# WHITE-COLLAR CRIME FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

VOLUME 12 NO. 4
APRIL 2010


## IN THE NEWS

### Disturbing Data on Mortgage Fraud

Total mortgage fraud rose by 7% in 2009 compared with 2008, despite the bottoming out of housing prices subsequent to the market's crash.

***Key details:*** In 2009, 18% of loans reported to the Mortgage Asset Research Institute (MARI) contained fraudulently inflated property values of less than 15% compared with 15% in 2008. Meanwhile, loans with inflated appraisal values of 15% to 30% rose from 39% to 40% between 2008 and 2009.

***Disturbing:*** Despite mortgage fraud's well-documented prominence among drivers of the financial crisis, the much-anticipated economic recovery of late 2009 was not accompanied by a decline in mortgage-related crime.

MARI attributes some of the continued pervasiveness of mortgage fraud to new technologies that enable criminals to gain access to confidential information necessary for falsifying loan-related documents.

Other causes may include enhanced desperation on the part of owners to sell homes they could no longer afford as well as the rapid spread of foreclosure schemes.

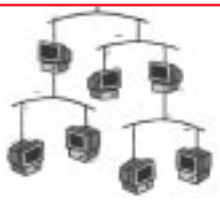
***White-Collar Crime Fighter*** **source:** *Twelfth Periodic Mortgage Fraud Case Report,* Mortgage Asset Research Institute, a unit of Lexis-Nexis. It is available at http://solutions.lexisnexis.com/forms/MortgageFraudCaseReport12?source=RD_fraudreport

## IN THIS ISSUE




Stephen M. Plotnick, Esq., *Stern & Kilcullen LLC*


# New Anti-Fraud Approach from SEC



In an apparent attempt to redeem itself following the embarrassing events surrounding the Bernard Madoff Ponzi scheme and more recently, criticism of its oversight of unusual securities transactions by Lehman Brothers prior to its demise, the Securities and Exchange Commission (SEC) is implementing new "weapons" in its arsenal for fighting corporate fraud.

Specifically, the Commission's newly announced Enforcement Policy Initiative contains details of incentives it plans to offer prospective fraudsters whose assistance in conducting corporate fraud investigation would substantially enhance the Commission's investigative efficiency and effectiveness.

**The Securities and Exchange Commission (SEC) is implementing new "weapons" in the arsenal for fighting corporate fraud**

***Specifics:*** In the Initiative's *Policy Statement Concerning Cooperation by Individuals in its Investigations and Related Enforcement Actions,* the SEC states that "Cooperation by individuals and entities in the Commission's investigations and related enforcement actions …can enhance the Commission's ability to detect violations of the federal securities laws, increase the effectiveness and efficiency of the Commission's investigations, and provide important evidence for the Commission's enforcement actions. There is a wide spectrum of tools available to the Commission and its staff for facilitating and rewarding cooperation by individuals, ranging from taking no enforcement action to pursuing reduced charges and sanctions in connection with enforcement actions."

#### RELIEVING TENSION

The "tools" to which the Policy Statement refers is a set of measures designed to ease the opposing forces of feeling pressed to go full force after every "bad guy" on the one hand, and seeking the cooperation of guilty parties to expedite the agency's law enforcement objectives on the other.

*Thus, the SEC will now offer civil counterparts to the Department of Justice's prosecutorial tools of...*

•**Cooperation agreements.** Here, the Division of Enforcement would agree to recommend to the Commission that an individual believed to be party to a corporate fraud be awarded "credit" n exchange for cooperating with an investigation by providing valuable information or testimony.

•**Deferred prosecution agreements.** These are "deals" between the enforcement body and a prospective cooperative party in which enforcement action is suspended if the individual agrees to cooperate fully and truthfully and to comply with specific prohibitions and actions during the period of deferred prosecution. It does not necessarily mean the cooperating party will never be pursued civilly by the SEC, but it does give the individual the chance to receive leniency from enforcement offi-

cials by assisting them with fraud investigations…and by adhering to strict rules and restrictions during the period of deferment.

