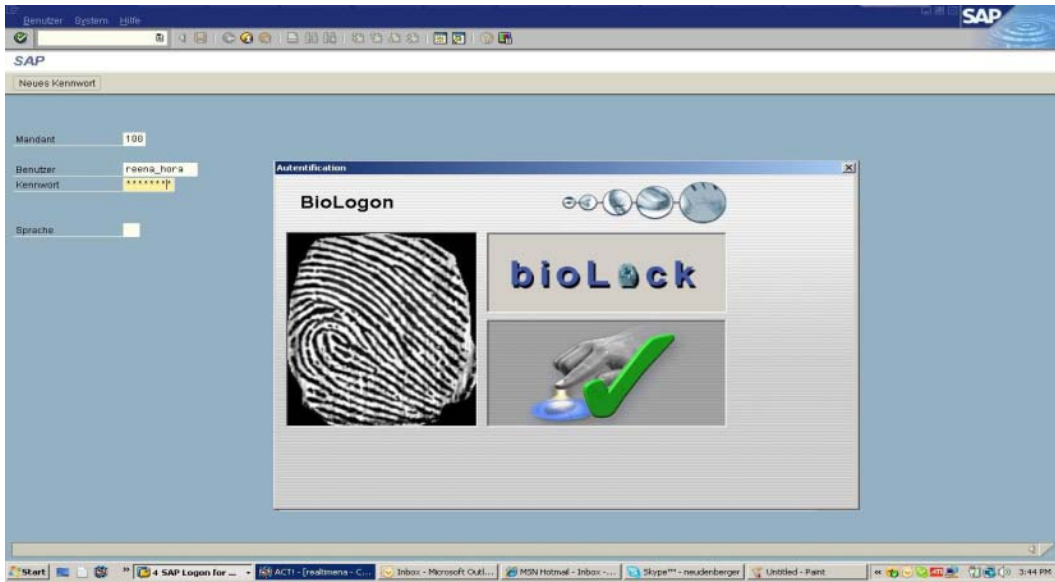
Another easy way to access passwords is small cameras that now are built in cell phones, pens, and buttons. Someone can record a password and play it back slowly to see what the password was. Even if you cannot play the password back, you can determine the password. To view a demonstration of this, visit the following educational website www.showpasswordsthefinger.com and see, if you can figure out the password in the video. It is quite easy to determine what she is typing. The following link shows how truly dangerous it is to use only passwords for security.

http://www.realtimenorthamerica.com/download/Fishing_for_Passwords.pdf

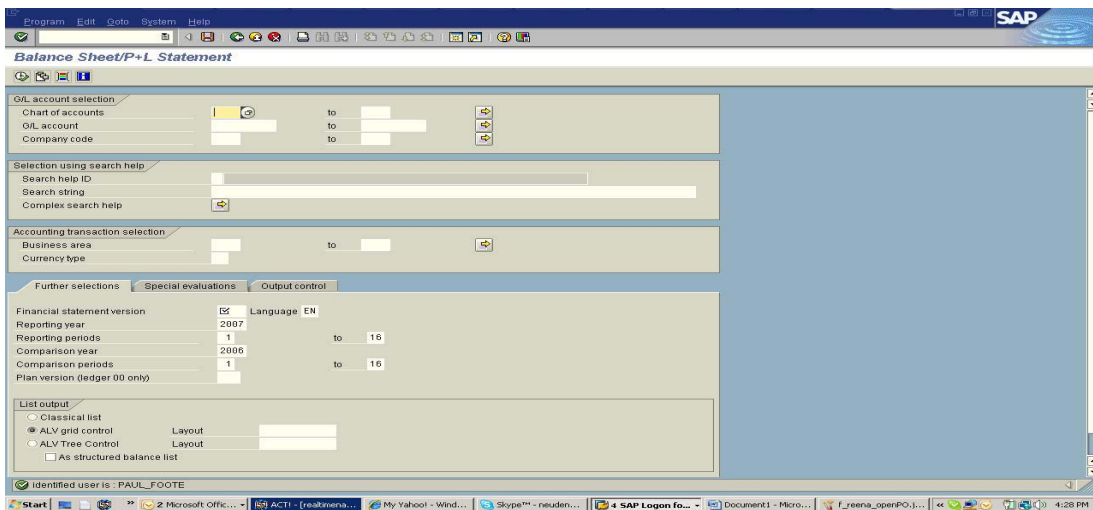
realtime has used biometrics to create bioLock. The bioLock system is currently the only biometrics system certified by SAP for use with SAP's systems. [10]

bio Lock provides 3 levels of security in an SAP environment.

