

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

VOLUME 10 NO. 10
NOVEMBER 2008

YOUR SECRET WEAPON IN THE WAR ON FRAUD

IN THE NEWS

Bribe At Your Own Risk

The number of bribery investigations initiated by the US Department of Justice (DOJ) more than tripled from nine in 2003 to 29 in 2007. And this year, more than 80 US companies are under investigation for alleged violations of the Foreign Corrupt Practices Act (FCPA).

Key areas in need of improvement: While most companies (84%) have formal FCPA and anti-corruption policies, whistleblower hotlines and anti-corruption training programs, less than 70% distribute these policies in written form to all employees. Moreover, while three-quarters of companies have hotlines in place, just over one-quarter (27%) promote the use of them among vendors, joint venture partners and other third parties whose actions could put the company on the wrong side of anti-bribery laws.

Essential message: All major companies must initiate "frank discussions and quick action...around the necessity of appropriate compliance programs and activities to lower the risk of violating the FCPA and other anti-bribery and anti-corruption laws."

White-Collar Crime Fighter source: KPMG 2008 Anti-bribery and Anti-corruption Survey. For further information and to obtain the full survey, contact KPMG and www.kpmg.com or Richard H. Girgenti, Forensic National Practice Leader at rgirgenti@kpmg.com.

IN THIS ISSUE

•ROLES/RESPONSIBILITIES

Defining roles eliminates the confusion in fraud prevention..... 3

•DETECTION DUTIES

Audits versus investigations...4

•CARD CRIME CRISIS

Time to get serious about credit card fraud 5

•THE CON'S LATEST PLOY

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

Judge William Wilkins, Nexsen, Pruet, LLC

Criminal Fallout from The Financial Crisis

How to Protect Your Organization



William W. "Billy" Wilkins, Ronald Reagan's first selection in the nation for a federal judgeship and former Chief Judge of the U.S. Court of Appeals for the Fourth Circuit, subsequently served as the first Chair of the U.S. Sentencing Commission (USSC). The Guidelines crafted by the USSC have had a profound impact on white-collar crime litigation since they went into effect in 1991.

Judge Wilkins recently returned to private practice in Greenville, SC. He maintains an avid interest in the role of fraud in US and international business.

We recently spoke with him about his views on the impact of fraud on the current economic crisis and how companies with potential culpability can minimize their risk of damaging legal consequences...

I'm no economist, but having spent 40-plus years in the legal world of white-collar crime, I am certain that criminal conduct played a significant role in getting our financial and economic systems into their current state of unprecedented crisis.

The problem: We won't understand the real extent to which different types of fraud were instrumental in bringing the financial system to the brink of collapse. However, you can be sure that an explosion of allegations of criminal conduct is inevitable. They will involve (among many others) such

activities as...

•**Fraudulent financial reporting**—to conceal the dramatic deterioration of mortgage-related assets on financial institution balance sheets.

•**Misrepresentation of the value of asset-backed securities** by investment banks, securities brokers and related parties.

•**Deception of prospective investors** as to the safety of many of the arcane derivative securities whose

riskiness no one really understood.

•**Mortgage fraud**—perpetrated by a small army of unscrupulous mortgage brokers, collusive appraisers, attorneys, lenders and home builders.

RISKS FOR ORGANIZATIONS

There is no doubt that much of the criminal action initiated in the wake of the financial crisis will target individuals among the groups mentioned above. How successful plaintiffs will be in suing these people is anyone's guess.

More worrisome: The impending legal assault on banks, investment banks, pension funds, insurance companies, hedge funds and similar institutions for fraud, conspiracy, earnings manipulation and other crimes.

Already, the FBI has initiated high-profile investigations of the insurance giant AIG, as well as Lehman Brothers, Fannie Mae and Freddie Mac. And FBI Director Robert Mueller recently testified before Congress, stating that his agency was already investigating more than 25 cases

You can be sure that an explosion of allegations of criminal conduct is inevitable

of alleged corporate fraud related to the collapse of the mortgage industry.

Separately—and perhaps indicative of the type of criminal action that will be making headlines with increasing frequency in coming years—are the convictions in September of four top AIG executives. Former AIG CEO, Ronald Ferguson, faces life imprisonment for his role in a sham transaction going back to 2000 to fraudulently add \$500 million to the insurer’s loss reserves. The latest FBI probe is a clear indication of a history of fraud-related problems facing AIG which

is now front and center in the financial crisis.