•**Non-prosecution agreements.** These are what might be considered civil "get-out-of-jail-free" cards for individuals who committed or conspired to commit fraud. Under these arrangements, the Commission would agree not to pursue an enforcement action if the individual agrees to cooperate fully and truthfully.

In these cases, though, the information that the SEC obtains from such individuals must be very useful, and the chances of obtaining a non-prosecution agreement are expected to be greatest if the individual has decided to, or is planning to enter into a plea agreement with criminal prosecutors in connection with the case under investigation.

•**Streamlined immunity processing.** As part of the Initiative, the SEC has also eliminated some of the cumbersome red tape involved with obtaining immunity from the Department of Justice for witnesses the Enforcement Division deems to be potentially helpful in investigations.

***Key advantage:*** From the perspective of pursuing and forcing corporate fraudsters to "pay their dues" for violating federal securities laws, the SEC's use of these cooperation agreements will give potential cooperators a clear idea of what their fate will be should they decide to cooperate with the Commission.

Prior to this, there was little or no incentive for fraudsters or co-conspirators to help the SEC because there was no guarantee that the full force of the Commission's enforcement arsenal wouldn't be turned against them after volunteering their assistance.

***Potential problem:*** While the SEC's offers of enforcement leniency may be very successful in persuading more guilty parties to come forward with information that expedites investigations, there remains the uncertainty as to whether the Department of Justice will take a cue from the Commission and afford individuals the same incentives on the criminal side. It thus remains to be seen if the SEC can coordinate its new Initiative with DOJ to prevent such uncertainty about potential criminal prosecution from deterring prospective cooperators from accepting SEC leniency in exchange for their assistance in the Commission's civil investigations.

**There is a wide spectrum of tools available to the Commission and its staff for facilitating and rewarding cooperation by individuals**

## SPECIALIZED UNITS

The second key part of the Commission's Initiative is establishment of five new specialized enforcement units each of which will, according to SEC Enforcement Division Director, Robert Khuzami, "use enhanced training, hiring of and consultation with individuals with industry experience or specialized skills, targeted investigative approaches and… new technology, to conduct more efficient and comprehensive investigations."

*The five new units are…*

•**Asset Management Unit,** which will concentrate on investment firms, mutual funds, hedge funds and private equity funds.

•**Market Abuse Unit,** which will focus on large-scale and organized insider trading and financial market manipulation cases.

•**Structured and New Products Unit** will handle the types of structured securities instruments, also known as derivatives, that were central to the financial meltdown of 2007-2008 and which are at the heart of the Commission's controversial civil fraud case against Goldman Sachs. These include credit default swaps (CDS), collateralized debt obligations (CDO) and other complex securitized instruments and new financial products.

•**Foreign Corrupt Practices Unit,** which will cover investigations of corporate bribery of foreign officials

•**Municipal Securities and Public**



WHITE-COLLAR CRIME FIGHTER

*Editor*
Peter Goldmann. MSc, CFE
*Consulting Editor*
Jane Y. Kusic
*Managing Editor*
Juliann Lutinski
*Senior Contributing Editor*
David Simpson
*Associate Editor*
Barbara Wohler
*Design & Art Direction*
Ray Holland, Holland Design & Publishing



*White-Collar Crime Fighter* (ISSN 1523-0821) is published monthly by White-Collar Crime 101, LLC, 213 Ramapoo Rd., Ridgefield, CT 06877. www.wccfighter.com. Subscription cost: $295/yr. Canada, $345. 

## 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 edi tor@wccfighter.com. Visit us on the Internet at www.wccfighter.com.

**Pension Unit,** which, as the name suggests, will specialize in fraudulent activity in the municipal securities market and in public pension funds.

### PREDICTION

Establishment of the specialized enforcement units parallels the apparent effort by the SEC in introducing the new cooperation tools to move away from a "generalist" enforcement agency bent on pursuing every financial criminal in its jurisdiction with every weapon in its arsenal, to one with more efficient investigative processes and targeted enforcement focus enabling it to more quickly identify potential violations in complex areas of the securities laws and capital markets.

These policy changes could result in a significant improvement of the Commission's enforcement operations through more prompt and cooperative response by individuals and corporations to allegations of civil fraud.

