

WHITE-COLLAR CRIME

FIGHTER

www.wccfighter.com

VOLUME 11 NO. 2
FEBRUARY 2009

YOUR SECRET WEAPON IN THE WAR ON FRAUD

IN THE NEWS

Information Breach Solution: "Incident Ownership"

Common corporate mistake after an information breach is discovered: Failing to immediately make one competent manager fully accountable for remediation and provide him or her with the authority to execute all necessary actions.

Results: In a large organization, each business line will attempt to initiate its own remedial steps and failure will result from lack of coordination.

Essential: The accountable manager must have the authority to force leaders from each business line to work under his or her lead to coordinate planning for a clear and efficient organization-wide response.

Important: Ensure that the manager in charge of response can *require* needed personnel such as IT security and other technology professionals to stick with the remediation program until it is complete. Often, companies ask these professionals for their help, but before the task is completed, they say their "regular" workload is piling up and they must excuse themselves.

Key: With a "throat to choke"—i.e., a person whom top management can "put the screws to" when a breach is discovered and urgent action is needed—the organization has the best chance of minimizing damage from a security incident.

White-Collar Crime Fighter source:

Kevin Mandia, Mandiant Corp., information security consultants, speaking at Black Hat 2009 conference in Washington, DC. He can be reached at 703-683-3141.

IN THIS ISSUE

• DANGER IN DENIAL

Can management afford to ignore the fraud threat?.....3

• AUDIT ISSUES

Pivotal legal opinion..... 4

• LESSONS FROM THE TRENCHES

The casino business on employee fraud prevention..... 5

• THE CON'S LATEST PLOY

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

Janet Mielke Schwartz, PhD, *Forensic Fraud Research, Inc.*

Minimizing Fraud Is Not Hard: How One Company Does It



It is common knowledge that employee fraud increases during tough economic times. But this period of economic weakness is unique in that it may largely have been brought on by high-level fraud. This is why public trust in corporate America is eroding.

The good news is that there are companies out there that continue to do well while strictly adhering to basic principles of ethical conduct, where earning a profit is not a justifiable means to an end and where fraud by insiders or outsiders is demonstrably prohibited.

For these organizations, the "perp walks" of high-profile corporate titans that many prosecutors predict in the wake of the stunning financial catastrophe of 2008-2009, will seem almost incomprehensible.

A MODEL OF VIRTUE

Welcome to Shearer's Foods, Inc., a mid-sized family-run snack food maker, completely lacking in the glitz of the likes of Apple, Google, GE or Disney.

But scratch below the plain-Jane surface and you see a model of corporate prowess that members of any major stock exchange would envy.

This is a progressive company that has been led by CEO Robert J. Shearer and his dynamic management team to the status of one of the fastest growing snack food manufacturers in America. With worldwide distribution, the award-winning Brewster, OH-based firm

employs approximately 700.

Most impressive, though, from the standpoint of business integrity is its solid grounding in core values that have stood the test of time for 35 years.

FRAUD-DETERRING LEADERSHIP

Bob Shearer and his brother, Tom, Vice President of Business Development, started working in the original family grocery store when they were 10 years

old. Rung by rung, they worked their way up the company ladder by honoring their roots, staying true to company values, adding busi-

ness partnerships and making the necessary decisions for expansion. But, an in-depth look at the company's policies and practices reveals a culture that produces a no financial fraud result.

Like most successful business owners, Bob Shearer is supremely comfortable with his own authority. But he has other qualities that set him apart from many of his peers. *He...*

- Is progressive, yet naturally humble.
- Is a man of high expectations for himself and for others.
- Enjoys people and has a natural capacity to bond.
- "Walks the talk" regarding business and social integrity.
- Insists on all behavioral standards being set at a level of excellent...and to be adhered to at all costs.
- Is flexible and adaptable, but holds people at all levels and in all positions

accountable for their actions.

- Easily shares power. When the company experienced major growth in the early 2000s, Shearer created the company's first management team, and then empowered it to step into roles he had held exclusively for years.

HIRING PRACTICES REDUCE FRAUD RISK

Shearer's Vice President and Corporate Controller, Alan Fritts, describes his department as the information clearinghouse for Shearer's Foods. He explains the company's unique hiring process by explaining that, through rigorous screening, candidates must...

