WHITE-COLLAR CRIME FIGHTER
www.wccfighter.com
YOUR SECRET WEAPON IN THE WAR ON FRAUD
VOLUME 15 NO.2
FEBRUARY 2013

David Clements, *Deloitte Corporate Finance, Ltd.*

You've Discovered a Fraud... What Now?

It is possible to prevent many frauds …but not all of them. That is news to no one. Neither is the obvious implication that if your organization is perpetually vulnerable to some fraud, having a carefully conceived response plan in place is smart.

Key: A Fraud Response Plan (FRP) can help companies to handle incidents in a systematic and efficient manner—not only to conduct an effective investigation—but also to show that the organization acts in a prudent and lawful manner.

BLUEPRINT FOR DAMAGE CONTROL

Here is a sample blueprint for responding to a fraud if and when it does actually occur...

•**Initial action.** When fraud is first suspected, the matter may be more serious than it may initially appear.

Reason: Fraudsters rarely restrict their illegal activities to only one modus operandi or method.

Important: Obtain as much information as possible before questioning anyone who may be either directly or indirectly involved in the fraud. This can help you to avoid being misled…failing to recognize untruthful answers…tipping off potential fraudsters to destroy evidence…or making false accusations that lead to lawsuits.

This is especially critical in organizations or business units with a close working environment or an action-oriented boss, where there may be a strong temptation to question an employee as soon as suspicion is raised.

Also important: Be aware that large-scale frauds are often international in scope. This applies especially to cases of bribery, kickbacks and financial reporting fraud.

Essential: Your fraud contingency plan should include seeking legal advice to help

IN THIS ISSUE

comply with local laws and regulations governing investigations in different jurisdictions. Consulting attorneys and forensic accountants with investigative experience is key.

Because of the dependency of business activity on electronic tools and communication, electronic evidence is often vital to investigating corporate fraud.

Caution: Prior to initiating a fraud investigation, consult with your information security or IT team about obtaining the necessary computer forensic and investigative skills for gathering digital evidence that may be pertinent to the fraud case.

Bottom line: Initial actions are crucial to the eventual outcome of any fraud investigation. If a response plan is put in place and adhered to, the extent of fraudulent activity can usually be assessed more easily and action taken more quickly to resolve the matter. This usually means gathering sufficient evidence to discipline staff and to commence civil and/or criminal proceedings against those involved in the fraud, or claims against insurers.

•**Fraud response team.** Some FRPs only deal with situations where an employee discovers a fraud and hands it over to a fraud examiner or investigation department to follow up. However, some frauds have impact far beyond the limits of your investigation capabilities—such as when the organization's reputation, stock price or overall financial viability is threatened.

Key: The FRP also should include contingencies for these eventualities. Most large organizations have formed crisis management committees to respond to major incidents (such as fires or explosions) and it is prudent to take a similar approach in a fraud response plan.

Guidelines: Typically, this means forming a Fraud Incident Management Team, comprising essential members and "stand-by" members.

In some types of fraud, the victim organization may only have a few hours to take action to freeze funds, which have been illicitly transferred. It is essential that contact information for essential service providers is organized and made readily available beforehand, including internal support departments, such as legal, corporate security, insurance, external lawyers, law enforcement, telecommunications providers, forensic accountants and investigators.

•**Initial responsibility designation.** Fraud investigation is, by necessity, a confidential process and is a highly sensitive matter for most organizations.

Result: It is vital that allegations of fraud be treated seriously and that responsibility for handling fraud incidents is assigned to a senior, experienced and trusted individual or team of individuals. In many organizations, this responsibility is assigned to a compliance officer, lawyer, corporate security advisor, internal audit executive or risk management director.

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, 2417 Havershire Dr., Raleigh, NC 27613. www.wccfighter.com. Subscription cost: $295/yr. Canada, $345.

In other organizations, the responsibility is shared between members of senior management or an audit committee and the organization's human resources personnel and corporate lawyers are involved from a very early point.

Important: Fraud incident management responsibility is a critical role and those designated to administer the role should possess the appropriate skills and experience to identify the key risks involved and to coordinate the organization's response.