***White-Collar Crime Fighter* source:**
Stephen M. Plotnick, Esq., partner in the litigation department of Stern & Kilcullen LLC, New York. Steve can be reached at splotnick@sgklaw.com.



**GLOBAL CORRUPTION UPDATE**

# OVERSEAS BRIBERY

## Latest Mega-Case and New International Preventative Guidance

"In February 1999, Germany outlawed foreign bribery when the Organization for Economic Cooperation and Development ("OECD") Anti-Bribery Convention, which Germany ratified, entered into force. Daimler, however, had been prohibited from making bribes to foreign government officials under the FCPA since 1993 when its predecessor, Daimler-Benz AG, registered a class of securities under…the [1934 Securities] Exchange Act."

Thus reads a passage from the Securities and Exchange Commission's (SEC) complaint in the latest mega-violation of the Foreign Corrupt Practices Act (FCPA).

According to the SEC complaint, the alleged Daimler violation involved paying $54 million in bribes between 1998 and 2008 through over 150 individual transactions. Countries whose government officials profited from this alleged illegal activity include China, Nigeria, Russia, Egypt, Greece and even North Korea.

Moreover, the SEC charges Daimler with paying more than $6 million to Iraqi officials between 2001 and 2003 to obtain business under the Iraqi Oil-for-Food Program.

A large number of slush funds were allegedly used by numerous Daimler subsidiaries to execute the bribery transactions, according to the SEC. Weak internal controls at the company contributed to the alleged widespread practices that are expressly forbidden not only by the FCPA but also by the OECD Convention On Combating Bribery Of Foreign Public Officials In International Business, signed by 38 countries including Germany and the US.

***Critical lesson:*** This is one of several recent attempts by the SEC to coordinate its stepped-up enforcement of US anti-corruption law with comparable international efforts.

### NEW INITIATIVES

***Latest international anti-bribery initiative:*** A new set of guidelines for deterring and detecting bribery of foreign government officials released by the OECD's Working Group on Bribery in International Business Transactions.

In the light of the new aggressiveness on the part of the US Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) in enforcing the Foreign Corrupt Practices Act (FCPA), the document may prove valuable as a roadmap for implementing policies and measures that can reduce your organization's risk of finding itself in the crosshairs of the two federal anti-bribery enforcement agencies. US experts in overseas bribery matters say that American companies with existing or prospective overseas operations are well-advised to familiarize themselves with and to adhere to the new guidelines.

What the OECD entitles "The Good Practice Guidance" is addressed to companies for formulating and enforcing effective internal controls, ethics and compliance programs for preventing and detecting bribery of foreign public officials in their international business transactions.

***Key finding:*** To be effective, anti-bribery measures must be interconnected with a company's overall compliance framework.

***Essential:*** According to the new Guidance, anti-bribery controls, ethics, and compliance programs or measures

*Continued on pg. 4*

FRAUD PERSONALITY

# The Psychology of Executive-Level Fraud

A new study of the psychology of how executives transform from honest leaders to high-level fraudsters was recently published by three Canadian researchers. Their theory is that there are three overriding psychological or emotional motivators that lead top executives to cross the line to serious fraudulent activity:

***Motivator #1:*** **Personality and life circumstance.** These executives are often achievement-oriented, focusing on outcome over process and see their power as strong enough to influence others whose cooperation is required to execute fraud.

***Common psychological motivation:*** Poor self image. The person will go to any lengths to see himself or have others see him favorably. Depending on the level of pathology, the person develops a sense of superiority that ranges from "acting" or "putting on a show" in which he compensates for weakness, to narcissistic illusions such as in "I am king of the world."

These individuals will do anything—including committing fraud—to compensate for their negative opinion of themselves.

***Example:*** Rogue trader Nick Leeson who nearly brought down Barings Bank, was inexperienced and in fact incompetent as a trader. Yet his drive to prove his self-worth drove him to commit massive securities frauds.

***Motivator #2:*** **Emotional need to support another perpetrator.** These fraudsters are called "drivers." They work for the organization in positions of power, but turn a blind eye — condoning or supporting illegal actions by a corrupt superior.

Typically drivers are outcome-oriented, rather than process-oriented. They distance themselves from the specific actions of the perpetrator by not asking questions, but are supportive of the perpetrator's activities.