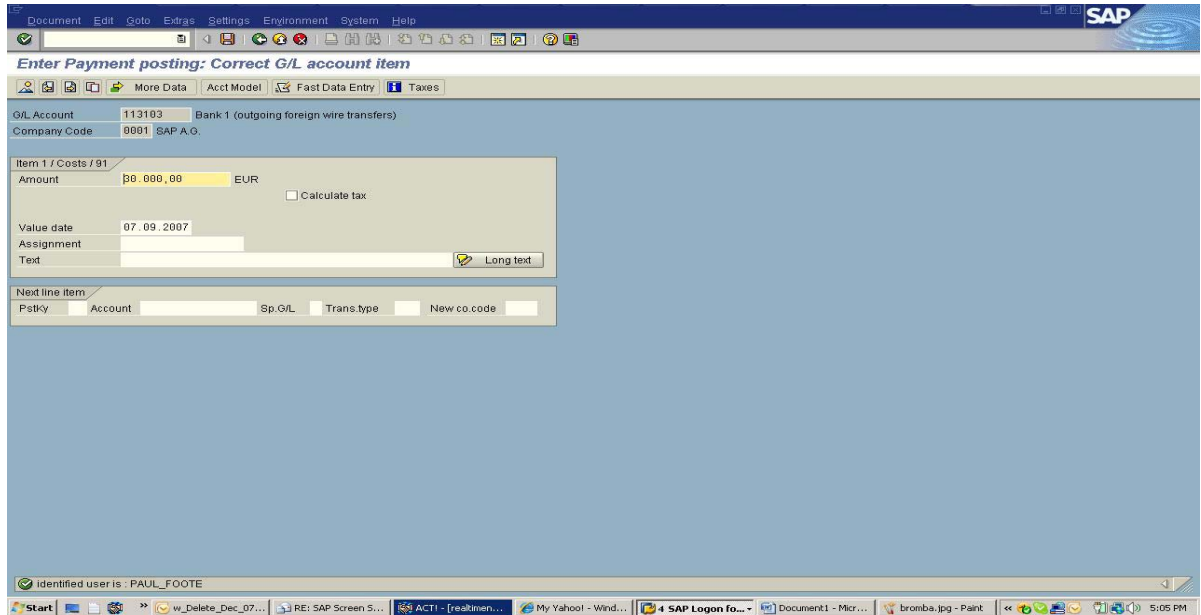
1. Firstly, the user will have to provide fingerprint identification to get access into the SAP system.



2. Secondly, bioLock controls can be installed at certain transaction levels requiring fingerprint verification before allowing the transaction. For example: A company's balance sheet has sensitive data and the access to this can be restricted to authorized personnel. So, whoever tries to view the balance sheet will be asked for fingerprint authentication. If someone who does not have access to this balance sheet tries to view this balance sheet, the system will kick them out and also log that they tried to access the system to view the balance sheet. Unlike the Enron case, this system can also provide evidence in court cases if the executive management had viewed the balance sheet in case of fraud.




3. Thirdly, the security can be further tightened by requiring fingerprint authentication at the individual field level. For example:
 Something as secure as a wire transfer can be set to require a fingerprint authentication if the amount to be transferred is more than \$10,000. If any amount more than \$10,000 is entered in the field, then the system would automatically require fingerprint authentication. To add security, the wire transfers could be set to require dual fingerprint authentication which would require an additional designated person to approve the wire transfer.



bioLock can create a log of who accessed or tried to access the system and of who performed or tried to perform certain transactions within SAP. It even has a feature of 911 alerts wherein you can designate a finger as your 911 finger and use it if somebody forces you to perform a transaction. This will immediately alert security.