COMING CLEAN

As these latest developments indicate, the depth and breadth of the current crisis—coupled with the intensity of consumer outrage over the “greed factor” on Wall Street that they attribute at least in part to their own financial woes—is already spurring prosecutors to aggressively scrutinize companies believed to have culpability for the financial mess.

Several prosecutors in the New York area have already ramped up their investigations of mortgage fraud and securities law violations and white-collar defense attorneys have expressed concern about a rash of indictments that might not have been handed down if the financial and economic crisis had never occurred.

Prediction: Companies that have committed illegal acts related to the mortgage and credit crisis still have some time to gird themselves against the prosecutorial onslaught that is gathering steam with each passing day. However, it may take a couple of high-profile convictions of companies and/or executives in connection with the current crisis to motivate other guilty companies to take action to mitigate the risk of being targeted by aggressive prosecutors.

Key: Executives of corporations who know that their organizations have or may have committed fraud related to the current “meltdown” should do themselves a favor and immediately initiate their own internal investigations.

Reason: While woefully inadequate investigative and prosecutorial resources at all levels of government provide high odds that a culpable organization will “get away with” financial wrongdoing, if they don’t the consequences could all but ruin the organization as it is subjected to increasingly aggressive investigation and prosecution, and potentially devastating punitive measures.

Essential: Cooperate fully with prosecutors. If an internal investigation reveals substantive evidence of wrongdoing, take prompt corrective measures and self-report the wrongdoing to the appropriate prosecutorial office.

Doing so may result in a decision not to prosecute...or to offer a deferred prosecution, where your organization’s admission of wrongdoing results in a

WHITE-COLLAR CRIME FIGHTER

Editor

Peter Goldmann

Consulting Editor

Jane Y. Kusic

Managing Editor

Juliann Lutinski

Senior Contributing Editor

John Middleton

Associate Editor

Barbara Wohler

Design & Art Direction

Ray Holland, Holland Design & Publishing

Panel of Advisers

Credit Card Fraud

Tom Mahoney, Merchant 911.org

Forensic Accounting

Stephen A. Pedneault, Forensic Accounting Services, LLC

Fraud and Cyber-Law

Patricia S. Eyres, Esq., Litigation Management & Training Services Inc.

Corporate Fraud Investigation

R.A. (Andy) Wilson, Wilson & Turner Incorporated

Corporate Integrity and Compliance

Martin Biegelman, Microsoft Corporation

Securities Fraud

G.W. “Bill” McDonald, Investment and Financial Fraud Consultant

Prosecution

Phil Parrott, Deputy District Attorney Denver District Attorney’s Office, Economic Crime Unit

Computer and Information Security

Kenneth Newman, CISM Secure PIKE

Fraud Auditing

Tommie W. Singleton, PhD University of Alabama at Birmingham

White-Collar Crime Fighter (ISSN 1523-0821) is published monthly by White-Collar Crime 101, LLC, 213 Ramapoo Rd., Ridgefield, CT 06877. www.wccfighter.com. Subscription cost: \$295/yr. Canada, \$345. Copyright © 2008 by White Collar Crime 101, LLC. No part may be reproduced without express permission of the publisher.

Mission Statement

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

This community includes law internal auditors...fraud examiners...regulatory officials...corporate security professionals...senior executives...private investigators...and many more.

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

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

Where A Fraud Risk Assessment Can Go Wrong

There is practically an unlimited variety of ways to conduct a successful fraud risk assessment (FRA). However, there are critical elements of a FRA that if not well-executed can render the exercise flawed at best and useless at worst. *Examples...*

- Not having the proper personnel involved in the process.** Most FRAs require the participation of at least the CFO, CIO, general counsel, business unit managers, a senior human resources manager, the accounting manager, chief internal auditor and representatives of the board and the audit committee. (See also page 3.)

- Limiting the FRA to risk factors**—such as motives, opportunities and incentives to commit fraud—while failing to identify the critical fraud schemes and scenarios that potentially threaten the organization.

- Failure to identify potential perpetrators.** This usually means insufficient consideration of management override of internal controls.

- Failure to assess the risk of collusion** between insiders and vendors, customers or other external parties.

- Failure to obtain management “buy-in.”** Without the unqualified support of the CEO, COO and other top executives, your FRA will not be taken seriously and may prove inadequate as a tool for strengthening the organization’s anti-fraud defenses.