***Example:*** At Enron, COO Jeffrey Skilling was one of the alleged perpetrators. It was Skilling's drive and vision, in conjunction with CFO Andy Fastow (another perpetrator), that took Enron to its heights and eventual depths.

The driver was CEO Ken Lay who was aware of what was happening but was not a participant in designing the financial frauds that brought Enron down. However, he directly benefited through share value from the activities of Skilling and Fastow.

**There are overriding psychological or emotional motivators that lead top executives to cross the line to serious fraudulent activity**

***Key:*** Drivers do not mastermind unethical activities. Slowly they become aware of these activities, recognizing that their success is so closely linked to the success of the perpetrator's actions that it is in their best interest not to ask questions.

***Motivator #3:*** **The art of manipulation.** This is demonstrated in a need and ability to surround oneself with employees too new at a job to raise questions, appear malleable or are organizational conformists.

***Example:*** Former Hollinger International CEO, Conrad Black. He carefully selected a board whose approval of anything he wished to do was essentially automatic.

The corrupt leader may attract followers who have particular psychological make-ups, such as low self-esteem, or circumstances that lead them to be more vulnerable.

There may be employee indebtedness to the leader for giving them a job and a "chance of a lifetime, and letting them keep their job,"which they believe they really do not deserve. They may lack the skills for the job but they are loyal and certain never to blow the whistle.

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

*A 12-Step Process of White-Collar Crime,* by Ruth McKay, an Associate Professor at Carleton University's Sprott School of Business …Cary Stevens, PhD, Ottawa, Canada-based clinical psychologist and business consultant…and Jae Fratzl, MA,ATR, Registered Art Therapist with the American Art Therapy Association, and a Professional Member of the Canadian Art Therapy Association, published in *International Journal of Business Governance and Ethics,* Inderscience Publishers, Olney, UK, www.inderscience.com.

*Continued from page 3*

should be developed on the basis of a risk assessment addressing the individual circumstances of a company, in particular the foreign bribery risks facing the company such as the geographical and industrial sector of its operations. These circumstances and risks should be regularly monitored, re-assessed and adapted as necessary to ensure the continuous effectiveness of the company's anti-bribery controls.

*Additional anti-bribery policy and program essentials...*

•**Clear and visible corporate policy prohibiting foreign bribery.** There should be no opportunity for violators to deny having knowledge of the anti-bribery policies of the organization.

•**Strong, explicit and visible support and commitment from top management** to the company's anti-bribery internal controls, ethics and compliance programs or measures. This is an obvious derivation of Tone at the Top, so commonly cited in the US as a critical element of any corporate anti-fraud initiative and policies.

•**Enforcement of enterprise-wide compliance with anti-bribery rules** and related internal controls, ethics, and compliance policies as the duty of individuals at all levels of the company.

•**Oversight of ethics and compliance policies and programs regarding foreign bribery.** Oversight should be the duty of one or more senior corporate officers, with an adequate level of autonomy from management, resources and authority.

***Essential:*** All employees must have the authority to report violations of anti-bribery rules directly to an independent monitoring body such as internal audit committees of boards of directors or of supervisory boards.

•**Ethics and compliance programs or measures designed to prevent and detect foreign bribery must be applicable to all directors, officers and employees,** and to all entities over which a company has effective control, including subsidiaries. *Measures should detail anti-bribery policies pertaining to payment for...*

☐ Gifts, Hospitality, entertainment and expenses

☐ Customer travel

☐ Political contributions

*Continued from page 4*

☐ Charitable donations, sponsorships

☐ Facilitation payments

☐ Solicitation and extortion.

•**Third-party anti-bribery policies.** Companies must enforce rules designed to prevent and detect foreign bribery applicable to third parties such as agents and other intermediaries, consultants, representatives, distributors, contractors and suppliers, consortia and joint venture partners. *Essential elements...*

☐ Fully documented risk-based due diligence pertaining directly to the hiring and regular oversight of business partners.

**American companies with existing or prospective oversees operations are well-advised to familiarize themselves with and to adhere to the new guidelines**

☐ Insistence on reciprocal commitment from business partners.