Helpful: As part of your fraud control plan, assign responsibility for fraud incident management to an appropriate person(s) prior to adopting an incident management plan, and tailor the assignment responsibility based on the type of fraud.

Recommended: Assign the appropriate level of involvement of corporate lawyers and human resources (HR) personnel, in the conduct of the investigation or in responding to its findings, such as termination of guilty individual(s), prosecution or other employment-related legal decisions.

•**Receipt and assessment of suspicion, allegation or tip.** Fraud investigations are often initiated after an allegation or an employee or customer tip (often anonymous) is received.

In addition, some fraud incidents are initially discovered by accident, perhaps as a result of an internal audit, job change or resignation.

The checklist below highlights initial actions to be taken—or avoided—in most cases of discovering a fraud or receiving a tip.

At the conclusion of this stage, a decision must be made as to whether the allegation or suspicion warrants investigation or is implausible or vexatious.

Caution: This decision must be made carefully. If an allegation cannot be quickly dismissed as false, further action ordinarily should be taken.

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

"Keep Calm and Carry On," by David Clements, director, Deloitte Forensic, Deloitte Corporate Finance Ltd., Dubai, UAE, davclem ents@Deloitte.com.

More from David Clements...

Typical Initial Actions Upon Discovering a Potential Fraud

1. Alert the fraud incident manager about an allegation or suspicion. He or she may be required to notify legal or regulatory authorities, or your insurer, and in some cases get their permission before investigating further.

2. Document date, time and details of initial report/discovery.

3. Take notes of all observations and actions.

4. Maintain confidentiality (only inform those who need to know about the suspected act). Unwarranted disclosure can undermine investigations.

5. Do not initially confront the suspect.

6. Write out in full the suspected act or wrongdoing, including:

   - Details of the alleged offense.
   - Identity of suspected perpetrator.
   - Is the activity continuing?
   - Where did it occur?

- Value of the loss or potential loss.
- Who knows of the activity?

7. Identify documentary and other evidence connected to the activity, including…
   - Invoices
   - Receipts
   - Contracts
   - Purchase orders
   - Checks
   - Computers
   - Credit card statements
8. Secure evidence.
9. Protect evidence from damage or contamination.
10. List each item individually, taking note of acquisition (including time, date and location) and where the item was securely stored.
11. Identify potential witnesses.
12. Unless electronic evidence is being destroyed do not go into the suspect's computer systems.
13. If possible, secure and/or remove the suspect's access to relevant computers/systems. Do not allow your IT department to examine computers that may be involved in the suspected fraud.
14. Consider other potential suspects and extent of fraud.

MORTGAGE FRAUD

Have We Learned Anything from the Financial Crisis?

Several studies have confirmed what has been widely reported and analyzed — that lenders weren't just making bad mortgages during the mid 2000s—they were falsifying documents in order to make loans look better on paper. Banks then sold these bogus mortgages to investors all over the world. The securities backed by the loans ultimately turned in large part to junk.

Reason: Ultimately, many of these mortgages turned out to be toxic. In their paper, three prominent academic researchers found that the pool of misrepresented mortgages they studied were 60% to 70% more likely to default than other loans.

Disconcerting now: According to a new report, researchers conclude that, "A significant degree of misrepresentation exists across all reputable [financial organizations] involved in sale of mortgages."

To avoid a repeat disaster, lead researcher, Tomasz Piskorski of Columbia University wants to see regulation on disclosure between lenders and investors alongside the kind of proposals

out now that would regulate qualified mortgages and mortgage servicing.

Key issue: Laws governing disclosure are far and few between. Creating rules to limit this type of fraud would be another step in making sure that what took place during the bubble doesn't happen again.

***White-Collar Crime Fighter* source:** "Asset Quality Misrepresentation by Financial Intermediaries: Evidence from RMBS Market," by Tomasz Piskorski and James Witkin of Columbia University and Amit Seru of the University of Chicago , http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2215422.

INVESTIGATOR'S EDGE

FRAUD COVER-UPS
How to Tell When Something Doesn't Smell Right...

