

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

LUME 6 NO. 4
APRIL 2004



IN THE NEWS

Internet Banking Doing Booming Money Laundering Business

New research shows a disturbing surge in the use of Internet banks and on-line financial services to launder money.

Details: The Financial Crimes Enforcement Network (FinCEN) reports that while fewer than 30 SARs relating to electronic banking were filed in 1999, that number jumped to nearly 100 in 2000 and to just under 300 in 2002. Preliminary data indicate that the number will have surpassed the 300 mark in 2003.

Sixty-eight of the total 776 Internet/on-line-related SARs filed between 1996 and the first quarter of 2003 implicated Internet banks. There are only 40 such banks licensed to do business in the US, compared with approximately 20,000 "brick-and-mortar" banks.

Significance: A mere 0.2% of total banks were used for transactions leading to filing of 8.7% of all Internet/on-line-related SARs in 1996-2003. The rest of the electronic banking-related SARs involved brick-and-mortar banks, with leading violations including check fraud...computer intrusion... BSA/structuring/money-laundering... and check counterfeiting.

White-Collar Crime Fighter source: SAR Activity Review—Trends, Tips and Issues, SAR Activity Review Project, co-chaired by John Byrne, Senior Counsel, American Bankers Association and David Gillis, Assistant Director, Financial Crimes Enforcement Network (FinCEN). The full report is available at <http://www.fincen.gov/sarreviewissue6.pdf>

IN THIS ISSUE

- **IS IT REAL, OR...**
Better check fraud detection... 3
- **GOING THROUGH THE MOTIONS**
Importance of posture.....4
- **GETTING EVEN**
Recovering stolen assets.....5
- **THE CON'S LATEST PLOY**
Law-enforcement successes
from around the country..... 7

Michael Comer
Cobasco Group, Ltd.

HOW TO CATCH FRAUDSTERS IN THE LIES THEY TELL



One thing all fraudsters have in common: They all lie. From an employer's point of view, this is actually good news.

Reason: Because fraudsters start lying from the minute they walk into a job interview, you can often spot them if you know what to look for. That can be the key to avoiding a hiring decision you'll later regret.

Example: An applicant was asked "Have you ever used narcotic drugs such as cocaine, crack or heroin?" He answered: "No."

"Or cannabis, LSD or ecstasy?"

"Not that I can recall."

"But you have experimented with them?"

"Yes, but I did not inhale."

"Then why didn't you volunteer that information when I first asked you?"

"Because you only asked about cocaine, crack and heroin."

Red flag: The applicant interpreted questions and delivered subjective truths—not precise, honest and forthright answers. An exchange like this during a job interview lets you know up-front that the person before you is likely to lie and might not hesitate to defraud the company.

LYING MATTERS

If you don't catch liars during the pre-employment process, don't worry—you'll have plenty of opportunity while they're working for you to gain insight into their true character.

Liars lie while performing normal job duties...during performance reviews... at networking functions...in project meetings...and everywhere else.

Key: Understand how, why and when

they lie and you'll have a chance of getting them out before they wreak havoc in the workplace.

TWO TYPES OF LIES

Two primary types of lies told by fraudsters at different stages of a crime...

• **Achievement lies.** Told prior to committing a fraud, these lies aim to achieve a financial benefit—and typically involve a story completely fabricated by the fraudster. He or she chooses the time and the place to lure a co-worker in and shares minimal details about the scam he or she is trying to pull off.

Example: "Too-good-to-be-true" schemes, where doing something simple for an employee will result in major benefits. *Employee to boss:* If you can just give me access to the computer system for one hour, I can save the company \$2 million.

Key: Stop achievement lies from resulting in fraud by questioning the liar, probing for specific details about the proposed scheme and insisting on documentation or other backup. If a fraudster who told an achievement lie gets the sense that the chances of success aren't in his or her favor, he'll move on to another victim, another time or another place/method.

• **Exculpatory lies.** These are the lies a criminal tells *after* a fraud has been committed, in an effort to...

Permanently remove suspicion or stop a suspicious employer's or investigator's questioning. Fraudsters typically do this by verbally or physically attacking the interrogator and/or launching a high-intensity initiative to convince you of their innocence.

□ Escape—feeling he or she has resolved the situation without incriminating himself. *Example:* “Well, you know I didn’t take the money from the safe. I don’t even know the combination.”

□ Find out what you know about the fraud so he or she can plan appropriate action to deflect suspicion—or flee. *Example:* “Which vendor did you say the thief was in cahoots with? I saw the electronic delivery guy hanging around the back entrance last week for a really long time...”