•**System of financial and accounting procedures,** including a system of internal controls to ensure the maintenance of accurate books, records and accounts, and to ensure that they cannot be abused for the purpose of foreign bribery or hiding such bribery.

•**Periodic training for all levels** of the company on the organization's ethics and compliance program including measures regarding foreign bribery.

•**Disciplinary procedures to address violations** at all levels of the company, of laws against foreign bribery.

•**A system for confidential reporting of violations of anti-bribery laws.** The system should legally protect all employees, and business partners who are not willing to violate professional standards or ethics under instructions or pressure from their superiors.

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

•Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in *International Business Transactions, Annex II: Good Practice Guidance on Internal Controls, Ethics, and Compliance,* issued by the Working Group on Bribery in International Business Transactions, OECD, www.oecd.org/document/5/0,3343,en_2649_34859_35430021_1_1_1_1,00.html.

•*United States Securities and Exchange Commission v. Daimler AG,* case number 1:10-cv-00473, United States District Court for the District of Columbia.

**CYBER-CRIME FIGHTER**

# CYBER-SECURITY
## A Six-Step Plan for Self-Defense

On May 29, 2009, the Federal government issued a report stating that, between 2008 and 2009 American businesses lost $1 trillion worth of intellectual property due to cyber attacks. *This staggering number does not include the cyber-related losses due to:*

•Theft of personally identifiable information (PII).

•System inefficiency and downtime.

•Loss of customers.

•Negative impacts on share values (which, research has shown, follow publicity of cyber incidents).

Unfortunately, the problem is continuing to grow. Moreover, research by PricewaterhouseCoopers reveals that approximately one-half of all organizations are reducing or deferring budgets for improved information security.

### IT'S NOT MY JOB

***Danger:*** The common misconception that "the IT guys can handle the problem" causes employees to feel that they are not responsible for the security of their own data. But even the best IT team in the world cannot mitigate risk of an information security breach without the support of employees throughout the organization.

***Challenge:*** Cost is the biggest obstacle to optimal organization-wide information security. With top management's often inadequate appreciation of the cyber-crime threat, it is difficult for IT managers to obtain the funds to implement defenses and communicate best practices to employees.

***Important:*** Cyber-security is an enterprise-wide risk management issue that needs to be addressed from a strategic, cross-departmental and economic perspective. The chief financial officer (CFO), as opposed to the chief information officer (CIO) or the chief security officer (CSO), is the most logical person to lead this effort.

***Key:*** Organizations must understand the potentially devastating financial impact of insufficient cyber-security. They must then enact management systems, guided by their CFOs, that bring all necessary executives together to address cyber-security issues on an enterprise-wide basis. This process would certainly involve security and technology personnel, but these groups should not be in charge of cyber risk management. An effective enterprise-wide management team is described below.

### A SIX-STEP SOLUTION

***Step 1:*** **Establish accountability.** There are few organizations that haven't adopted productivity-enhancing technology for essential business processes such as record keeping, supply chain management, online sales, etc.

***Problem:*** Data security has largely been relegated to an isolated, and often under-funded, operational department.

***Solution:*** Senior executives with cross-departmental authority such as CEOs, CFOs or chief risk officers (CRO) must take direct control and responsibility for their organizations' digital systems.

***Caution:*** The designated information security executive must thoroughly understand the role that technology plays in the organization, including the financial risks that technology places on the organization and the steps to mitigate these risks.

***Step 2:*** **Appoint a Cyber Risk Team.** Senior executives cannot know

*Continued on page 6*

# FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE

## Case Shows Entrenchment of Rating Agency Conflict

Among the core issues widely agreed to have contributed to the financial meltdown was the systemic conflict of interest between the three main securities rating agencies and the issuers that pay them for those ratings.

***Key:*** Because of this conflict, it has been argued, high-risk derivatives, including billions of dollars worth of bonds backed by subprime mortgages were given AAA ratings by the agencies in the years leading up to the crisis.

***Latest development:*** Moody's Investors Service Inc., Standard & Poor's and Fitch Ratings won dismissal of a negligence and fraud lawsuit by two California investors who lost money on highly rated bonds.