When investigators start looking into an organizational fraud, they typically adhere to the tried and true rule of "follow the money." This approach is based on decades of fraud examination and forensic auditing technique for detecting red flags and even hard evidence of such crimes as embezzlement, inventory theft, check fraud and financial reporting fraud.

However, in today's digital age, following the money doesn't always go far enough. It is now essential to enhance investigative techniques by following the *information*.

Key: Most major corporate fraud concealment is orchestrated at the top levels of management. Falsification of financial records is a management misdeed—often motivated by the need to satisfy shareholder or board expectations.

However, key pieces of information related to a cover-up of a financial fraud are almost always known to lower-level employees such as accountants, purchasing employees, etc. These individuals may not have the stomach to risk their jobs by blowing the whistle, so they often document the fact that they had just been following orders by their superiors when they, for example, made false journal entries, altered sales figures, falsified receivables, etc.

Important: This documentation typically exists in the form of E-mails, but it may also exist in hard copy if the employees anticipate that their computers may eventually be confiscated in an investigation and they will need documentation to prove their innocence.

Problem: Despite the existence of laws that protect whistleblowers from retaliation, few are willing to risk their jobs to divulge the truth about internal wrongdoing. This is often because of an environment of intimidation where employees are given to believe that if they do blow the whistle, unpleasant consequences will result.

SIGNS OF COVER-UP

• **Denial.** According to Harvard Business School Professor Max Bazerman, speaking recently on NPR Radio, "...what we often do is try to deny that we were involved in any bad behavior to begin with. One of the interesting themes…is loyalty, and to the extent that we feel loyal to our organization, that really keeps us from admitting to the wrongdoing and admitting…the bad behavior that we've been involved in and the bad behavior that our organization has been involved in."

Participating in the same discussion on NPR, Bruce Antkowiak, a former federal prosecutor, now director of the criminology program at St. Vincent College, described the cover-up patterns in cases where "…you know from the outset that you need to keep this thing covered up [and] you will turn to almost any means possible, to buying people off, to promising them a great benefit, to threatening them that they will in fact suffer dire consequences if they blow the whistle on this.

"[In such cases] the role of outside lawyers [is] one of the most important things that I always look at when I see a case involving a cover-up.

"Was there an attorney who was brought in from the outside to assist in this? And what role did they play? Did they uphold what we all hope to be the highest standards of the profession and do what the client needs in that circumstance, which is sit down with that client across the table and say, what you're doing is wrong?"

• **Inventory shenanigans.** One of the great cover-up stories of recent memory is that involving the now-defunct consumer electronics retailer Crazy Eddie. To cover up a massive accounting scheme which included enormous exaggerations of inventory value, the company had employees stack empty television cartons to the ceiling of company warehouses whenever it was known that the auditors would be visiting.

• **Firing, demoting or intimidating.** Management fraud such as accounting schemes, high-level embezzlement, bribery and other costly frauds can be covered-up by:

☐ Firing/demoting or threatening potential whistleblowers.

☐ Shredding documentation and/or attempting to delete incriminating E-mails.

Examples: The termination in November 2011 of Ming Li Liu, a senior compliance manager at Siemens (See also *White-Collar Crime Fighter,* January 2013), when he tried to report to senior management the existence of what he concluded to be serious violations of anti-bribery laws in connection with the sale of big-ticket medical equipment to China.

Or the well-publicized intimidation and layoff tactics of former Sunbeam CEO, Al "Chainsaw" Dunlap.

• **Preventing internal audit or the fraud prevention team from gathering potential evidence of fraud.**

Example: Countrywide Financial, the mortgage lender that become synonymous with fraudulent subprime lending in the years leading up to the financial crisis of 2008. In its obsessive quest for more and more mortgage-related fees, Countrywide approved loans with fictitious income statements, phony asset listings, fraudulent employment histories and much more. When investigators came to get to the bottom of what Countrywide had been doing they were forbidden from interviewing key employees, and were obstructed by senior manager warnings to employees to delete E-mails.