Call bioLock Protocol and System-Log

Selection:
 Date from 07.09.2007
 Date to 07.09.2007



Current Date	Time	User Name	function	Text	Area	N	bioLock-User	Text	Transaction Code	Transaction text
07.09.2007	22:09:18	REENA_HORA	000	SAP Logon	Y4	3	PAUL_FOOTE	not authorized for this function	SESSION_MANAGER	Session Manager Menu Tree Display
07.09.2007	22:13:38	REENA_HORA	000	SAP Logon	Y4	1	REENA_HORA	was recognized	SESSION_MANAGER	Session Manager Menu Tree Display
07.09.2007	22:24:14	REENA_HORA	104	Display Purchase Order ME29N	Y4	1	REENA_HORA	was recognized	ME29N	Release purchase order
07.09.2007	22:24:42	REENA_HORA	104	Display Purchase Order ME29N	Y4	2		was rejected	ME29N	Release purchase order
07.09.2007	22:24:55	REENA_HORA	104	Display Purchase Order ME29N	Y4	1	REENA_HORA	was recognized	ME29N	Release purchase order
07.09.2007	22:25:32	PAUL_FOOTE	000	SAP Logon	Y4	1	PAUL_FOOTE	was recognized	SESSION_MANAGER	Session Manager Menu Tree Display
07.09.2007	22:25:53	PAUL_FOOTE	104	Display Purchase Order ME29N	Y4	3	REENA_HORA	not authorized for this function	ME29N	Release purchase order
07.09.2007	22:26:24	PAUL_FOOTE	001	bioLock	Y4	1	PAUL_FOOTE	was recognized	/REALTIME/BIOLOCK	bioLock - Administration
07.09.2007	22:26:46	SAPALL	000	SAP Logon	Y4	1	THOMAS	was recognized	SESSION_MANAGER	Session Manager Menu Tree Display
07.09.2007	22:26:57	SAPALL	001	bioLock	Y4	1	THOMAS	was recognized	/REALTIME/BIOLOCK	bioLock - Administration
07.09.2007	22:30:09	PAUL_FOOTE	006	Open Balance Sheet Transaction	Y4	1	PAUL_FOOTE	was recognized	S_ALR_87012284	Balance Sheet/P+L Statement
07.09.2007	22:32:01	PAUL_FOOTE	007	Display Balance Sheet	Y4	3	REENA_HORA	not authorized for this function	START_REPORT	Starts report
07.09.2007	22:32:18	PAUL_FOOTE	006	Open Balance Sheet Transaction	Y4	1	PAUL_FOOTE	was recognized	S_ALR_87012284	Balance Sheet/P+L Statement
07.09.2007	22:32:32	PAUL_FOOTE	007	Display Balance Sheet	Y4	1	PAUL_FOOTE	was recognized	START_REPORT	Starts report

The above report shows that using bioLock no one can logon as a different user. The report gives the following details.

When SAP user Paul (bioLock-User Column) tried to log on as Reena (SAP User / User Name Column to the left) the system identified him and denied access. When user Reena tried to logon as herself the system uniquely identified her and allowed system access to release a purchase order of \$40,000 car. When user Reena was away and another unidentified person who didn't even have a biometric template tried to access the purchase order on user Reena's computer, the bioLock could not identify the stranger and rejected him. When user Paul tried to access the system as himself, the system uniquely identified him and granted access. When user Reena tried to create a Purchase order on this computer the system rejected her. The report shows next Thomas logged on as administrator and accessed the bioLock transaction. The next line shows that Paul opened the balance sheet transaction. Next, Reena tried to view this balance sheet and as this was protected by bioLock the system identified her and denied access to the balance sheet. The last line shows Paul opened the balance sheet transaction again.

A report like this gives details of who tried to access the system and performed or viewed which transaction. This can prove which officers and managers looked at certain financial statements or documents. This report can be used as evidence in court cases of who accessed the financial and other documents and performed which tasks.