- Be highly motivated and energetic.
- Exhibit a strong sense of personal responsibility.
- Possess and value personal integrity.
- Be ambitious.
- Have extensive work experience at a public accounting firm or other business. This ensures that the individual has developed a professional demeanor and has an established work ethic.

Key: The company seeks to have new managers step in as professionals rather than just bosses collecting a nice salary.

There may be four interviews in total before the decision to hire is

made. The final interview is usually in a casual atmosphere—over lunch or dinner with three of the management team in addition to Bob Shearer himself. On many occasions, spouses are included in the final interview to make sure they are comfortable with Shearer's culture.

Aim: To get to know the candidate from a dimension other than the one he or she presents within the office. Shearer's wants to see humor, humility and natural intelligence.

COMPANY CULTURE

Shearer's Foods expects a lot from its

There may be four interviews in total before the decision to hire is made

associates and many of them work far more than 40 hours a week. However, while the expectations are high, so are the rewards—both material and non-material. Shearer's works diligently to ensure that its associates are paid at or more than market rates for their level of expertise.

In addition, workforce development is ongoing and this is the way to advance within the company. Alan Fritts considers himself more of a coach and mentor than a boss.

Important: Unlike many, if not most, corporate cultures, the one at Shearer's is devoid of toxic competitiveness. It only encourages competition with oneself. Learning is continuous, and the environment is casual, creative and fun.

FOCUS ON THE INDIVIDUAL

Shearer's ensures that its associates feel a sense of equality within the company. This absence of hierarchy is achieved through several practices. Every month there is a birthday lunch or breakfast for employees and everyone attending is greeted by name. While Bob Shearer may not personally know the name of each employee, he expects at least one other member of the management team to know the name of any given employee attending.

Associates are expected to attend four "State of the Company" meetings each year. During these events, associates are informed about trends and latest details about the company's progress and finances. Management openly explains the company's current condition and employees are encouraged to share comments, questions or ideas for

WHITE-COLLAR CRIME FIGHTER

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

Panel of Advisers

- Credit Card Fraud**
Tom Mahoney, Merchant 911.org
- Forensic Accounting**
Stephen A. Pedneault, Forensic Accounting Services, LLC
- Fraud and Cyber-Law**
Patricia S. Eyres, Esq., Litigation Management & Training Services Inc.
- Corporate Fraud Investigation**
R.A. (Andy) Wilson, Wilson & Turner Incorporated
- Corporate Integrity and Compliance**
Martin Biegelman, Microsoft Corporation
- Securities Fraud**
G.W. "Bill" McDonald, Investment and Financial Fraud Consultant
- Prosecution**
Phil Parrott, Deputy District Attorney Denver District Attorney's Office, Economic Crime Unit
- Computer and Information Security**
Kenneth Newman, CISM
Secure PIKE
- Fraud Auditing**
Tommie W. Singleton, PhD
University of Alabama at Birmingham

White-Collar Crime Fighter (ISSN 1523-0821) is published monthly by White-Collar Crime 101, LLC, 213 Ramapoo Rd., Ridgefield, CT 06877. www.wccfighter.com. Subscription cost: \$295/yr. Canada, \$345. Copyright © 2009 by White Collar Crime 101, LLC. No part may be reproduced without express permission of the publisher.

Mission Statement

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

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

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

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

Simple, Powerful Anti-Fraud Measure

Give people overlapping spheres of trust. This is what security professionals refer to as *defense in depth*. It applies in any situation where people are trusted to handle the organization's secured assets.

Examples:

- Requiring two signatures on corporate checks over a certain value.
- Requiring bank tellers to obtain management overrides for high-value transactions.
- Double-entry bookkeeping.
- The hundreds of guards and cameras at casinos.
- Requiring bank employees to take their two-week vacation all at once—so their replacements have a chance to uncover any fraud.

And—in a national security context: Having two people with two separate keys to launch nuclear missiles.

White-Collar Crime Fighter source:

Bruce Schneier, leading information and computer security consultant, and chief security technology officer for BT Group, writing in *The Wall Street Journal.com*, www.wsj.com.

progress or improved operations.

THE FRAUD FACTOR

Bob Shearer claims that his company experiences no material financial fraud. Though it is difficult to definitively confirm this, it is not Shearer's style to sugarcoat the facts.