White-Collar Crime Fighter source:

Jim Lombardo, CFE, Director in the Enterprise Risk Services practice, Deloitte & Touche LLP, and Mohammed Ahmed, CPA, Senior Manager, Deloitte Financial Advisory Service LLP’s Forensic & Dispute Services practice. www.deloitte.com.

period of “probation” monitored by the authorities, thereby avoiding the damaging fallout of a criminal conviction.

At worst, many companies that voluntarily disclose their financial misconduct will end up with sentences much lighter than what they would get had they chosen not to cooperate with prosecutors. That’s because the US Sentencing Guidelines recommend significantly lower penalties for organizations that meet some or all of the seven key compliance criteria of the Guidelines...


- Oversight by high-level personnel.
- Due care in delegating substantial discretionary authority for implementing and enforcing a compliance program.
- Effective communication to all levels of employees.

Cooperate fully with prosecutors. If an internal investigation reveals substantive evidence of wrongdoing, take prompt corrective measures and self-report the wrongdoing

Essential: For a compliance program to be recognized as effective, it must include periodic training of all employees at all levels within the organization regarding the responsibility of everyone to act ethically and lawfully at all times. These periodic educational programs must be designed to ensure that all employees understand what is legal and what is not.

- Substantive measures to achieve compliance, which include implementing systems for monitoring, auditing and internally reporting suspected wrongdoing without fear of reprisal.

Key: An anonymous hotline that employees can use to report criminal conduct without fear or reprisal.

- Consistent enforcement of compliance standards including disciplinary action.
- Meaningful steps to respond to and prevent further repeat offenses upon detection of a violation. 

White-Collar Crime Fighter source:

Judge William Wilkins, member and chair of the White-Collar Crime, Appellate Advocacy, and Corporate Compliance/Crisis Management practice groups at Nexsen, Pruet, LLC, a Columbia, SC-based law firm, www.nexsenpruet.com.

ROLES AND RESPONSIBILITIES

Nidhi Gupta, CPA, CFE, CIA, *BDO Consulting*

ELIMINATING THE CONFUSION

Defining the Roles of the Board, Audit Committee and Senior Management in Fraud Prevention



The public outrage and increased enforcement actions by regulatory and legislative bodies resulting from the mega-frauds at Enron, Tyco, Worldcom, HealthSouth and dozens of other multi-billion dollar companies has raised public expectations regarding the responsibilities of the board of directors, audit committee and senior management.

When an organization is in the news due to fraud, among the most frequently heard questions are, “Where was the board of directors?...Where was the audit committee?... where were the honest executives?”

DEFINING ROLES

Key lesson:

Some of these organizations may not have become household names had the roles of the board of directors, audit committee and senior management been clear with regard to identification, monitoring and response to fraud risks.

To reduce the confusion, listed below are a few best practices describing these critically important roles in the four key areas essential to an effective fraud prevention program...

- Tone at the Top
- Fraud Risk Assessment
- Fraud Prevention Controls
- Mechanisms for Reporting and Investigating Fraud

TONE AT THE TOP

The board of directors is responsible for establishing this tone by ensuring that it is in a position to exercise adequate oversight over senior management and the overall organization.

Example: If a majority of the board is comprised of owners, senior executives and/or parties related to these individuals, then the board has no independence and both Tone at the Top and board oversight responsibilities are severely compromised.

Important: As part of its oversight responsibilities, the board also must ensure that management implements policies that promote ethical behavior throughout the organization. To accomplish this, the board must

As part of its oversight responsibilities, the board must ensure that management promotes ethical behavior throughout the organization

review, help fine-tune and approve the corporate vision and mission statements, the company’s code of ethics and the communication process used to distribute this message throughout the organization as well as to vendors, customers and shareholders.

Example: Enron’s 65-page code of conduct was thorough and well-written but was by no stretch of the imagination an integral part of the organization’s culture. Had the Board been doing its job, it would have detected not only management’s lack of a company-wide communication system for ethics, but also management’s own egregious disregard for the code itself.

FRAUD RISK ASSESSMENT

The board also has responsibility to ensure that management designs effective fraud risk management procedures. Often, the board delegates this oversight responsibility to the audit committee.

Important: The board should detail these responsibilities in the audit committee’s charter as well as its own.

To ensure that appropriate steps are taken to identify and prioritize

Continued on pg. 4

Audits and Investigations Important Differences

As most readers know, conventional audits are not designed to detect fraud. They are designed to find errors and improper applications of accounting rules.

Problem: As the debate continues over how much responsibility auditors should have for detecting fraud, the question of where an audit which incorporates screening for evidence of fraud ends and a full-blown fraud investigation begins is fueling that debate.