07.09.2007	23:06:13	PAUL_FOOTE	030	Financial Transaction on input Level	Y4	3	REENA_HORA	not authorized for this function	FB01	Post Document
07.09.2007	23:07:10	PAUL_FOOTE	030	Financial Transaction on input Level	Y4	1	PAUL_FOOTE	was recognized	FB01	Post Document
07.09.2007	23:11:28	SAPALL	001	bioLock	Y4	1	THOMAS	was recognized	/REALTIME/BIOLOCK	bioLock - Administration
07.09.2007	23:14:50	SAPALL	001	bioLock	Y4	5	APRIL	was confirmed	/REALTIME/BIOLOCK	bioLock - Administration
07.09.2007	23:16:06	PAUL_FOOTE	030	Financial Transaction on input Level	Y4	2		was rejected	FB01	Post Document
07.09.2007	23:17:32	PAUL_FOOTE	030	Financial Transaction on input Level	Y4	3	REENA_911	not authorized for this function	FB01	Post Document

The above report gives the following details.

It shows that Reena was identified but rejected as she tried to perform a wire transfer on computer which was logged on as SAP user Paul. Next the report shows that SAP user Paul tried to make a wire transfer above a certain amount which had an internal control requiring biometric confirmation. The report also shows that SAP user Thomas who was logged in as SAP ALL administrator tried to access the bioLock transaction. The next line shows that SAP user April confirmed Thomas’s request for the bioLock transaction. For extremely critical task two different people and their biometric authentication can be required to perform a task. This ensures the 4-eye principle within the SAP system.



The next to the last line shows that an unauthorized user who was not their employee tried to make a wire transfer on Paul’s computer which was logged onto SAP. AS the system did not recognize him, he was rejected. In a desperate attempt, the intruder forces Reena to execute the wire transfer for him on Paul’s computer. Reena reacts calmly and uses her separately enrolled 911 finger for authentication. This system rejects the task visible for the intruder, but notes in the log file that a “911 finger” was used to alert authorities about a known security breach. An automated scanner could alert security when a 911 is posted in the log file.

This report demonstrates how a sensitive transaction, such as a wire transfer, is protected by bioLock and will also provide evidence in a court case.

Using a technology like bioLock provides true segregation of duties and internal controls as the system uniquely identifies each user and only allows certain users access to sensitive data or transactions. All users in a company do not need to have a bioLock controlled access. Only certain users having access to sensitive data can be set to access the critical data using bioLock. Once the sensitive transactions are locked by access to restricted users by bioLock all other users are automatically filtered out and blocked from accessing the sensitive data. For the first time, the business can clearly define a simple “invitation only” list for certain transactions and users. bioLock will ensure that no other

actual users will access the protected functions. bioLock packages are available with as low as 50 users and can be available for as many users as required. A complete installation package starts under \$100,000 and would go up depending on the number of users. This will provide evidence in case of a court case and also make it very transparent to auditors. This will truly make SAP compliant with SOX.

In the DuPont case, the company's management did not detect Min's unusually high activity on the server with the intellectual property until he resigned. The management did not have effective internal controls securing access to the server. They could have set controls which would flag the authorities if there was such unusual activity. They could have purchased a bioLock package of 1,000 seats protecting their top 1,000 users with access to their various departments including finance, human resources, research to name a few. This would have cost them a few hundred thousand dollars, a small price to protect their intellectual property, image, stock price and hassles of a court case. This would have mitigated the risk of losing \$ 400 million of intellectual property. If DuPont had lost millions of dollars, there would have been shareholder lawsuits. Using bioLock, they could have restricted scientists such as Min's access to a small reasonable part of the system for research. Anything above normal could have been set to require dual fingerprint authentication and also raise a flag to be investigated if found unreasonable. bioLock could also have provided a report of who accessed and who tried to access the data. This evidence could have been used in the court case against Min. DuPont's internal controls were inadequate for this type of fraud. While DuPont's executives and external auditors (PricewaterhouseCoopers) certified the adequacy of internal control systems for accounting frauds, there are other types of frauds for which shareholders can sue companies and external auditors.

Conclusions

Contrary to popular beliefs, corporate managements and external auditors have legal obligations to mitigate fraud. In addition to frauds perpetrated by persons not working for a company and accounting frauds perpetrated by employees, companies can be exposed to large risks of losses from the theft of intellectual property. Laws and regulations provide only minimum standards for corporate internal control systems. For corporate managers, directors, and external auditors who want to avoid lawsuits, they need to implement better security than the use of only passwords. Using only passwords is an invitation to fraudsters. Biometrics systems provide fraud mitigation.