• **Financial reporting manipulation tactics.** A study of the accounting policies of the failed Canadian Commercial Bank (CCB) identified five specific accounting decisions that prevented the CCB's insolvency from coming to light much earlier than it otherwise might have, including:

☐ Avoiding or delaying recognition of loan losses by delaying reclassification of loan s as non-performing as long as possible, using unrealistic values for collateral, and making workout agreements for loans in danger of becoming non-current;

☐ Recognizing fee and interest income from renegotiated/uncollectible loans.

☐ Making insufficient transfers of retained earnings to the Statement of Appropriations for Contingencies despite increasing loan loss experience.

☐ Using income tax recoveries to more than offset losses without sufficient assurance that there would be future taxable income.

• **Willful blindness.** Where victims of fraud enable a cover up by choosing not to question possible wrongdoing. According to attorney Neal Levin, this insidious psychological syndrome occurs when victims of fraud trust in the fraudster and simply decide not to question their actions.

Example: Bernard Madoff's victims chose not to scrutinize the investment reports they were receiving from him because they felt there was no reason to distrust them. Moreover, the favorable returns they thought they were getting never influenced them to wonder if they were too good to be true.

Key: Fraudsters exploit this knowledge that their victims will never question their actions. The same occurred with Wall Street firms such as Goldman Sachs which knew that the clients it was knowingly selling "toxic" investments to would never question the virtues of the securities which Goldman Sachs was vouching for.

• **Covering up for others.**

Example: A former New York State senator pleaded guilty to falsifying evidence in an attempt to cover up the theft of taxpayer money from a nonprofit agency that she founded.

Details: The former senator Shirley L. Huntley told a judge that she drafted and backdated a letter in March 2011 to create a false record that the nonprofit agency, Parent Workshop Inc., held an event that never actually happened. The agency was supposedly dedicated to helping parents navigate the school system, but prosecutors said employees there and at another nonprofit organization she ran stole more than $100,000 in state grants instead of spending the money on programming.

Key detail: Huntley was not accused of stealing the money herself but rather of covering up $30,000 in thefts by others. Her actions came to light after a joint investigation by the state attorney general, Eric T. Schneiderman, and the state comptroller, Thomas P. DiNapoli. Schneiderman filed the charges.

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

• Joseph Dooley, CPA/CFF/CITP, CFE, CIPP, Managing Director, Stroz Friedberg, New York-based fraud and cyber-crime investigation consultants, jdooley@strozfriedberg.com.

• Neal Levin, fraud and internal investigations practice, Freeborn & Peters LLP, attorneys, freebornpeters.com.

• Press reports.

FUNDS TRANSFER FRAUD

Practical Tips for Preventing Internet-Based ACH Fraud

Cyber-attacks on organizations of all kinds to steal sensitive information, disable system networks and steal money have been on a disturbingly rapid rise in recent years.

Among the most lucrative assaults by cyber-fraudsters: ACH account takeover.

How it works: There are several variations on the theme of ACH account takeover, but

in general many of the attacks involve acquiring the access information—username and password—of account administrators through planting of Trojan horse "malware" and then using that access information to illegally access the account and fraudulently transfer stolen funds to an account they control.

Added threat: New malware—installed on victim computer browsers—validates that the person logging on is who he/she claims to be. When the user initiates an on-line transaction, the infected browser covertly carries out illicit transactions such as wire transfers and ACH withdrawals deposited into accounts owned by money mules who believe they were hired as payroll coordinators, collection agents or similar occupations. The money mules then withdraw cash to be forwarded via Western Union or MoneyGram to the fraudsters. Neither the bank nor the customer are aware that the fraudulent activity has taken place.

Variation: Anti-fraud mechanisms and risk-based tools are rendered ineffective by a virus that has compromised the victim's login credentials, thereby making the transaction appear to have been legitimately initiated by the account owner.

These tools require answers to pre-determined authentication questions used to validate the requested transaction(s). Those validating questions are captured through key-logging software planted on victims' PCs via Trojan horse malware. Once the user is validated the transactions are processed and funds are fraudulently transferred according to the instructions provided.

THE GOOD NEWS

Many of these cyber-schemes have been around for several years now, giving law enforcement, the banking industry and information security experts time to come up with best practices for protecting against these crimes.