Semantics: Fraud investigations are regularly referred to as “fraud audits” or “forensic audits”—which is one reason for the confusion. An audit is a specific type of service offered by accountants, while a fraud investigation is best described as a fraud examination or forensic accounting project.

Helpful: Audits tend to be based on routine plans—with the review of specific financial statement items, such as inventory test counts, being conducted in the same manner every time. And, while auditors are supposed to apply “professional skepticism” in evaluating potential evidence of identified risks of fraud, as prescribed in SAS 99, auditors often don’t exercise a high level of such skepticism during audits.

Auditors are essentially looking for documentation that supports the accounting entries, but aren’t usually trying to verify the authenticity of the documentation or to make a judgment as to whether the transactions under review are suspicious.

Contrast: While audits are based largely on standard work programs that outline areas of testing and examination, with auditors selecting a sample of transactions within their predetermined scope, there is *no* such standardized process during a fraud examination. Work is not done on a test basis, as it is with an audit. An

area of suspicion is isolated, and the fraud investigator typically examines *all* transactions within that area to find evidence of fraud.

MATERIALITY MATTERS

Auditors carefully consider whether an item or transaction would make a material difference in the eyes of the user of financial statements. Materiality is usually defined in terms of dollars, but also involves circumstantial considerations that a financial statement user might consider important.

Example: In a company with annual sales of \$10 billion, an improperly recorded sale of \$25,000 wouldn’t make a difference to someone reviewing the financial statements. The amount is simply too small to matter when compared with total sales of \$10 billion.

By contrast, a theft of \$25,000 at the same company that was committed by the CFO would be considered material by a fraud investigator.

Key: In the latter situation, the theft is definitely material because it was perpetrated by the top finance official in the company.

Bottom line: Materiality is not relied upon in fraud investigations to dismiss irregularities. *Any* fraud may be important to the organization—especially, as in the case above, it tips investigators off to other larger frauds.

The other major difference between audits and investigations relates to the opinions expressed. Audits are designed to give “negative assurance”: The auditors are not aware of anything that would make the financial statements incorrect.

Contrast: Fraud examinations give positive assurance—we found X,Y, and Z incidents of fraud during our examination and here is the evidence. 🚫

White-Collar Crime Fighter source:

Tracy Coenen, CPA, CFE, Sequence Inc., Chicago-based fraud investigation and forensic accounting consultants, www.sequence-inc.com. This article is based in part on Tracy’s soon-to-be-published book, *Expert Fraud Investigations: A Step-By-Step Guide* (Wiley).

Continued from page 3

the fraud risks for an organization, the audit committee should...

- Ensure that management assigns the responsibility of fraud risk assessment and management of identified risks to a qualified individual. Though many individuals within the organization must be involved in the fraud risk assessment, many organizations undermine their fraud risk assessment processes by failing to put someone in charge of coordinating the process and reporting to the audit committee. Often, a senior member of the organization’s internal audit (I/A) department is best qualified to take on this role.

- Evaluate the fraud risk assessment process and methodology implemented by management. Audit committee members must understand and question management on the methods used to conduct a fraud risk assessment.

Effective: Because there is no standard for conducting a fraud risk assessment, the methodology and documentation of the risk assessment process must be tailored to the organization’s size, complexity, industry and goals. Internal audit’s familiarity with these factors again often proves valuable in determining if management’s assessment methodology is effective.

Aim: To ensure that the organization’s fraud risks are properly prioritized by using an effective ranking system.

FRAUD PREVENTION CONTROLS

There is general consensus among anti-fraud experts that management has the responsibility to reduce the risk of fraud in response to the findings of the fraud risk assessment.

Specifically, management must design, implement and maintain an adequate anti-fraud internal controls system. *These controls can include:*

- Appropriate segregation of duties.
- Fraud awareness training for employees so that they can detect the red flags of fraud and blow the whistle (see below).
- Background checks on new hires, vendors, customers and existing employees being promoted to significant levels of authority.

Important: The audit committee is responsible for reviewing management reports on the effectiveness of fraud prevention controls. To verify the accuracy of these reports, the audit committee should use the external and internal auditors to assess the effectiveness of the fraud prevention controls established by

Continued on page 5

Continued from page 4

management.

REPORTING MECHANISMS

No system of internal control can provide absolute assurance against fraud. Therefore, organizations must establish mechanisms that employees, vendors, and/or customers can use to confidentially report on suspected fraud issues.