□ Minimize the penalties, if there is no escape. *Example:* “Yeah, I took a little extra money out of the till a few times, but it’s because I have terminal cancer and I couldn’t otherwise afford to pay for treatment...”

□ Frustrate follow-up action by further attacks, often on grounds of racial, sexual or another form of alleged discrimination that throws the interrogator off track.

□ Resume the deception as soon as he or she believes it is safe to do so.

THE TRUTH ABOUT LIARS

Most fraudsters tend to be non-judgmental when it comes to the personalities and behaviors of others...have no clearly ingrained beliefs or morals...and assume everyone else is as dishonest as they are. In fact, their suspicious nature—leading to finger-pointing and suggestions of additional crimes committed by others—is often one of the indicators that they are distorting the truth during an investigation.

More qualities liars tend to share...

•**They refuse to commit to an answer.** Liars rarely answer questions with a simple “yes” or “no.” Instead, they waffle, pad and qualify their answers in an effort to avoid bold-faced lies.

Examples: Prefacing remarks with clauses like “To the best of my recollection...” “I want to say...” “Don’t hold me to this, but...”

•**They’re incapable of answering questions as an innocent person would.** Truthful individuals are usually confident about their innocence and therefore willingly offer candid explanations for their behavior.

When asked if he or she has, say, stolen money from the company, an innocent person will typically reply with a straight “No,” or “I did not do it”. Liars asked the same question tend to offer pseudo-denials of guilt by...

□ Answering subjectively, saying “There isn’t a shred of evidence or proof

that I took the money.”

□ Side-stepping flat-out denial, “If I had taken the money, do you think I’d admit it?”

□ Answering from “inside” the heart or mind, “I know in my own heart/mind that I’m innocent.”

□ Making guilt seem impossible, “I couldn’t have taken the money because I don’t have keys to the office!”

□ Answering by using odd language, like the conditional passive voice, “I would not steal from the company.”

•**They say too much.** Liars always know just a bit too much about crimes in the workplace, and they often give their knowledge away in an effort to reduce their own anxiety about being questioned about a crime they committed.

Example: Sensitive files were stolen on a Saturday from a storeroom in a company’s office. Employees were told only that “information” had been stolen over the “weekend” and asked to write down everything they knew about the thefts. One statement said: “I had nothing whatsoever to do with the removal of the files and I can account for every second of my time last Saturday 14th.” This thief knew and said too much, and he later admitted his guilt.

•**They provide inconsistent details.** Caught up in the mental space between memory and imagination, habitual liars often convey information using the past and present tense in the same sentence. Or—they leave key details out while inserting mundane and irrelevant details.

Example: In answering questions about the unusual way he’d parked his white Bronco on the night his ex-wife was murdered, O.J. Simpson explained, “Well, it’s parked because...I don’t know if it’s a funny angle or what. It’s parked because when I was hustling at the end of the day to get all my stuff, and I was getting my phone and everything off it, when I just pulled it out of the gate there...it’s like a tight turn.” Among other things, the change of tense throughout the answer and the odd use of the preposition “off” instead of “from” suggest Simpson was probably lying.

Important lesson: It’s close to impossible to memorize all the signs of deception that give fraudsters away. Instead, let your senses and

WHITE-COLLAR CRIME FIGHTER

Editor
Peter Goldmann
Consulting Editor
Jane Y. Kusic
Managing Editor
Juliann Lutinski
Senior Contributing Editor
Linda Stockman-Vines
Associate Editor
Barbara Wohler
Design & Art Direction
Ray Holland, Holland Design & Publishing

Panel of Advisers

- Credit Card Fraud**
Barry F. Smith, BFS (Bankcard Fraud Solutions), Inc.
 - Audit & Risk Management**
Steven I. Adler, Senior Auditor, Health Net Inc.
 - Victim Services & Support**
Debbie Deem
Financial Crime Victim Advocate
 - Corporate Fraud Investigation**
Barry Brandman, Danbee Investigations
 - Corporate Integrity and Compliance**
Martin Biegelman, Microsoft Corporation
 - Securities Fraud**
G.W. “Bill” McDonald, Investment and Financial Fraud Consultant
 - Prosecution**
Phil Parrott, Chief Deputy District Attorney Denver District Attorney’s Office, Economic Crime Unit
 - Computer and Internet Investigation**
Donald Allison, Senior Consultant Stroz Friedberg LLC
 - Public-Private Sector Cooperation**
Allan Trosclair, Former Executive Director, National Coalition for the Prevention of Economic Crime
- 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: \$275/yr. Canada, \$299. Copyright © 2004 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 prosecuting economic crime.