From Financial Services-Information Sharing and Analysis Center (FS-ISAC):

- Continuously educate customers about account features for fraud prevention—such as check cashing limitations and automated payment filters (ACH debit filters).
- Perform daily reconciliations of all transactions and follow-up on any discrepancies.
- Implement and enforce dual control for all ACH and wire transfers—a transaction originator and a separate transaction authorizer.
- Use only stand-alone, "locked down" computer systems disabled from E-mail and Web browsing.
- Be alert to new phishing attacks—E-mails purporting to be from your bank/financial institution or any other "institution" requesting personally identifiable information such as Social Security number, date of birth, employee number, home address, etc.
- Enforce use of strong passwords— with 10 or more characters comprising a mix of upper and lower case letters and numbers.
- Prohibit use of shared usernames and passwords.
- Periodically change passwords (monthly if possible).
- Strictly limit admin rights on users' workstations.
- Enforce regular updates of virus protection and security software.
- Install spyware detection software.
- Never leave an ACH-originating computer unattended while a transaction is in process.
- Clear browser cache before starting online banking sessions.

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

• Thomas Nash, Directory of Training, International Association of Financial Crimes Investigators (IAFCI), www.iafci.org.

• Financial Services-Information Sharing and Analysis Center (FS-ISAC), financial services industry anti-fraud and security information-sharing services, www.fsisac.com.

CYBER-CRIME **FIGHTER**

Important New Insights Into the Cost of Cyber-Crime

A group of researchers from the Computer Laboratory at the University of Cambridge in the UK came out with a report which provides much-needed clarity to the entire cyber-crime crisis. *The team starts with a three-part definition of cyber-crime:*

1. Traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems.

2. Publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to ethnic hatred).

3. Crimes unique to electronic networks—such as attacks against information systems, denial of service and hacking.

HOW MUCH DOES CYBER-CRIME REALLY COST?

Some experts believe that many estimates of the cost of cyber-crime are vastly overstated. This is not surprising in light of the fact that many of the studies produced each year are released by companies that also sell anti-virus software and other products designed to protect organizations and individuals against the bad guys in cyber-space.

This is not to suggest that cyber-crime isn't highly costly and that nearly every entity and individual is a potential victim. But it is helpful to senior managers to have reliable data when trying to make decisions about how best to protect against these crimes.

Key: The Cambridge researchers acknowledge this and have attempted to apply a more scientific methodology to their analysis.

They started by studying the various individual cyber-crimes plaguing organizations today and analyzed the financial damage resulting from each.

To do this, the researchers first broke down the complex cyber-crime problem into distinct cost categories...

• **Criminal revenue.** This refers to the monetary equivalent of the gross receipts from a crime. It does not include "lawful" business expenses of the criminal(s).

Example: An illegal on-line pharmacy may purchase hosting services from a legitimate provider and pay the market price. This reduces the criminal's profit, but contributes to the gross domestic product (GDP) of the economy in which the provider is located.

Contrast: Phishing advertised by E-mail spam. The "phisher's" ill-gotten revenue is the

sum of the money withdrawn from victim accounts. If spamming is also a crime, and is carried out using a botnet (a network of subverted PCs), then the revenue of the spammer, possibly split with the "owner" of the malicious software, must be accounted for as part of overall criminal revenue contribution to GDP.

• **Direct losses.** This includes the monetary equivalent of losses, damage or other suffering by the victim as a consequence of a cyber-crime. *Direct losses include:*

- Money withdrawn from victim accounts.
- Time and effort to reset account credentials (for both financial institutions and consumers).
- Secondary costs of overdrawn accounts—deferred purchases, inconvenience of not having access to money when needed, etc.

• **Indirect losses.** This refers to the monetary equivalent of the losses and opportunity costs imposed on the economy by the fact that a cyber-crime is carried out, no matter whether successful or not and independent of any specific instance of that cyber-crime.