Management is responsible for establishing and developing:


- Reporting mechanisms such as a confidential hotline.
- Policies that protect whistleblowers against retaliation.
- A process for prompt review, investigation and resolution of reported fraud allegations.
- A case management system to track complaints reported and facilitate management of the resolution process.

The audit committee is responsible for reviewing and approving this process as well as that for ensuring that fraud-related complaints are disseminated to appropriate parties.

Details: To confirm that fraud-related complaints are addressed and brought to the attention of management and the audit committee, they should be distributed to several parties within the organization such as internal audit, legal, security, human resources—so that no one individual or functional area receives and controls this information (and thereby has the power to “overlook” or “bury” complaints it is the target of).

Finally, but by no means least important, the responsibility for investigating allegations of fraud should be shared between the audit committee and management.

Specifics: Management is responsible for overseeing the investigation and resolution of the majority of fraud complaints. To ensure the integrity of the investigation, the responsibility for overseeing an investigation should be given to an individual with a level of authority at least one level higher than anyone potentially involved in the incident.

Exception: If an allegation involves a member of senior management, the responsibility of overseeing the independent investigation of the complaint shifts to the audit committee. 

White-Collar Crime Fighter source:

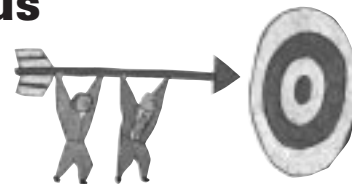
Nidhi Gupta, CPA, CFE, CIA, CAMS, Director, BDO Consulting, a division of BDO Seidman, LLP. Nidhi can be reached at NGupta@bdo.com.

CARD CRIME CRISIS

Tom Mahoney, *Merchant 911*

The State of Credit Card Fraud

Time to Get Serious About Controls



Reports by the Association for Payment Clearing Services (APACS), the umbrella body for the UK payments industry, indicate that Chip and PIN technology has reduced Card Present (CP) fraud in countries where it is deployed by 35% since its introduction in 2005.

Chip and PIN technology (also known as Smart Cards) combines an embedded microchip requiring a manually entered PIN.

Problem: Chip and PIN didn't convince fraudsters to “go straight.” It just pushed them to countries where Chip and PIN isn't in use and to the Card Not Present (CNP) world of E-commerce. Now APACS is reporting a 190% increase in overseas CNP fraud in the same period.

By 2010, Chip and PIN will be ubiquitous in Europe. We can only imagine what that will do to CNP fraud rates. Canada has completed a market test of the technology and will be rolling it out nationwide over the next few years. However the U.S. card companies have no plans to change.

Result: The U.S. will therefore become a prime target for CNP fraudsters in the Internet's global economy because it will be one of the few countries without Chip and PIN.

SOURCES OF FRAUD

While we haven't seen a credit or debit card-related breach as large as the TJX fiasco of 2007 in which some 94 million credit card records were stolen by cyber-thieves, there are indications that 2008 hasn't escaped unscathed. In fact, data loss reports are up almost 70% this year, and there is a

marked rise in ATM hacks. (The most devastating breach of 2008 was the Hannaford Brothers attack in March which compromised 4.2 million accounts.)

The Hannaford breach was especially disturbing in that credit and debit card information was collected from the POS terminals instead of from secured databases. Hannaford was considered compliant with security rules but the bad guys still penetrated the company's security systems.

The US will become a prime target for CNP fraudsters in the Internet's global economy

Important lesson for issuers, merchants and cardholders: The

fraudsters are getting more sophisticated and too many companies are still as careless as ever about handling Personal Identifying Information (PII).

Even more distressing is the number of reports of lost backup tapes, missing disk drives and other improper handling of well over 30 million records related to credit cards, debit cards or PII.

Examples: Medical Mutual of Ohio lost a disk drive with the personal information of 36,000 people...the City of Indianapolis posted Social Security numbers, names and dates of birth of about 3,300 on a public Web site...and Blue Cross and BlueShield of Georgia sent 202,000 medical records to the wrong address.

These are just a few of the organizations that have suffered the consequences of poor data handling. Any of this data could end up in the wrong hands (if it hasn't already) and be used for identity theft and credit card fraud.

Important: These incidents could have been prevented by nothing

Continued on page 6

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE



A “Perfect Storm” for Fraud

If anyone had any doubts before this September that economic downturns foment fraud, the deluge of reports and quotes by experts sounding this warning should by now have convinced even the staunchest doubters that financial crime will only get worse in coming months.

In one of the more compelling assessments of the current crisis, one seasoned forensic accountant described the current economic climate as “a perfect storm” of forces combining to create a surge in fraud.