And this is consistent with his policy for handling those minor fraud offenses that do occur: They are immediately addressed and those involved are held accountable.


Example: If a plant associate failed to clock out prior to taking a break, this would come to the attention of Human Resources. HR would investigate to determine the root cause.

Important: Discipline for the offense may include termination, not just for the associate, but also for the supervisor who allowed the work environment to deteriorate to a point where an employee would think he or she could get away with the crime.

Moreover, if an associate falsely indicates that he or she completed an assignment, the associate is shown the door. The incident is then discussed among the associate's team only.

Result: Associates learn that their actions have consequences. This consistently enforced approach reinforces the sense among long-term employees that the company is fair in all situations.

Finally, in seeking to deter fraud, Alan Fritts places great faith in the Fraud Triangle. Donald J. Cressey's hypothesis that, opportunity, motivation and rationalization explain why individuals commit fraud is common knowledge among accountants and auditors. Fritts feels that while management may not be able to do anything about the external pressures in an associate's life, Shearer's can make sure that no one is over-worked and that their attitudes at work are positive.

As for opportunity, Shearer's executives know that it is impossible to eliminate all vulnerabilities to fraud. Yet, Shearer, Fritts and the rest of the management team believe that the controls they do have in place are effective, not only as stand-alone preventive measures, but also because of the reduced pressure and need for rationalization that the company's culture creates. 

White-Collar Crime Fighter source:

Janet Mielke Schwartz, PhD, DABFE, DACFM, DABPS, FACE, President, Forensic Fraud Research, Inc., a Canton, OH-based consulting firm assisting law enforcement in white-collar crime investigations, www.whitecollarcorruption.com. Jan can be reached at janschwartz@mac.com.

DANGER IN DENIAL

CORPORATE COMPLACENCY

Can Management Afford to Continue Ignoring the Fraud Threat?



According to research released just prior to the full-blown meltdown of the financial markets by the anti-fraud consulting firm, Protiviti*, management at a majority of organizations is still surprisingly complacent about the threat of fraud.

Example: The Protiviti study determined that only 49% of executives believe their organizations' strategies for addressing fraud risk are "very well defined."

Translation: Less than one-half of organizations proactively identify fraud risk and have anti-fraud programs, policies and controls in place that are monitored and enforced by the board and senior management.

Similarly, a Deloitte Forensic Center survey** concluded that only 41% of executives considered their companies to be "more effective" in the area of fraud control, compared with the remaining 59% who described their organizations' fraud control efforts as "less effective."

While Deloitte notes that companies overall have in recent years enhanced their efforts to implement effective anti-fraud measures, a substantial "fraud control gap" is still glaringly evident from the data collected.

Disturbing implication: Six-plus years into the Sarbanes-Oxley "era," and now in the throes of the worst financial and economic catastrophe since the 1930s, most companies are still highly vulnerable to fraud of all kinds, and management appears to show little intention of "tightening" up its anti-fraud defenses. In fact, as recession-phobic executives slash budgets for

anti-fraud training, internal audit and security, the opportunities for fraudsters to exploit softened anti-fraud defenses are growing.

SHORTSIGHTEDNESS IS RISKY

Unfortunately, despite the increasingly urgent warnings about the spike in fraud during economic downturns, fraud remains an issue most managers still find easy to ignore. Why? Because fraud is unpleasant...investing in fighting it has no immediately quantifiable

Only 49% of executives believe their organizations' strategies for addressing fraud risk are "very well defined"

ROI...and it is desirable—indeed reassuring—to assume that the organization is so well managed that it is at minimal risk of being victim-

ized by fraud. Moreover, many executives of large public companies have convinced themselves that the multi-millions spent on SOX compliance is more than enough to protect them against major fraud.

WRITING ON THE WALL

Problem: For anti-fraud professionals, the writing on the wall just keeps getting clearer and clearer. As the fraudsters continue to keep a step (or three) ahead of them, it matters little whether or not another Enron-type disaster hits the headlines.

The fraud epidemic in America will slowly but surely claim more and more victims. And more often than not, we can be sure that those victims will be the organizations that persist in believing in their inherent invulnerability.

A BETTER WAY...