Key: Indirect costs generally cannot be attributed to individual victims. *Indirect losses include:*

- ☐ Loss of trust in online banking, leading to reduced revenues from electronic transaction fees, and higher costs for maintaining branch staff and check- clearing facilities.
- ☐ Missed business opportunity for organizations to communicate with their customers by E-mail.
- ☐ Reduced electronic business as a result of lessened trust in on-line transactions.
- ☐ Efforts to clean up PCs infected with the malware for a spam-sending botnet.

• **Defense costs.** Defense costs are the monetary equivalent of prevention efforts. They include direct prevention costs, such as the cost of development, deployment and maintenance of prevention measures, as well as indirect costs, such as inconvenience…and opportunity costs caused by the prevention measures. *Specifically, defense costs include:*

- ☐ Security products such as spam filters, antivirus and browser extensions to protect users.
- ☐ Security services provided to individuals, such as training and awareness measures.
- ☐ Security services provided to industry, such as Web site "take-down" services.
- ☐ Fraud detection, tracking and recuperation efforts.
- ☐ Law enforcement.
- ☐ The inconvenience of missing an important message falsely classified as spam.

• **Cost to society.** The cost to society is the sum of direct losses, indirect losses and defense costs.

DOLLARS AND CENTS

According to the researchers, annual monetary losses to cyber-crime break down as follows:

• "Actual cyber-crime (including online banking losses and anti-malware defense, intellectual property-related loss and several high-profile consumer crimes): $2.5 billion.

• "Transitional cyber-fraud" (including credit card fraud—both online and offline,

indirect costs of payment fraud (primarily lost customer confidence in online payment): $41 billion.

• "Cybercriminal infrastructure" (including anti-virus expenditures, software patching, ISP and end-user cleanup, anti-cyber-crime defense cost to business generally and law enforcement services): $24.8 billion.

Critical conclusion: While it is understandable that organizations will continue to invest heavily in protection against direct and indirect losses, the Cambridge research suggests that, "It is possible to spend too much on defense."

This is plausible in light of the fact that despite the gargantuan investments in cyber-crime protection, losses to on-line bad guys continue to rise.

Companies worldwide spend an estimated $10 billion on basic cyber-crime prevention (not including the specialized anti-fraud costs borne by financial institutions and merchants).

An additional estimated $1 billion is spent globally on creating security patches for software vulnerabilities, while another $400 million is spent annually on cyber-crime-related law enforcement activity (roughly one-half of which is spent by the US).

Critical conclusion: Regardless of which numbers you use, the indisputable fact is that they are all going up.

Key message: Companies and government agencies should "spend less in anticipation of computer crime (on antivirus, firewalls etc.) [...and an] awful lot more on catching and punishing the perpetrators.

Note: This article is based in large part on "Measuring the Cost of Cyber-crime" by Ross Anderson, Computer Laboratory, University of Cambridge, Chris Barton, Rainer Boehme, University of Munster, Department of Information Systems, Richard Clayton, Computer Laboratory, University of Cambridge, Michel J.G. van Eeten, Faculty of Technology, Policy and Management, Delft University of Technology, Netherlands, Michael Levi, School of Social Sciences, Cardiff University, Cardiff, UK, Tyler Moore, Department of Computer Science and Engineering, Southern Methodist University, Dallas, TX, and Stefan Savage, Department of Computer Science and Engineering, University of California, San Diego, CA.

A version of this article originally appeared in *The Fraud Examiner* newsletter, a publication of the Association of Certified Fraud Examiners, www.acfe.com

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE

Continuous Fraud Detection

The following steps have proven useful in implementing effective fraud detection programs:

Even in organizations where strong anti-fraud controls are in place, it is prudent to monitor transactions and look for the signs of potential fraud.

A continuous fraud detection program will follow some of the same principles and steps

as a continuous risk and control assurance (CRCA) program, even if the continuous auditing activity is limited to fraud detection rather than a full CRCA program:

A CRCA program will typically include fraud risks, monitoring their level, testing the controls and examining activity for potential issues of concern.

• Design the program and define your needs before selecting software or developing detailed testing techniques.

• Identify the fraud risks specific to your organization. Every company is different, and the risks from fraud will vary.

• Assess each fraud risk for likelihood and potential damage.