Specifics: With increased pressure to sustain profitability in today’s economic slowdown, motivation for management at the unit, division and even corporate level to make the numbers look as positive as possible is extremely strong.

Add to that the probability that rank-and-file employees, worried about job security and the diminished value of their retirement savings, will seek to enrich themselves at the company’s expense by stealing cash or merchandise and you’ve got a recipe for a potentially costly epidemic of internal fraud.

Self-defense: Review and if necessary “harden” your policies and procedures to prevent, detect and deter fraud and other inappropriate behavior. Meet with the individuals responsible for internal control over financial reporting, human resources, compliance and other key risk areas and ask the following questions:

- 1) In terms of fraud risk, what keeps you awake at night?
- 2) If someone wanted to misappropriate assets or misstate the financial results of the company, how do you think they would do it?
- 3) In what ways are our internal controls failing to prevent, deter and detect fraud?

Listen to their responses and then go back to your control assessment and risk management documents and look for weaknesses, control gaps and repeatedly ask yourself, “Have we done everything we can to batten down the hatches?”

White-Collar Crime Fighter source: David S. Zweighaft, CPA, CFE, principal of New York City-based DSZ Forensic Accounting & Consulting Services, <http://www.DSZForensic.com>, quoted by *Checkpoint*, a news and research service of Thomson Reuters, www.thomsonreuters.com.

Cyber-Criminals Growing More Aggressive

Cyber-criminals are reducing the time it takes to launch computer attacks that take advantage of publicly disclosed security holes. According to IBM’s latest *Internet Security Systems XForce* report, there are two growing trends in Internet threats...

- On-line criminals’ use of programs that help them automatically generate attacks based on publicly available information about vulnerabilities. In the past they spent more time finding those security holes themselves. Now finding them is no longer required...it occurs automatically.

- Quicker and increasingly detailed release by security researchers of information relating to newly discovered software flaws.

Details: Though researchers have typically waited until the affected company has released a software patch before revealing details, increasingly they are releasing not only details of the vulnerability but also “proof-of-concept” exploit code to show the flaw is legitimate.

Problem: This gives criminals a framework for creating new cyber-attacks.

Example: In Web browsers, hacking exploits are now available within one day after flaws are discovered 94% of the time—up from 79% in 2007.

White-Collar Crime Fighter source: *IBM Internet Security Systems Xforce Report*, cited in *The Cyber Crime Newsletter*, a bi-monthly publication developed under the Cyber Crime Training Partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi School of Law. The newsletter is written and edited by Hedda Litwin, Cyber Crime Counsel. She can be reached at hlitwin@naag.org.

Continued from page 5—
more than diligent tracking of data.

AND IT GETS WORSE

The faltering global economy is now pushing more and more people to commit credit card fraud that they wouldn’t have thought about as recently as a year ago. They see it as a matter of survival.

As sub-prime mortgages continue to go south and the government pumps out boatloads of taxpayer money to prevent further bank failures, lending standards for consumer credit have been sharply tightened.

Prediction: Identity theft and opening of fraudulent accounts will become more difficult to perpetrate, inducing fraudsters to step up their attacks on existing credit and debit card accounts.

WHAT CAN BE DONE?

In the short term, extra vigilance is the best answer for all parties—merchants, issuers, processors and cardholders. This holiday season could produce some of the highest fraud rates on record which, combined with the anticipated weakness in sales, could be devastating for merchants as well as issuers.

Self-defense: All organizations involved in financial transactions should take whatever steps are necessary to protect themselves and their customers against fraudulent chargebacks, theft of credit and debit cards, employee card fraud and skimming, on-line CNP fraud, etc.

Additional anti-fraud steps to take now...

- Make every effort to assure complete PCI compliance.** If some good came from the Hannaford event, it was the release by card companies of PCI-DSS version 1.2 that went into effect on October 1.

- Upgrade from the older wireless encryption standard known as Wired Equivalent Privacy (WEP).** PCI Security Standards require merchants to have eliminated it by June 2010 anyway.

- E-commerce merchants should review their manual fraud screening procedures to make sure they are doing everything they can to weed out fraud.** That could require investing in more fraud screening technology like


Continued on page 7

Continued from page 6

Payer Authentication, IP-Geolocation and neural networks.