References

1. Whittington, O. Ray, and Kurt Pany, *Principles of Auditing & Other Assurance Services*, Sixteenth Edition, McGraw-Hill Irwin, 2008.
2. Sarbanes-Oxley Act Section 302. Retrieved September 2007 from http://www.sox-online.com/act_section_302.html
3. Sarbanes-Oxley Act Section 404. Retrieved September, 2007 from http://www.sox-online.com/act_section_404.html
4. The Sarbanes-Oxley Act of 2002. Retrieved September, 2007 from <http://www.sox-online.com/soxact.html#sec906>
5. “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
6. “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>
7. “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
8. 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>
9. “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
10. www.fraudmitigation.com

Appendix – A-1

CONSENT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

We hereby consent to the incorporation by reference in the Registration Statements on Form S-3 (No. 33-53327, No. 33-60069, and No. 333-86363) and Form S-8 (No. 33-51817, No. 33-60037, No. 33-61703, No. 333-32185, No. 333-34004, No. 333-44358, No. 333-44360, No. 333-44362, No. 333-82573, No. 333-106585, No. 333-106527, No. 333-105228, No. 333-105224, No. 33-85599, No. 333-118042, No. 333-114330, and No. 333-114329) of E. I. du Pont de Nemours and Company of our report dated February 25, 2005, relating to the consolidated financial statements, management's assessment of the effectiveness of internal control over financial reporting, and the effectiveness of internal control over financial reporting, which appears in this Form 10-K.

/s/ PricewaterhouseCoopers LLP
Philadelphia, Pennsylvania
March 2, 2005

Appendix A-2

CERTIFICATIONS

I, Charles O. Holliday, Jr., certify that:

1.

I have reviewed this report on Form 10-K for the period ended December 31, 2004 of E. I. du Pont de Nemours and Company;

2.

Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3.

Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4.

The registrant's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

a)

Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

b)

Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

c)

Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

d)

Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5.

The registrant's other certifying officer and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

a)

All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

b)

Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: March 2, 2005

By: /s/ CHARLES O. HOLLIDAY, JR.

Charles O. Holliday, Jr.
Chief Executive Officer and
Chairman of the Board

Appendix A-3

CERTIFICATIONS

I, Gary M. Pfeiffer, certify that:

1.

I have reviewed this report on Form 10-K for the period ended December 31, 2004 of E. I. du Pont de Nemours and Company;

2.

Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3.

Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4.

The registrant's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

a)

Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

b)

Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

c)

Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the

disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

d)

Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5.

The registrant's other certifying officer and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

a)

All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

b)

Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: March 2, 2005

By: /s/ GARY M. PFEIFFER

Gary M. Pfeiffer
Senior Vice President and
Chief Financial Officer

Appendix A-4

**Certification of CEO Pursuant to
18 U.S.C. Section 1350,
As Adopted Pursuant to
Section 906 of the Sarbanes-Oxley Act of 2002**

In connection with the Annual Report of E. I. du Pont de Nemours and Company (the "Company") on Form 10-K for the period ending December 31, 2004 as filed with the Securities and Exchange Commission on the date hereof (the "Report"), Charles O. Holliday, Jr., as Chief Executive Officer of the Company, hereby certifies, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that:

(1)

The Report fully complies with the requirements of Section 13(a) of the Securities Exchange Act of 1934; and

(2)

The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

/s/ CHARLES O. HOLLIDAY,
JR.

Charles O. Holliday, Jr.
Chief Executive Officer
March 2, 2005

Appendix A-5

**Certification of CFO Pursuant to
18 U.S.C. Section 1350,
As Adopted Pursuant to
Section 906 of the Sarbanes-Oxley Act of 2002**

In connection with the Annual Report of E. I. du Pont de Nemours and Company (the "Company") on Form 10-K for the period ending December 31, 2004 as filed with the Securities and Exchange Commission on the date hereof (the "Report"), Gary M. Pfeiffer, as Chief Financial Officer of the Company, hereby certifies, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that:

(1)

The Report fully complies with the requirements of Section 13(a) of the Securities Exchange Act of 1934; and

(2)