This community includes law enforcement officers...regulatory officials...corporate security professionals...business owners and managers...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.

intuitions run free while focusing on and listening to employees...decide whether a suspected lie is dangerous to the company, and—if it is—plan an interview strategy to catch the liar. (For guidance on picking up the *non-verbal* signs of deception, see page 4.) 🚫

White-Collar Crime Fighter source:

Michael Comer, Managing Director of Cobasco Group Limited (www.cobasco.com), fraud and compliance consultants specializing in helping corporate clients prevent, detect, investigate and recover from fraud. He is the author of several books and E-books on fraud, including *Deception At Work*. Mike can be reached at comer@btinternet.com.

Computer Forensics for FREE

Knoptix is a Linux-based open source CD enabling examiners to conduct complex hard drive examinations at no cost.

With Knoppix, you simply pop the CD into a suspect's PC and bypass Windows passwords and logging applications... and get access to the hard drive.

Added advantages: Knoppix requires no installation and includes an astonishing variety of forensic tools and applications for examining files.

Example: Your company's fraud examiner receives a tip during a routine audit that John, a purchasing manager, has been taking bribes from a preferred customer. Sam needs to search John's PC but John has installed software that logs all system activities, and he frequently changes his password.

Solution: Sam has a secret weapon. With authorization from the company's legal counsel, he enters John's office one night, slips his Knoppix CD into John's PC and pushes the "on" button. Sam is able to view spreadsheets, database information, and E-mail correspondence...and copy suspicious files to his USB keychain drive.

John never has a clue that an examiner was inside his PC. With Knoppix, Windows never boots and his logging program passwords are useless. His disk timestamps aren't updated because the disk is accessed in read-only mode.

White-Collar Crime Fighter sources:

- Conan C. Albrecht, PhD, Assistant Professor of Information Systems at Brigham Young University, Provo, UT, writing in *The White Paper*, Association of Certified Fraud Examiners. Professor Albrecht can be reached at conan_albrecht@byu.edu.

- Art Bowker, computer crime specialist, US Probation Office, Cleveland, OH and author of *Knoppix First Responder Guide for Law Enforcement and Corrections Officers*, arthur_bowker@ohnp.uscourts.gov. The manual is available at www.linux-forensics.com/forensics/knoppixManual.pdf.

To get a copy of the Knoppix CD, visit <http://www.knopper.net/knoppix-vendor/s/ind-ex-en.html>.

IS IT REAL, OR...

Judy Krasnow
Romark Fraud Prevention Services

CHECK FRAUD

How to Improve Counterfeit and Forgery Detection

To identify fraudulent checks, travelers checks, money orders and other payment instruments, employees in charge of handling these items must be trained to recognize as many of the staggering number of check fraud techniques as possible...as well as the numerous types of check-related transactions that can be presented.

Key: A major reason for the large and growing number of undetected fraudulent checks is that financial institution employees tend to view individual check transactions the way they know they are supposed to be... rather than the way they are.

Example: If you've ever tried to proofread your own written work, you've undoubtedly had the experience of reading through a document several times, and determining that it's perfect, only to later discover that you overlooked a typo or a repeated word.

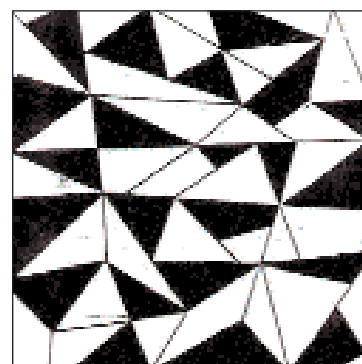
Cause: Our eyes play tricks and tell us we see things the way we expect them to be—not the way they are...so we unconsciously overlook things that we should notice. This can of course be extremely costly when a bank teller or other check-handling employee is so used to seeing routine transactions go through without a glitch that he or she isn't properly trained to detect suspicious details about a check when it is presented.

SEE FOR YOURSELF

In the mosaic design above, there is a perfect five-point star. Many people have a difficult time finding it and some will never see it unless it is pointed out to them. The reason you can't spot the star right away is the same reason most employees who process

check transactions miss the clues that a check is fraudulent: They don't *expect* to see a star, so they don't see one.

Key: The same principle applies when looking at a check. We see what appears



to be a legitimate check because that's what we're used to seeing.