The case, initiated by a teacher, Sally Grassi and her husband, claimed that the couple lost $40,000 by investing in securities issued by Lehman Brothers and rated by the three agencies because of "fraud and deceit" by Lehman Brothers. The Grassis alleged that the three agencies "over-rated the quality and value of the bonds…knowing that potential investors and investment advisors would rely on the ratings and would not know [the] ratings were inaccurate and excessively high. [This] conduct…was done for the purpose of both assisting Lehman Bros. in the sale of [the] bonds, and also allowing [the] rating companies to retain the rating business of investments sold by Lehman Bros."

The case was moved to federal court where a U.S. Magistrate Judge ruled that "the circumstances constituting fraud…shall be stated with particularity." He further noted that the plaintiffs' case does not allege facts that establish each element of the two claims, and it falls far short of stating a plausible, cognizable claim..."

***Key lesson:*** Plaintiffs suing the rating agencies with allegations of fraud and deception will need to present extremely precise and relevant evidence proving these allegations. Despite overwhelming evidence of bias and deception by the rating agencies with respect to the high-risk derivatives, this legal objective may be exceedingly difficult to achieve in current and future cases.

***White-Collar Crime Fighter*** **source:** Order By Magistrate Judge Dale Drozd in *Ronald M. Grassi and Sally Grassi v. Moody's Investor's Services, et al.,* No. CIV S-09-0543 JAM DAD PS.

## Out-of-Band Authentication Update

Out-of-band authentication includes any technique that allows the identity of the individual originating an on-line transaction to be verified through a channel different from the one he or she is using to initiate the transaction.

***Example:*** If a customer makes a banking transaction via the Internet, the bank can automatically generate a telephone call or a text message. When the proper response (a verbal confirmation or an accepted transaction affirmation) is received, the transaction is completed. The non-Internet authentication is considered out-of-band because it uses a network separate from the Internet.

***Trap:*** Cyber-fraudsters have found ways of hacking into on-line financial institution or merchant systems to change customer telephone numbers, thereby enabling them to falsely authenticate a fraudulent transaction.

Lately, financial institutions and other on-line commercial organizations have been adopting SMS text-messaging to prevent fraudulent out-of-band authentication.

Experts now urge on-line commercial entities to use SMS messaging to minimize the risk of having customers defrauded by sophisticated hackers.

***Important:*** Different information security experts have different definitions of out-of-band security and offer varying technology solutions for mitigating risk. Consult with at least three respected security experts to ensure that you fully understand the best application for your organization.

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

- Search Security Channel, www.searchsecuritychannel.com.
- Security industry and academic information security reports and research.

*Continued from page 5*

all of the answers to the complex web of cyber-security issues within their organization.

***Solution:*** Form and lead a Cyber Risk Team that can address cyber-security from a strategic perspective. This team will need input from all affected operational departments and relevant professionals, assess this input and feedback, and make informed strategic decisions for the entire organization.

Draw team members from such key areas as human resources… legal…compliance…IT… major business units…communications.

***Step 3:*** **Meet regularly.** A face-to-face setting is ideal for the initial meeting of the Cyber Risk Team. Face-to-face discussions are particularly productive to counter the challenges of separate business units that don't "speak the same language."

**The common misconception that "the IT guy can handle the problem" causes employees to feel that they are not responsible for the security of their own data**

Moreover, approaching the critical but often complex issue of cyber-security can lead to misunderstandings about both organizational strategy and the unique needs and perspectives of various departments.

If an in-person meeting is difficult due to geographical obstacles, insist on at minimum an initial teleconference or videoconference.

***Important:*** Subsequent regularly scheduled follow-ups should occur through quarterly "check-ups" to stay current on shifting cyber threats and attacks, as well as mitigation strategies.

***Step 4:*** **Develop and enforce a Cyber Risk Management Plan.** Information security risk control is practically impossible without thorough planning.

***Essential:*** The Cyber Risk Team should determine which actions and roles—either existing or new—must be allocated to each functional area and establish the means to communicate and coordinate among all major functional areas. The result should be a well-defined, comprehensive information security "master plan." *The plan must include:*

☐ Measures for increasing employee awareness about the critical importance of information system and data security. Employees must be clear

*Continued from page 6*

about company policies on data categorization, data retention and incident response. The organization's plan must also include provisions for securing connections with business partners, outsourced suppliers and other remote connections.