•**Brick and mortar merchants must do a better job of educating employees about fraud prevention.** Make sure that employees know how to spot counterfeit cards and know the procedures to follow if one is presented. They should also understand that “See ID” is not a valid signature and they must not accept the invalid card. Recent reports of fraudsters slicing the numbers off of expired cards and then carefully gluing them on to another card in the sequence of a legitimate account number either stolen, purchased on the black market or otherwise obtained, describe a scam known as “shaving.” This indicates that there are many inept cashiers handling retail transactions. These poorly counterfeited cards require manual keying and can easily be caught by any employee with little more than five minutes of training.

COMING SOON...

The credit card companies are working on some solutions, their latest offering being a display and keyboard built into the credit card to generate one-time passcodes. That’s taking place in Australia now but don’t look for it in the U.S. anytime soon, especially since the cost is keeping Chip and PIN away. 

White-Collar Crime Fighter source:

Tom Mahoney, founder and director of Merchant 911.org, a leading Internet information exchange for E-merchants seeking to prevent on-line fraud against themselves and their customers, www.merchant911.org.

Card Fraud: The Foreign Threat

Credit card fraud perpetrated by overseas criminals is becoming increasingly sophisticated. A recent article in the *UK Times Online*, citing information from British police and US counterintelligence sources, reported that Chip and PIN readers located throughout Europe had been rigged with sophisticated electronic devices that prompted the readers to record MasterCard numbers and PINs and wirelessly “phone” the data to a known Al-Qaeda group in Pakistan.

Caution: The global nature of credit card commerce means US issuers, merchants and processors are potential targets of high-tech fraud.



THE CON'S LATEST PLOY...

From *White-Collar Crime Fighter's* files of new scam, scheme and scandal reports

New York, NY

Round-tripping in the Big Apple gets wormy. The former chiefs of New York City’s largest retail drug store chain, Duane Reade, finally got hauled before the judicial system to account for their alleged web of decidedly sleazy real estate-related round-tripping deals that resulted in more than \$13 million of fraudulently inflated income.

Background: In New York City, where Duane Reade had more than 200 retail stores in the late 1990s, it was not uncommon for landlords to offer early termination buyouts of existing retail store leases in order to rent the space to new tenants at higher rates. Duane Reade accepted several of these legitimate so-called “real estate concession” deals.

But then Anthony Cuti, Duane Reade’s former CEO and the appropriately named William Tennant, the company’s former Real Estate Administrator and CFO, got greedy. Now they are charged by the SEC with numerous frauds involving phony transfers of retail leases to shell company landlords in exchange for payments used to doctor the company’s books before being returned to shell company “principals.”

Details: In most of their “deals,” Cuti and Tennant relied on a single real estate broker to negotiate its leases.

Working with Tennant, the broker ultimately came to serve as Duane Reade’s real estate department—conducting most of the company’s real estate-related administrative functions, including maintaining and updating a list of Duane Reade’s real estate holdings, and its rights and obligations with respect to those holdings, and negotiating with landlords for over 90% of the company’s real estate transactions.

Key detail: The principals of the brokerage firm were included in most of the real estate-related decision-mak-

ing at the company. At Cuti’s invitation, the principals attended weekly meetings with Duane Reade management to discuss Duane Reade’s real estate holdings, expiring leases, planned store openings and related issues.

At the end of many of the regular weekly real estate meetings, Cuti held a second meeting with just Tennant and the principals. At these sessions, Cuti typically discussed the real estate concession transactions—known to the principals as “the Cuti deals.”

Strong-arming in the face of poor performance: When Cuti first approached the principals in 2000 and told them that he wanted them to pay Duane Reade for an option to purchase certain real estate rights, the principals objected, and told Cuti that the option had no value.

The stick: Cuti replied that if they did not do the deal and pay Duane Reade, he would find another brokerage firm that would.

The carrot: Cuti committed to repay the principals through separate transactions, and promised that they would break even on the real estate concession transactions.

Based on these promises, and because Duane Reade represented the majority of the broker’s business, the principals agreed to participate in the Cuti deals.

Details: At Cuti’s suggestion, the principals set up two shell companies—“Shell A” and “Shell B”—to act as counterparties on Duane Reade’s real estate concession contracts. From December 2000 through July 2004, Cuti structured and Tennant implemented at least 13 sham real estate concession transactions between Duane Reade and the principals through their shell companies.

The transactions were typically concluded at the end of a quarter, or

after the end of the quarter and back-dated.

Despite their lack of any financial value, Cuti and Tennant structured the transactions so that the payments would appear to be legitimate concession payments, and Cuti and Tennant convinced Duane Reade management and its auditors that the payments should therefore be recognized as current income.