The FBI's recent announcement of its accelerated shift of investigative

Continued on pg. 4

Pivotal Legal Opinion Could Impact Legal Liability of Auditors in Fraud Cases

Parmalat, the Italian dairy products company that went bankrupt in 2003 under the weight of a \$16 billion accounting fraud, continues in its reorganized form to wield potentially significant influence over US law governing liability for failed audits of companies tainted by fraud.

Details: According to an amended shareholder complaint in the case, filed in 2004 by former Parmalat investors, "Among the most notorious participants in the Parmalat fraud were its outside auditors, Grant Thornton and Deloitte. For more than a decade the Company was able to conceal massive losses and huge accumulations of debt. Yet, Parmalat was not flying solo in constructing the way its financial health was presented to investors. Its auditors, Grant Thornton and Deloitte, did far more than turn a blind eye to the misconduct: they directly participated in it. Indeed, when forced

to choose between their professional responsibilities as auditors and alienating the Parmalat insiders who controlled their fees, they repeatedly placed their own interests ahead of those of the Company's shareholders, investors and other creditors. Even after Parmalat's collapse, Deloitte and Grant Thornton continued to keep the truth from coming out."

Whether any of this is true remains for a jury to decide. However, subsequent to the filing of this case, Deloitte Touche Tohmatsu (DTT), the parent entity of former Parmalat auditors, Italian-based Deloitte SpA, filed a motion arguing that it had nothing to do with the audit of Parmalat, and that only Deloitte SpA was involved in the case.

Unfortunately for DTT, the presiding judge in the case, Judge Lewis Kaplan of the US District Court for the Southern District of New York,

ruled at the end of January that DTT could not be dismissed from the case because it has not shown that it is separate from its Italian affiliate.


Specifically, Judge Kaplan's rather direct opinion stated, among other things that, "...it is uncontroverted that several [Deloitte & Touche-US] partners hold key leadership positions at DTT, including the position of Chief Executive Officer, and that DT-US, through loans and outright contributions provided a large portion of DTT's funding. There is evidence also of at least one instance in which DT-US may have influenced DTT's decision-making."

Important implication: If the underlying lawsuit against DTT turns out in favor of the plaintiffs, it will set a new legal standard for audit firms with

The Kaplan opinion does represent an important indicator as to the liability of audit firms in cases where their clients have perpetrated massive financial statement frauds

regard to their liability in failed audits due to fraud. Specifically, if an overseas affiliate of a US-based audit firm is shown to be culpable in perpetuating a financial fraud at one of its clients, the entire audit firm of which it is a part could be held liable.

Of course, there is no guarantee that if this standard is affirmed in the upcoming trial, that all such audit cases involving alleged fraud-related audit failures caused by subsidiaries or affiliates of an audit firm will result in liability being placed on the parent firm.

However, plaintiffs attorneys and financial fraud experts concur that the Kaplan opinion does represent an important indicator as to the liability of audit firms in cases where their clients have perpetrated massive financial statement frauds. 

White-Collar Crime Fighter sources:

• Steven Toll, Partner, Cohen, Milstein, Hausfeld & Toll, Washington, DC.

• Memorandum Opinion of Judge Lewis Kaplan in re: Parmalat Securities Litigation, case number 1:04-md-01653-LAK-HBP, filed January 27, 2009.

Continued from page 3

resources from counter-terrorism to white-collar crime investigation is the clearest recent sign that fraud-fighting is fast becoming a national priority. This can only help—as indicated by the tripling in the past two years of the Bureau's number of active investigations of mortgage fraud to over 1,800.

This all begs the obvious question: Why doesn't management see the fraud risk the way the fraud prevention profession—and now federal law enforcement—does? Why is it not obvious to senior management that fraud losses far exceed the financial outlay required to reduce those losses?

After all, as the ACFE's 2008 *Report to the Nation* concludes, the costs of implementing key anti-fraud measures is dwarfed by the savings in fraud losses directly stemming from such measures.

Example: Organizations that implement fraud awareness training, hotlines and other key elements of a Fraud Risk Management (FRM) program are rewarded with a more than 50% reduction in fraud losses.

One major cause of management passivity lies in simple human nature. It is always easy to put off dealing with a risk that is described on paper until it becomes reality—in our world, via a costly fraud.

SWIMMING AGAINST THE CURRENT

Management that wisely chooses to operate counter to this mindset of course immediately earns the reputation of being shrewd and forward-thinking as soon as its anti-fraud actions pay off in the apprehension of one or more would-be fraudsters.