☐ A formal incident response and crisis communications plan to notify stakeholders (and the media, when appropriate), since even the best-protected companies cannot totally eliminate the risk of a cyber incident.

***Step 5:*** **Develop and implement a cyber-risk budget.** Based on the Cyber Risk Plan, the Cyber Risk Team should calculate the gross financial risk for the organization.

***Useful guideline:*** The CSIS survey revealed that the cost of 24 hours of downtime from a major information security incident would average $6.3 million. A company in the oil and gas industry can expect a cost of up to $8.4 million per 24 hours of downtime.

***Also helpful:*** A study from the Ponemon Institute estimated that in 2009 the average cost of data breaches per compromised record was $204. Total cost per incident ranges from $750,000 to nearly $31 million.

Of the $204, 60% represents "direct" costs such as investigations and forensics, audit and consulting services, notification of affected individuals, public relations and communications, legal defense and compliance, and credit and identity monitoring. The remaining 40% is accounted for by the "indirect" cost of lost business.

***Caution:*** Appropriate security budgets for individual companies will vary. Whichever formula an organization chooses, it is important to run this calculation through a cross-departmental risk management team to get a true enterprise-wide perspective on financial cyber risks and to develop a consensus on the budget.

***Step 6:*** **Implement, analyze, test feedback.** Your cyber risk management plan must use clear metrics, including audits and penetration testing to generate feedback to update and upgrade each segment of the cyber risk management plan.

***Aim:*** To avoid overlooking or disregarding key information about an upcoming attack.

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

*The Financial Management Of Cyber Risk: An Implementation Framework For CFOs*, report by Internet Security Alliance (ISA) and American National Standards Institute (ANSI), available at www.TK.

# THE CON'S LATEST PLOY...

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

## Adrian, MI

**CFO steals for three years; company defaults on loans; CFO files for bankruptcy; 70 of 100 employees laid off. Who's fault is it?**

Donald Gerald Johnston, the former CFO of Kecy Products, pleaded guilty to charges of embezzling $380,000 from the auto parts manufacturer. A scheduled jury trial was canceled after Johnston entered the plea to a single embezzlement count carrying a maximum 20-year prison term. Ten other embezzlement charges and 11 counts of using a computer to commit a crime will be dismissed at sentencing which was postponed pending repayment of the stolen funds which could keep Johnston out of jail.

***Background:*** Police began an investigation in February last year after company officials reported suspicions of embezzlement of an estimated $390,000. The money was reportedly taken between September 1, 2005, and December 31, 2008. Johnston, was fired by Kecy Products in February.

But Johnston wasn't the only one out of a job. Seventy of the company's 100 employees were laid off. Management claimed that the lay-offs were unavoidable due to the extreme financial damage caused by Johnston's crimes.

***The plot thickens:*** At the same time Fifth Third Bank filed suit, demanding repayment of $8.7 million in loans. The plant was sold in July under a court order to new owners who are operating it under the name Kecy Corp.

Johnston's lawyer disputed the claim that his client's embezzlements caused the failure of Kecy Products last year. The judge in the case, however, demurred, stating that he counted the workers who lost their jobs and company investors as victims of the crime. The judge went further to suggest that Johnston used his position as chief financial officer to falsify the books and carry out thefts for more than three years, conduct the judge defined as "predatory." According to the judge, the embezzlement was carried out over 38 months with thefts of approximately $10,000 per month.

Though the defense argued that the bank debt owed to First Third was the cause of Kecy's failure, the company's court-appointed receiver stated Johnston was at fault. The receiver stated the discovery of the embezzlement and disarray of the company's books caused Fifth Third Bank to go to federal court to call its loans.

## Boston, MA

**One small victory for investors defrauded during the unregulated years of subprime mania.** In what surely will prove to be just one of hundreds if not thousands of similar financial crisis-related legal episodes, SEC settled a civil action it initiated in February against State Street Bank and Trust for misleading investors during the subprime mortgage crisis in 2007.