Critical: That's why so many bad checks are passed. The counterfeiter creates a check based on his or her perception of what a check looks like and the inattentive or untrained acceptor "sees" a perfectly good check—despite glaring flaws.

CHECK BASICS TELL ALL

The layout of legitimate checks is not random. The numbers and other identifying characters on valid checks are placed in specific places, for very specific purposes, including compliance with federal regulations. Fortunately for fraud investigators, these details are often overlooked by check fraudsters. While creating bogus checks on their computers, fraudsters include "the five parts of a check," which are taught to almost all new tellers as key factors for determining if a check is good or not.

Challenge: While tellers, retail

Continued on pg. 4

GOING THROUGH THE MOTIONS



The Importance of POSTURE in Suspect Interviews

Experienced fraud investigators are intimately familiar with, and use, the intricacies of body language when interviewing subjects. *Some of the most important posture subtleties include...*

•Dynamic vs. static posture. The degree of change in the subject's posture during a 30- to 40-minute interview tells a lot about guilt and honesty. Truthful subjects usually exhibit a variety of postures throughout the course of an interview. These postures—crossing legs, gesturing, leaning forward to emphasize a point—are always natural and appropriate for the subject of conversation.

Contrast: Deceptive subjects often assume an initial posture and maintain it for the duration of the interview.

Theory: The subject is exerting so much thought and energy to generate convincing responses to the interviewer's questions, that nonverbal communication becomes frozen. A static posture clearly reflects a subject's lack of confidence.

Exceptions: Dishonest interviewees sometimes reinforce suspicion with posture changes that occur "on cue" to a question. Crossing or re-crossing the legs...or using the hands to momentarily lift or shift the body in the chair are signs for the investigator to watch for during two key points in the interview...

□ **Before the subject answers a question.** *Example: Did you leave your house at all that night?* If the subject shifts in his or her chair before answering with *No, I really had nowhere to go so I stayed home*, this is a red flag.

□ **During the subject's verbal response.** *Example: Were you experiencing any financial difficulties last month? Nothing out of the ordinary (shift in chair) that I can recall.*

•Forward vs. retracted posture. When a subject leans forward in the chair during a response, he or she is non-verbally reinforcing the verbal content of the response. This often occurs with truthful subjects during early portions of the interview.

As the interview progresses, honest subjects will assume a more relaxed and comfortable posture in the chair.

Contrast: Deceptive subjects often lean forward in the chair throughout the entire interview. This behavior expresses an attitude of challenge... similar to the deceptive subject who stares at the investigator throughout the interview.

Retracted posture is characterized by constraining hands and/or feet. The subject's feet may be pulled up under the chair, or tucked behind the front legs of the chair.

Result: The subject cannot lean forward to reinforce a verbal response.

As for hands, deceptive subjects often sit on their hands or keep hands wedged between the knees.

•Frontal alignment. A truthful subject exhibits high levels of interest and emotional involvement during an interview. To communicate with the interviewer the interviewee will line up his or body with that of the interviewer.

Contrast: A deceptive subject may turn his or her legs and hips away from the interviewer, conveying a lack of interest and emotional detachment.

•Leg-crossing "tells." At the beginning of an interview, when anxiety levels are highest and critical questions are being asked, most truthful subjects will have their feet flat on the floor. As the interview progresses, and the subject realizes that the investigator is not accusatory or aggressive in his questioning, truthful subjects typically cross their legs—indicating a relaxed frame of mind.

Contrast: A guilty subject is likely to start out the interview with crossed legs.

But—unlike honest interviewees, the deceptive subject's leg cross is often tense and restricted.

Example: The subject grabs the ankle of his or her crossing leg to bring it up higher on the thigh. 🚫

White-Collar Crime Fighter source:
Evaluating A Subject's Posture During An Interview, John E. Reid Associates, loss prevention and corporate security consultants and trainers, Chicago, IL, www.reid.com.

Truthful subjects usually exhibit a variety of postures throughout the course of an interview

Continued from page 3

cashiers and other check acceptors are taught to recognize these five parts—maker, date, payee, amount and payor

Our eyes play tricks and tell us we see things the way we expect them to be—not the way they are...so we unconsciously overlook things that we should notice.

bank—they notice very little else. That is the tremendous advantage the crooks have, and why so many fraudulent checks are passed undetected. Often-overlooked signs of fraud...

- Misspellings.
- Missing payor address.
- Missing MICR numbers.
- Unusual check stock.