• Select the fraud risks that the program will address.

For each risk, identify how the fraud would work: What are the fraud schemes? Determine how an inspection of transactions or other activity (such as trend analysis, comparison of same product margins in different locations, or the detection of transactions approved by the same person who originated the transactions) might detect potential fraud. Design the process for investigating exceptions.

• Discuss the process with any management personnel who might be involved in reviewing and providing explanations for exceptions.

• Develop and implement the program. Monitor and adjust the testing procedures as necessary (such as changing tolerances on any automated tests that are producing false positives).

• Continue to monitor fraud risks and adjust the program as needed. Review and continually improve the fraud detection program.

White-Collar Crime Fighter **source:** Norman Marks, Vice President, Governance, Risk, and Compliance (GRC), SAP, writing at www.qfinance.com.

How to Identify Suspicious Employee E-mail

Software developed by the FBI and Ernst & Young can flag the most common words used in E-mail conversations among employees engaged in internal fraud.

Background: The software was developed using information from actual corporate fraud investigations. When implemented, it can identify and track such common fraud-related phrases as "cover up," "write off," "failed investment," "off the books," "nobody will find out" and "grey area."

Added findings: Phrases such as "special fees" and "friendly payments" are most common in bribery cases, while fears of getting caught are shown in phrases such as "no inspection" and "do not volunteer information."

The analytics software also scans for "out of band" events such as "call my mobile" or "come by my office"—words that suggest the writer does not want to be overheard.

The top fraud words and phrases in e-mail conversations:

1. Cover up
2. Write off
3. Illegal
4. Failed investment

5. Nobody will find out

***White-Collar Crime Fighter* source:** Rashmi Joshi, director, Fraud Investigation and Disputes Services, Ernst & Young, www.ey.com.

THE CON'S LATEST PLOY...

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

Monroe, OH

Maximum absence of segregation of duties enables 30-year fraud, ultimately bankrupting small credit union of devout members. Sharon Broadway, who pleaded guilty last December to embezzling more than $2 million from a now-bankrupt credit union was sentenced to at least 45 months in prison.

The plea pertained to felony counts of racketeering and financial institution embezzlement from Monroe County's United Catholic Credit Union, which closed in August after state regulators discovered it was insolvent.

A judge in Monroe County's 38th Circuit Court sentenced Broadway to 10 to 240 months on the embezzlement charge and a concurrent 45 months to 240 months on the other charge. She also was ordered to pay $2.6 million in restitution and is prohibited from working in the financial industry, according to reports from the state attorney general's office.

The Ohio Office of Financial and Insurance Regulation reportedly shut down the credit union, which had approximately 200 members belonging to area Catholic parishes.

How the fraud occurred: Broadway was, according to the Attorney General's office the credit union's "manager, secretary, board member and sole employee."

Officials said she hid her actions for nearly 30 years by using a scheme that included maintaining no record of certificates of deposit on credit union books.

Credit union members did not lose money because the funds were federally insured by the National Credit Union Administration, said John Kolhoff, deputy commissioner of the Office of Financial and Insurance Regulation credit union division. Any restitution will go to the National Credit Union Administration to cover its losses, he said.

Detection: State officials said the fraud was found during a routine examination by regulators.

New York, NY

Creators of seven-year-old mega-virus finally caught and charged. Preet Bharara, U.S. Attorney for Manhattan, Lanny A. Breuer, the Assistant Attorney General of the U.S., and George Venizelos, Assistant Director-in-Charge of the New York Field Office of the FBI, announced the unsealing of indictments of three individuals involved in creating and distributing the so-called Gozi virus, one of the most financially destructive computer viruses in history.

Background: The Gozi virus infected over one million computers globally and caused

tens of millions of dollars in losses. Nikita Kuzmin, a Russian national who created the virus, was arrested in the U.S. in November 2010 and pled guilty to various computer intrusion and fraud charges in May 2011. Deniss Calovskis, a/k/a "Miami," a Latvian national who allegedly wrote some of the computer code that made the virus so effective, was arrested in Latvia in November 2012. Mihai Ionut Paunescu, a/k/a "Virus," a Romanian national who allegedly ran a "bulletproof hosting" service that enabled cyber-criminals to distribute the Gozi virus, the infamous Zeus Trojan and other notorious malware, and conduct other sophisticated cyber-crimes, was arrested in Romania in December 2012.