The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

/s/ GARY M. PFEIFFER

Gary M. Pfeiffer
Chief Financial Officer
March 2, 2005

Appendix A -Source: DUPONT E I DE NEMOUR, 10-K, March 02, 2005

Appendix B-1

CONSENT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

We hereby consent to the incorporation by reference in the Registration Statements on Form S-3 (No. 33-53327, No. 33-60069, No. 333-86363, and No. 333-124683) and Form S-8 (No. 33-51817, No. 33-61703, No. 333-32185, No. 333-34004, No. 333-44358, No. 333-82573, No. 333-106585, No. 333-106527, No. 333-105228, No. 333-105224, No. 333-85599, No. 333-118042, No. 333-114330, No. 333-129494, No. 333-129495, and No. 333-129496) of E. I. du Pont de Nemours and Company of our report dated February 24, 2006, relating to the consolidated financial statements, management's assessment of the effectiveness of internal control over financial reporting, and the effectiveness of internal control over financial reporting, which appears in this Form 10-K.

/s/ PricewaterhouseCoopers LLP

Philadelphia, Pennsylvania
February 28, 2006

Appendix B-2

CERTIFICATIONS

I, Charles O. Holliday, Jr., certify that:

1.

I have reviewed this report on Form 10-K for the period ended December 31, 2005 of E. I. du Pont de Nemours and Company;

2.

Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3.

Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4.

The registrant's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

a)

Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

b)

Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

c)
Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

d)
Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5.
The registrant's other certifying officer and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

a)
All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

b)
Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: February 28, 2006

By: /s/ CHARLES O. HOLLIDAY,
JR.

Charles O. Holliday, Jr.
Chief Executive Officer and
Chairman of the Board

Appendix B-3

CERTIFICATIONS

I, Gary M. Pfeiffer, certify that:

1.

I have reviewed this report on Form 10-K for the period ended December 31, 2005 of E. I. du Pont de Nemours and Company;

2.

Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3.

Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4.

The registrant's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

a)

Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

b)

Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

c)

Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

d)

Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5.

The registrant's other certifying officer and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

a)

All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

b)

Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: February 28, 2006

/s/ GARY M. PFEIFFER

By: _____

Gary M. Pfeiffer
Senior Vice President and
Chief Financial Officer

Appendix B-4

**Certification of CEO Pursuant to
18 U.S.C. Section 1350,
As Adopted Pursuant to
Section 906 of the Sarbanes-Oxley Act of 2002**

In connection with the Annual Report of E. I. du Pont de Nemours and Company (the "Company") on Form 10-K for the period ending December 31, 2005 as filed with the Securities and Exchange Commission on the date hereof (the "Report"), Charles O. Holliday, Jr., as Chief Executive Officer of the Company, hereby certifies, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that:

(1)

The Report fully complies with the requirements of Section 13(a) of the Securities Exchange Act of 1934; and

(2)

The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

/s/ CHARLES O. HOLLIDAY, JR.

Charles O. Holliday, Jr.
Chief Executive Officer
February 28, 2006

Appendix B-5

**Certification of CFO Pursuant to
18 U.S.C. Section 1350,
As Adopted Pursuant to
Section 906 of the Sarbanes-Oxley Act of 2002**

In connection with the Annual Report of E. I. du Pont de Nemours and Company (the "Company") on Form 10-K for the period ending December 31, 2005 as filed with the Securities and Exchange Commission on the date hereof (the "Report"), Gary M. Pfeiffer, as Chief Financial Officer of the Company, hereby certifies, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that:

(1)

The Report fully complies with the requirements of Section 13(a) of the Securities Exchange Act of 1934; and

(2)

The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

/s/ GARY M. PFEIFFER

Gary M. Pfeiffer
Chief Financial Officer
February 28, 2006

Appendix B Source: DUPONT E I DE NEMOUR, 10-K, February 28, 2006

Appendix C-1

Management's Reports on Responsibility for Financial Statements and Internal Control over Financial Reporting

Management's Report on Responsibility for Financial Statements

Management is responsible for the Consolidated Financial Statements and the other financial information contained in this Annual Report on Form 10-K. The financial statements have been prepared in accordance with generally accepted accounting principles in the United States of America (GAAP) and are considered by management to present fairly the company's financial position, results of operations and cash flows. The financial statements include some amounts that are based on management's best estimates and judgments. The financial statements have been audited by the company's independent registered public accounting firm, PricewaterhouseCoopers LLP. The purpose of their audit is to express an opinion as to whether the Consolidated Financial Statements included in this Annual Report on Form 10-K present fairly, in all material respects, the company's financial position, results of operations and cash flows. Their report is presented on the following page.