Disturbing: In thousands of cases, the fraudsters create a bogus check by using the essential components of a legitimate check but paying no attention to the type of paper that real checks are printed on, or the proper layout or placement of characters. They don't need to because so many fraudulent checks are accepted by inattentive or apathetic payees. The losses are staggering—recently estimated in the billions of dollars each year.

THE IDENTITY THEFT CONNECTION

To cash a forged and counterfeit check, the fraudster usually must steal someone else's identity and make the bogus check out, or endorse it, to the victim which the fraudster poses as, using a phony ID.

Helpful: Many fraudulent checks are so poorly prepared, that they are "screaming" to be spotted as phonies.

On the adjacent page are two examples of actual counterfeit checks that were successfully passed. Had the acceptors been trained to view checks differently than they were accustomed to, they could have easily recognized the glaring flaws that each of them possesses, and large losses could have been prevented.

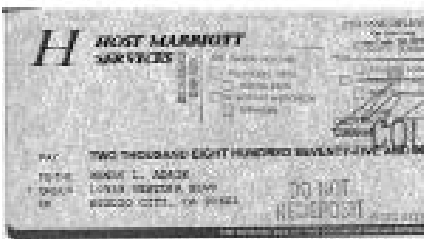
Key: Once tellers or other check handlers have been trained to "see" the flaws by knowing where to look for them, they jump out at them and they wonder why you didn't notice them before.

It should only have taken a few seconds to realize that the checks above were bad. How many flaws can you find? Would you or your employees have accepted these checks? How

Continued on page 5

Continued from page 4

much money could your business lose?
The bottom line: Many employees who work with checks on a daily basis have not been properly trained to



quickly spot the tell-tale signs of check fraud. Unfortunately, as uneducated as the criminals are in the production of legitimate checks, the recipients of their handiwork are too often even

Many fraudulent checks are so poorly prepared that they scream to be spotted as phonies

less knowledgeable.

Management has an obligation to their customers to provide the best training possible to their employees to prevent identity theft through fraudulent check losses.

There are many check fraud training offerings on the market. Be sure to choose one that not only describes the common traits of bad checks, but also trains employees how to *think* differently to avoid missing signs of trouble. ☹

White-Collar Crime Fighter source:

Judy Krasnow, President, Romark Fraud Prevention Services, providers of expert training on how to detect check fraud quickly, without impacting customer service. For additional information and to contact Judy, visit www.romarkfps.com.

Fraud Wisdom...

“There will always be dishonest people in any company. The only way to reduce fraud is to build a culture of honesty and integrity throughout the company.”

—Jack Welch, the legendary Chairman of GE (CNBC interview, 6/6/03)

GETTING EVEN

Ed Pankau, *Pankau Consulting*

How to Recover Stolen Assets Before It's Too Late



Scenario: You're a corporate fraud investigator who recently identified a massive embezzlement. You've helped law enforcement officers execute the arrest and supported the company's attorney(s) in slogging through the prosecution ordeal.

The case is won...with a substantial judgment. All you and the attorney have to do is levy the assets of the guilty party and reap the rewards. Sounds easy enough.

Minor glitch: The guilty party refuses to pay the debt, and the sheriff or constable can't locate sufficient assets to satisfy the judgment. What happens next?

SHOW ME THE MONEY

First step: Depose the perpetrator(s) in a post-judgment discovery action to determine their net worth and then locate the source of assets.

Challenge: During this post-judgment discovery, attorneys and investigators too often learn that the convicted fraudster has already hidden his ill-gotten assets. The criminal has either “relocated” the money offshore or transferred it to other entities, such as a child or family trust. Or—he or she has hidden the loot by using another name, such as the spouse's maiden name.

The good news: Stolen assets can be found in nine out of 10 cases.

EVERY EXCUSE IN THE BOOK...

In 20 years of fraud investigations, I have heard almost every story about how people have lost their assets and now can't pay the judgment. *Typical stories include:* I went to Las Vegas... My wife and I used the money to live on and spent it all...My bookkeeper or accountant stole the money...I lost it all on bad business deals trying to raise

enough money to pay this judgment.

First steps for locating hidden assets that can be seized and used to pay your company's restitution...

- **Determine whether the subjects made large payments on their home mortgages during the litigation**—especially in the last year of the legal proceedings. Many crooks try to hide assets by pre-paying their mortgages to increase the equity in their homes, which they believe to be “bullet-proof” against seizure.

- **Examine payment records of their universal life or whole life insurance policies.** A prepayment can accrue interest just like a savings account and doesn't show up on financial records except inside the insurance policy itself.