Key: To complete the fraud, and to minimize the impact of the repayments on current income, they disguised the repayments—paid to the principals through the shell companies or the broker—as “compensation for brokerage services” or for amounts that were deliberately inflated. Disguising the repayments as payments for legitimate brokerage services enabled the company to capitalize and amortize those payments over the life of other, unrelated leases.

Cuti and Tennant are alleged to have not only approved the repayments, but also to have dictated the structure of the payback transactions, including the amounts of the payments, and the properties to which the bogus invoiced services supposedly related.

Indianapolis, IN

Cyber-extortion attempt ends in failure thanks to new federal law and multi-agency investigation.

Kevin Michael Stewart was arrested by the FBI Cyber Crime Task Force and

the Safe Streets Task Force in Indianapolis on charges arising from the March 31, 2006, burglary of a computer server from the Indianapolis office of Medical Excess LLC, a subsidiary of the financially beleaguered insurer AIG.

Details: The server contained personally identifying and sensitive health care information for more than 900,000 policyholders. Stewart is also accused of extorting AIG for \$208,000 under a threat to release the data onto the Internet.

Important: According to Assistant U.S. Attorney Steven DeBrot, Stewart is the first person in the United States to be charged under a new criminal statute designed to address the theft of large amounts of electronic data from organizations.

Specifics: A criminal complaint was filed with the U.S. District Court for the Southern District of Indiana alleging violations of the extortion statute, Title 18, U.S.C. § 875 and the newly enacted Title 18 U.S.C. § 1030(a)(7)(B) and (C), which make it a federal crime to “commit extortion relating to unauthorized access of, or damage to, a protected computer system and/or to impair the confidentiality of information obtained from a protected computer.”

The case was initiated when AIG reported the theft to the FBI. The insurer cooperated closely with the FBI Cyber Crime Task Force to solve the

burglary and prevent the disclosure of sensitive customer information.

Background: The FBI Cyber Crime Task Force is a multi-agency unit with members in the FBI Indianapolis Field Office, Merrillville Resident Agency and Evansville Resident Agency. It is responsible for investigating high-technology crime and neutralizing national security threats involving computer networks.

Agencies participating in the task force include the Evansville Police Department, FBI, the Indiana Attorney General’s office, Indiana Department of Natural Resources, Indiana State Police, Indianapolis Metropolitan Police Department, United States Secret Service and the Vanderburgh County Sheriff’s Office. Purdue University’s Center for Education and Research in Information Assurance and Security (CERIAS) and Department of Computer and Information Technology’s Cyber Forensics Lab are special partners in the task force.

Hard Drive Data Danger

Hard drives of PCs being discarded often contain huge amounts of confidential data that can be used for commercial sabotage, identity theft and political compromise.

Survey findings: The percentage of disks that have been effectively wiped fell from 45% to 33%, since last year’s survey.

Urgent: Better education to teach that simply deleting a file from the hard disk does not actually remove it from the computer. To remove all traces of a file requires the actual data to be wiped using “digital shredding” software.

White-Collar Crime Fighter source: Survey by Andrew Jones, Head of Information Security Research at British Telecommunications in Martlesham Heath, UK...Glenn Dardick of Longwood University, Farmville, VA...Craig Valli of Edith Cowan University, Western Australia...and Iain Sutherland, University of Glamorgan, UK, cited at *Science Daily*, www.sciencedaily.com/.

COMING SOON IN

White-Collar Crime Fighter...

- New legal standards for internal investigations
- Update on fraud in the financial crisis
- Protecting against the growing threat of industrial espionage
- Secrets of successful forensic data-mining



YES! I want to save \$50 on a one-year subscription to **WHITE-COLLAR CRIME FIGHTER!** By subscribing now, I’ll get the money-saving introductory subscription rate of \$245. **That’s \$50 off the regular subscription price of \$295!** **Plus,** send me—for **FREE**—**THREE** Special Reports on how to prevent, detect and investigate fraud threatening MY organization.

Payment enclosed (or) Charge my Visa Mastercard AMEX Discover Bill me

Card # _____ Expiration date _____

Signature _____

Name _____

Affiliation _____

Address _____

City _____ State _____ Zip _____

Call 1-800-440-2261...Or Fax this order form to: 203-431-6054
Or subscribe on-line at www.wccfighter.com.

Or mail this form and your check to: White-Collar Crime Fighter, 213 Ramapoo Rd., Ridgefield, CT 06877. You can contact White-Collar Crime Fighter by E-Mail: subscribe@wccfighter.com