Management's Report on Internal Control over Financial Reporting

Management is responsible for establishing and maintaining an adequate system of internal control over financial reporting as defined in Rules 13a-15(f) and 15d-15(f) under the Securities Exchange Act of 1934. The company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. The company's internal control over financial reporting includes those policies and procedures that:

- i. pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;
- ii. provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles and that receipts and expenditures of the company are being made only in accordance with authorization of management and directors of the company; and
- iii. provide reasonable assurance regarding prevention or timely detection of unauthorized acquisitions, use or disposition of the company's assets that could have a material effect on the financial statements.

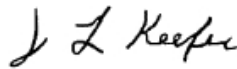
Internal control over financial reporting has certain inherent limitations which may not prevent or detect misstatements. In addition, changes in conditions and business practices may cause variation in the effectiveness of internal controls.

Management assessed the effectiveness of the company's internal control over financial reporting as of December 31, 2006, based on criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in *Internal Control-Integrated Framework*. Based on its assessment and those criteria, management concluded that the company maintained effective internal control over financial reporting as of December 31, 2006.

Management's assessment of the effectiveness of the company's internal control over financial reporting as of December 31, 2006 has been audited by PricewaterhouseCoopers LLP, an independent registered public accounting firm, as stated in their report presented on the following page.



Charles O. Holliday, Jr.
*Chairman of the Board and
Chief Executive Officer*



Jeffrey L. Keefer
*Executive Vice President
and Chief Financial Officer*

February 23, 2007

Appendix C-2

Report of Independent Registered Public Accounting Firm

To the Stockholders and the Board of Directors of
E. I. du Pont de Nemours and Company:

We have completed integrated audits of E. I. du Pont de Nemours and Company's consolidated financial statements and of its internal control over financial reporting as of December 31, 2006 in accordance with the standards of the Public Company Accounting Oversight Board (United States). Our opinions, based on our audits, are presented below.

Consolidated financial statements and financial statement schedule

In our opinion, the consolidated financial statements listed in the index appearing under Item 15(a)(1) present fairly, in all material respects, the financial position of E. I. du Pont de Nemours and Company and its subsidiaries at December 31, 2006 and December 31, 2005, and the results of their operations and their cash flows for each of the three years in the period ended December 31, 2006 in conformity with accounting principles generally accepted in the United States of America. In addition, in our opinion, the financial statement schedule listed in the index appearing under Item 15(a)(2) presents fairly, in all material respects, the information set forth therein when read in conjunction with the related consolidated financial statements. These financial statements and financial statement schedule are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements and financial statement schedule based on our audits. We conducted our audits of these statements in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit of financial statements includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements, assessing the accounting principles used and significant estimates made by management and evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

As discussed in Note 1 to the consolidated financial statements, the Company changed its accounting for defined benefit pension and other postretirement plans during 2006 and for the consolidation of variable interest entities during 2004.

Internal control over financial reporting

Also, in our opinion, management's assessment, included in "Management's Report on Internal Control Over Financial Reporting" appearing on page F-2, that the Company maintained effective internal control over financial reporting as of December 31, 2006

based on criteria established in *Internal Control — Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), is fairly stated, in all material respects, based on those criteria. Furthermore, in our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of December 31, 2006, based on criteria established in *Internal Control — Integrated Framework* issued by the COSO. The Company's management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting. Our responsibility is to express opinions on management's assessment and on the effectiveness of the Company's internal control over financial reporting based on our audit. We conducted our audit of internal control over financial reporting in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. An audit of internal control over financial reporting includes obtaining an understanding of internal control over financial reporting, evaluating management's assessment, testing and evaluating the design and operating effectiveness of internal control and performing such other procedures as we consider necessary in the circumstances. We believe our audit provides a reasonable basis for our opinions.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (iii) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.



PricewaterhouseCoopers LLP
Philadelphia, Pennsylvania
February 23, 2007

Appendix C Source: DUPONT E I DE NEMOUR, 10-K, February 23, 2006