- **Look for savings bond purchases**—either in the subject's name, his or her children's names or spouse's maiden name. Until recently, these transactions were not centrally registered and were a favorite purchase of money launderers and drug dealers.

- **Search the fraudster's bank records for cashier's check purchases.** These checks can be purchased and tucked away for the future just like cash.

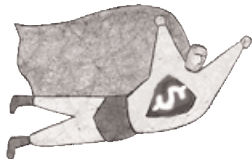
DIGGING DEEPER

When you bring the fraudster to the post-judgment deposition, you'll naturally want his or her attorney to produce the client's financial statements, tax returns and bank statements. Also, question subjects about their income and personal and business assets.

Important: Ask for copies of telephone and cell phone bills...E-mail logs...and travel documents. These are

Continued on page 6

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE



Legislation Would Change Credit Card Chargeback Game: Card Companies Not Pleased

A new West Virginia state bill would force credit card issuing banks to assume much of the responsibility for chargebacks resulting from Internet transactions using stolen credit cards.

The bill is a joint effort by Gary Howell, owner of a local on-line auto parts company, and State Senator Jon Hunter, to protect West Virginia businesses against the growing threat of on-line credit card fraud.

Howell's mission is fueled by an incident in which a "customer" charged \$4,200 worth of automotive parts using a stolen American Express card. Howell was required to cover the chargeback and Amex outright refused to help catch or prosecute the perpetrator.

Key provision: Under the new West Virginia bill, card-issuing banks whose credit cards are fraudulently used to make purchases over the Internet from a West Virginia company would not be allowed to charge the victimized merchant more than \$250 for each fraudulent transaction... unless the issuing bank cooperated in investigating the transaction.

Card-issuing institutions would also be required to report all fraudulent Internet credit card transactions involving West Virginia E-merchants to the state attorney general.

CARD COMPANY CONCERN

The major card companies—Mastercard, Visa, American Express—are decidedly displeased with the prospect of the bill's passage. Each has sent representatives to the West Virginia legislature to lobby against the bill. All three reportedly threatened to pull out of West Virginia completely if the bill does become law.

Potential impact: If the legislation ultimately is enacted, it would represent a powerful protection for West Virginia Internet merchants. As a result, it could attract new businesses that process and fulfill E-commerce transactions for E-merchants.

By one recent estimate, within three years of passage of the bill, E-commerce merchants moving to West Virginia could add up to 30,000 new jobs to the state's economy.

White-Collar Crime Fighter sources:

•Tom Mahoney, Founder and Director of Merchant911.com, an on-line fraud prevention information exchange with about 1,500 E-merchant members. Visit merchant911 at www.merchant911.com.

•Gary Howell, President, Howell Automotive, Keyser, WV; www.howellautomotive.com. Gary can be reached at gary@howellautomotive.com.

New Fraud Risk in Private Company Audits

The new Statement on Auditing Standards—SAS 99—is making it much harder for some companies to get a "clean" opinion. **Reasons:**

•Auditors are no longer allowed to "trust" a client just because it has never had a problem. Why? Because each year's audit stands on its own.

•Auditors are now required to assume that management is overriding internal controls in order to cook the books.

•Auditors are now required to assume that revenue is being manipulated.

•Auditors must now hold a "brainstorm" throughout the audit to predict how and why the client might cook the books.

Warning: Commercial lenders must be aware that because the tough new SAS compliance standards are boosting audit fees by 15% to 20% for private companies, a few businesses will fire their auditors and use desktop publishing software to create their own "clean" opinions.

Result: To avoid problems down the road, commercial lenders must confirm prospective borrowers' "clean" opinions with the borrower's auditor.

White-Collar Crime Fighter source:

Gary D. Zeune, CPA, is the founder of The Pros & The Cons, the only speakers' bureau in the United States for white-collar criminals. He teaches fraud prevention classes for the FBI, the U.S. Attorney, more than 30 state and national CPA societies, and numerous banks and accounting firms. He can be reached at 614-761-8911, gzfraud@bigfoot.com or via his Web site at www.bigfoot.com/~gzfraud.

Continued from page 5

among the most frequently overlooked areas of discovery because attorneys sometimes don't fully understand the process of investigation.

Key: Places an individual has visited and whom he or she has spoken with or received E-mails from is often more valuable than recent business activity or where financial assets were when those last financial statements and tax returns were filed.