Without admitting or denying any wrongdoing, State Street agreed to pay more than $300 million to a special fund to benefit the victims of its actions which, according to the Commission, involved deceiving investors about the amount of subprime mortgage-backed securities held in certain funds under its management, and then disclosing more complete and accurate information about these risky investments to certain select investors.

***Key details:*** Investors in the funds lost over $60 million during the sub-

prime market meltdown in mid-2007. But other investors in State Street funds lost much more. Prior to the settlement with the SEC, State Street had already paid back more than $300 million to harmed investors, Its agreement to pay more than $300 million more to settle the SEC's action makes a total of more than $600 million to be paid back to investors victimized by the bank's fraudulent activities.

***The alleged frauds:*** The SEC's complaint alleged that State Street established the Limited Duration Bond Fund in 2002 and marketed it as an "enhanced cash" investment strategy that was an alternative to a money market fund for certain types of investors.

By 2007, however, the Fund was almost entirely invested in subprime residential mortgage-backed securities and derivatives that magnified its exposure to high-risk subprime securities.The SEC alleged that State Street continued to describe the Fund to prospective and current investors as having "better sector diversification" than a typical money market fund, but failed to explain the extent of the Fund's concentration in subprime investments.

***Playing favorites:*** According to the complaint, beginning in July 2007, State Street sent investors a series of misleading communications concerning the effect of the turmoil in the subprime market on the Fund and other State Street funds that invested in the Fund. But at the same time, as noted above, State Street provided certain investors with more complete and accurate information about the Fund's subprime concentration and other problems with the Fund. These favored investors included clients of State Street's internal advisory groups, which provided investment advice to some of the investors in the Fund and the related funds. According to the Commission's complaint, State Street's internal advisory groups subsequently decided to recommend that all their clients redeem from the Fund and the related funds.

In what is most likely not a coincidence, the pension plan of State Street's publicly traded parent company (State Street Corporation) was one of those clients.

***Key:*** The SEC alleged that State Street sold the Fund's most liquid holdings and used the cash it received from these sales to meet the redemption demands of better informed investors, leaving the Fund and its remaining investors with largely illiquid holdings.

In addition to agreeing to the repayment, State Street committed to retaining an "Independent Compliance Consultant" to conduct a comprehensive review of the company's disclosures, compliance and other policies and procedures for its pooled investment strategies.

## A Not-Too-Subtle Message About Auditing for Repos

In what audit experts believe to be a direct response to the debate over Ernst & Young's controversial treatment of its client, Lehman Brothers' use of so-called Repo 105 off-balance-sheet transactions to allegedly hide liabilities in an effort to falsely reflect its financial condition as it was slipping toward collapse, the Public Company Accounting Oversight Board's (PCAOB) issued on April 7 Staff Audit Practice Alert No. 5.

The Alert is designed to remind auditors of public companies about their responsibilities to assess and respond to the risk of material misstatement of financial statements due to error or fraud posed by what it calls "significant unusual transactions."

***Key:*** In the PCAOB staff's view, although "economic conditions have changed since December 2008," the risk factors, including those of fraud related to significant unusual transactions, continue to exist today.

Alert No. 5 groups auditing requirements with respect to unusual transactions into key categories:

- Identifying and assessing risks of material misstatement.
- Responding to risks of material misstatement.
- Consulting others.
- Evaluating financial statement presentation and disclosure.
- Communicating with audit committees.
- Reviewing interim financial information.

***Key details:*** "In obtaining the information needed to identify risks of material misstatement due to fraud, the auditor… should inquire of others within the company about the existence or suspicion of fraud, including employees involved in initiating, recording, or processing significant unusual transactions."

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

- Staff Audit Practice Alert No. 5, *Auditor Considerations Regarding Significant Unusual Transactions,* Public Company Accounting Oversight Board http://pcaobus.org/Standards/QandA/04-07-2010_APA_5.pdf.

## COMING SOON IN White-Collar Crime Fighter…

- **Fraud-auditing with data mining**
- **Automating accounts payable: Essential anti-fraud factors**
- **Using e-mail to detect fraud**
- **Fraud prevention preparation for economic recovery**