Deadly details: The Gozi virus is malicious computer code or "malware" that steals personal bank account information, including usernames and passwords, from the users of infected computers. It was named by private sector information security experts in the U.S. who, in 2007, discovered that previously unrecognized malware was stealing personal bank account information from computers across Europe on a vast scale, while remaining virtually undetectable in the computers it infected.

Damage done: To date, the Gozi virus has infected over one million computers worldwide, including at least 40,000 in the U.S., some belonging to the National Aeronautics and Space Administration ("NASA").

Also affected: Computers in Germany, Great Britain, Poland, France, Finland, Italy, Turkey and elsewhere. It has caused tens of millions of dollars in losses to the individuals, businesses, and government entities whose computers were infected.

Key: According to court documents, Gozi was distributed to victims' computers in several different ways including being disguised as a benign .pdf document which, when opened, secretly installed the Gozi virus on the victim's computer. Once installed, the virus—which was intentionally designed to be undetectable by anti-virus software—collected data from the infected computer in order to capture personal bank account information including usernames and passwords. That data was then transmitted to various computer servers controlled by the cyber-criminals who used the Gozi virus. These cyber-criminals then used the personal bank account information to transfer funds out of the victims' bank accounts and ultimately into their own personal possession.

Refinement of the Gozi virus: Kuzmin and his co-conspirators reportedly paid others to refine, update and improve the Gozi virus.

Example: Calovskis, one of the co-conspirators, was hired to develop certain computer code, known as "Web injects," which altered how the Web pages of particular banks appeared on infected computers. Specifically, Calovskis's Web injects altered the Web pages of banks so that, when a victim used an infected computer to access the Web page, the victim was tricked into divulging additional personal information that cyber-criminals would need in order to successfully steal money from the victim's bank account.

One Web inject Calovskis designed altered the customer welcome page of a bank so that the victim was prompted to disclose additional personal information—mother's maiden name, Social Security number, driver's license information and a PIN code—in order to continue accessing the Web site.

Added problem: So-called "bulletproof hosting" services helped cyber-criminals distribute the Gozi virus with little fear of detection by law enforcement.

Key: Bulletproof hosts provided the critical online infrastructure such as Internet Protocol ("IP") addresses and computer servers, in a manner designed to enable them to preserve their anonymity.

Paunescu operated a "bulletproof host" that helped the alleged cyber-criminals distribute the Gozi virus and commit other cyber crimes, such as distributing malware including the "Zeus Trojan" and the "SpyEye Trojan," initiating and executing distributed denial of service ("DDoS") attacks, and transmitting spam. Paunescu rented servers and IP addresses from legitimate Internet service providers and in turn rented them to the cyber-criminals. He also is charged with providing servers that cyber-criminals used as command-and-control servers to conduct DDoS attacks…monitored the IP addresses that he controlled to determine if they appeared on a special list of suspicious or untrustworthy IP addresses…and relocated his customers' data to different networks and IP addresses, including networks and IP addresses in other countries, to avoid being blocked as a result of private security or law enforcement scrutiny.

Extradition proceedings against Cavloskis in Latvia and Paunescu in Romania are ongoing.

The case against Paunescu is being prosecuted jointly with the Department of Justice's Computer Crime and Intellectual Property Section ("CCIPS"), which is overseen by Assistant Attorney General Lanny A. Breuer.

Bharara praised the FBI for its work in the investigation, which he noted is ongoing. He also specially thanked the National Aeronautics and Space Administration Office of Inspector General, the Central Criminal Police Department of the Latvian State Police, the Romanian Intelligence Service, the Romanian Directorate for Combating Organized Crime, the Romanian Directorate for Investigating Organized Crime and Terrorism, and the Romanian Ministry of Justice.

The cases are being handled by the Complex Frauds Unit of the United States Attorney's Office.