REVEALING RECORDS

The following documents may be instrumental in locating hidden assets. *They may also help prove the intent to hide assets from the court...*

•**Passports.** Entry and exit visa stamps will disclose trips to money-laundering centers such as Switzerland, the Cayman Islands, the Bahamas, Isle of Man, Netherlands Antilles.

Aim: By documenting cash withdrawals from bank accounts and timing them with trips to foreign countries, you can often discover illegal offshore fund transfers.

Example: I know an accountant who made a trip to the Cayman Islands every month with his scuba gear. It took US Customs three years to figure out his tanks were filled with \$100 bills.

•**Cell phone records.** Standard telephone records only record long-distance calls. Cell phone records record all calls for billing purposes. They may reveal calls to or from undisclosed business partners or a "significant other."

•**Credit card statements.** These are valuable for documenting out-of-town travel and identifying individuals whom your subject has entertained or done business with.

•**Hotel records.** Despite our society's addiction to cell phones, hotel phone records sometimes reveal phone numbers of people the subject wouldn't call from home, such as an out-of-town banker, business associate or accountant.

•**Credit reports.** The trail of credit purchases follows us around the world. Credit reports contain details about a person's credit accounts, including mortgage debt...consumer credit...lawsuits...bankruptcies... payment histories on all accounts... life insurance records and more. You may find nuggets of information to

Continued on page 7

Continued from page 6

help in locating ill-gotten assets.

•**Fax records.** When investigating a guilty party's corporate assets, review the company's fax records to find information concerning foreign business entities, foreign bank accounts and other offshore activities. The monthly fax log or bill will point you in the right direction through the log of calls made from or received by that fax.

•**Overnight shipments.** Almost all of us use Federal Express, UPS, DHL or a similar carrier, to deliver our valuable mail and packages around the world. Examining the trash or the monthly bills for a subject's overnight packages gives a clear idea of the cities and countries that they are doing business in and can always add more information to the discovery process.

The bar coded records of these delivery services can track every package delivered to or from any address or person for up to six months.

All of the records listed are easy to obtain, particularly under a motion to

The good news is that stolen assets can be found in nine out of 10 cases.

produce. If you find that the opposing party is unwilling or unable to gather these documents, consider subpoenaing these records directly from the sources that produced them.

In many cases, once records have been requested, previously stubborn parties suddenly become much more amenable to settling their judgments. If they have anything to hide, they would much rather settle with the plaintiff's legal representative, than produce these records publicly for other creditors to find as well. ☹️

White-Collar Crime Fighter source:

Edmund J. Pankau, President, Pankau Consulting, prominent corporate and government fraud investigators and trainers, The Woodlands, TX, www.pankau.com. Ed can be reached at info@pankau.com.

COMING SOON IN

White-Collar Crime Fighter...

- **How to help employees help you fight fraud**
- **Forensic accounting: The power of digital data analysis**
- **Beating procurement fraudsters at their own game**
- **Public corruption: Top investigator's secrets of busting bad guys**



THE CON'S LATEST PLOY...

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

Miami, FL

It's tax time and the phony tax-preparer rings are in full swing.

Fourteen South Florida individuals were charged in eight indictments with presenting, or conspiring to present, fraudulent tax returns to the IRS, and/or preparing and assisting in the preparation and presentation of fraudulent tax returns to the IRS.

Eight additional Floridians, charged in three indictments with a variety of tax fraud offenses, pleaded guilty.

In total, the 22 defendants filed more than 1,700 false tax returns, generating about \$4.1 million in illegitimate refunds.

The defendants are accused of recruiting immigrants and the working poor with promises of big tax refunds. Most of the returns under-reported the taxable income and/or inflated the number of deductions and dependents.

Other cases involved identity theft or submitting false earnings statements. Fourteen of the defendants pleaded guilty before federal judges to various conspiracy charges relating to preparing and presenting false returns to the IRS. The remainder have either pleaded guilty or agreed to do so.

One of the defendants is Landa Mojica, 41, of Miami, who alone is charged with filing more than 500 fraudulent returns, resulting in more than \$1.5 million in refunds. Mojica was charged with eight counts of filing false claims.

Dead giveaway: The IRS was first alerted to two of the bogus tax preparers when its Questionable Refund Detection Team's computers in Atlanta picked up several suspicious returns that all reported the same income and same amount of taxes withheld.

The bust: The IRS set up an under-

cover sting operation. One defendant told an undercover agent to expect a \$4,000 tax refund if he could "find some kids" to claim as dependents.

Denver, CO

The fine art of stealing from steel building customers.

General Steel Corp. was sued by Colorado Attorney General Ken Salazar for, among other things, misrepresenting itself as a manufacturer of steel buildings and falsely advertising factory-direct clearance sales.

Details: In a lawsuit filed in district court, the Colorado AG charged General Steel with using deceptive marketing schemes to sell expensive manufactured steel buildings to customers in Colorado and throughout the United States.

General Steel allegedly used national radio, television, direct mail and Internet advertising to get prospective customers to call for details about discounts on "clearance" buildings.

Callers were greeted by sales representatives who were literally trained to pretend that the customer's phone call was somehow transferred to an employee who did not normally handle sales. Claiming to be from "production" or "shipping" or another department within the company, the "employee" would explain that while General Steel does not normally sell direct to the public, there "apparently" were some "clearance" buildings available for sale at big discounts.

In following the clever social engineering script provided by General Steel, the "sales rep" would then offer to "call down to the plant" to determine whether any of the "clearance" buildings remained.

During the initial sales call, the salesperson avoided answering the caller's questions by claiming that because he or she didn't normally handle sales, answers to the questions would have to come from someone else in the company.

However, during the call, the salesperson would ask for the dimensions of the building the caller was seeking to purchase.

The salesperson would then return to the phones to take new incoming calls from "customers."

Sometime later, he or she would call back the first caller and misrepresent that he or she had inquired about the "apparent" clearance buildings. The salesperson would say that while many of the clearance buildings had been sold, a few remained. Of the buildings listed by the salesperson as available, one was "luckily" very close to the size of the building needed by the caller.

Next step: The salesperson would explain that the "clearance" building was available for 50% or more below the regular price. The building is described as a "leftover" unit, such as one that had been purchased by "some dot.com company that went bankrupt"...or as being one of 20 previously purchased by a large aircraft company that changed its delivery order at the last moment.

The salesperson would imply or

directly explain that unless the customer immediately placed a deposit, "claim" or "hold" on the clearance building the opportunity to get the deep discount would be gone.

Result: General Steel's "top sales rep", Jeff Donelson allegedly made more than \$3 million in one year by such deceptive practices.

Added problem: As part of the deception, customers were asked to sign contracts for the "clearance" buildings requiring buyers who subsequently cancelled the order to pay 60% of the total building price.

Reality: According to the AG's lawsuit, General Steel doesn't even sell clearance buildings, existing buildings or ready-to-ship buildings as its boiler room operators claimed. Instead, General Steel sells buildings that it orders from manufacturers of steel buildings only after General Steel secures a deposit on the order.

The AG's lawsuit asks for an injunction against General Steel as well as "any such orders as [the] court may deem just and proper to effectuate the purposes of the Colorado Consumer Protection Act."

Topeka, KS

Convention fraud: How science fiction expo became subject of real-life fraud. Slanted Fedora

Entertainment and its owners, Jackie and Dave Scott, were sued by Kansas Attorney General Phil Kline for violating the Kansas Consumer Protection Act (KCPA). The alleged violations involve victimized consumers throughout the country. The company faces civil fines and penalties up to \$10,000 for each violation of the KCPA.

Details: The charges claim that Slanted Fedora, an organizer of exhibits and conventions for Star Trek fans, repeatedly cancelled conventions without refunding consumers' deposits...double-charged credit and debit cards, and promoted the appearance of Star Trek television stars who did not show up at the conventions.

The company was previously ordered by the court to shut down its Web site prompting them to refund many consumers who had filed complaints with the Kansas Attorney General and the Better Business Bureau of Kansas City, MO.

Bridgeport, CT

Bank executive's six-year embezzlement refines meaning of "internal controls." George Lopez pleaded guilty to conspiracy to embezzle money from a large regional financial institution, People's Bank.

Details: Until the fall of 2003, Lopez was Vice President in the Operations Department at People's Bank headquarters.

In that capacity, Lopez conspired with other bank employees to embezzle bank funds by, for example, intercepting checks he sent to the bank for payment of his own credit card bills and, as a result, reducing his credit card balances without having funds drawn from his People's Bank checking account.

Lopez also admitted to stealing from the bank's escheatable funds (unclaimed assets held at the bank by the state).

According to the prosecutor, the conspiracy lasted for about six years and involved multiple transactions resulted in losses to People's of nearly \$300,000.

The case was investigated by the FBI and prosecuted by Assistant United States Attorney Brian E. Spears. 🇺🇸



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 \$225. **That's \$50 off the regular subscription price of \$275!**

Plus, send me—for **FREE**—**FIVE** Special Reports on preventing, detecting and investigating 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