Unfortunately, as already noted, "forward-thinking" is not the preferred corporate attitude when it comes to proactive anti-fraud strategies.

This, despite ample evidence that significant reductions in fraud risk can be achieved by, among other things...

- Conducting annual Fraud Risk Assessments.
- Tightening and vigorously monitoring the effectiveness of all anti-fraud controls.
- Implementing stringent anti-fraud policies.
- Training employees and managers in basic fraud awareness—to enable them to spot red flags before fraud occurs.
- Conducting surprise audits.

Continued on page 5

FRAUD LESSONS FROM THE TRENCHES

Continued from page 4

- Continuously monitoring financial transactions.

PRESSING THE CASE FOR ACTION

So what can those of us who know that an organization with a cavalier attitude toward fraud risk is asking for trouble do to convince management to act before the inevitable occurs?

Peter Callaway, head of the Australian Chapter of the ACFE and a seasoned fraud prevention consultant, says it often helps to regularly bring to management's attention the misfortunes of others—preferably those in the same industry.

In addition, suggests Callaway, internal auditors and risk managers should take every available opportunity to alert top management to the findings of their fraud risk assessments which identify the specific vulnerabilities to serious fraud that must be addressed in order to minimize risk.

Callaway further urges internal auditors to continuously and assertively present to management the above-mentioned comparison of the cost of implementing anti-fraud controls to the much larger potential for fraud losses of up to 7% of revenue.

Additional effective tactic: Have the organization's audit committee exert pressure on the management team to implement anti-fraud measures. In organizations with proactive audit committees whose membership includes individuals with a keen appreciation of the potentially devastating impact of fraud, the leverage that comes along with board membership should be exploited at every opportunity to prod management to move aggressively against fraud risk.

In the succinct understatement of the AICPA Audit Committee Toolkit: "The members of the audit committee should understand their role of ensuring that the organization has antifraud programs and controls in place to help prevent fraud."

White-Collar Crime Fighter sources:

•Peter Goldmann, Editor and Publisher, *White-Collar Crime Fighter*, Ridgefield, CT, www.wccfighter.com.

**Preventing Fraud: Assessing the Fraud Risk Management Capabilities of Today's Largest Organizations*, www.protiviti.com.

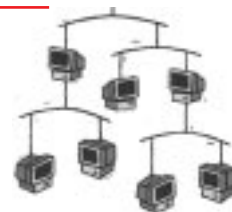
***Ten Things about Fraud, How Executives View the "Fraud Control Gap,"* available at www.deloitte.com/us/forensiccenter.

•Federal Bureau of Investigation, www.fbi.gov.

Note: A version of this article originally appeared in *The Fraud Examiner*, a publication of the Association of Certified Fraud Examiners (ACFE), http://www.acfe.com.

Derk Boss, CFE, CPP, CSP, *DJ Boss & Associates*

Lessons in Employee Fraud Prevention from the Casino Business



As a former casino security executive I have seen my fair share of employee theft and fraud.

As you can imagine, because the casino and hotel business runs on large amounts of cash, the temptation for employees to steal is substantial. But this doesn't make these industries all that different from most others when it comes to fraud. It's just that cash is often easier to steal without having to concoct elaborate embezzlement, kick-back bribery, credit card or check fraud schemes.

Over 30 years in the business, I've learned that theft and fraud *always* exists. You must look for it everywhere, fight it continuously and with every weapon available to you. You must work on the premise that some of your employees and some of your customers and vendors will devise ways to steal from you.

Some of the scams I've seen over the years may help put this in perspective...

CASE STUDY #1

One notable case I investigated illustrates how scams occur because we assume that everyone is watching out for a business's best interests when, in fact, they are not.

Details: Customers received scratch cards while they gambled that they could scratch off to locate cash symbols on the card. If they scratched off three of the same cash symbols they won that amount. Not only was the promotion losing money because people were winning more than expected, the people winning almost all of the money were employees (in many casin-

os, employees can gamble at the casino they work for when they are off duty).

My team's investigation determined that the scratch cards were issued to each department for distribution to players as they met the criteria. We tried to identify the department that was issuing the winning tickets but unfortunately the tickets did not have individual serial numbers for tracking; nor were the departments doing a great job of tracking what they gave

One notable case I investigated illustrates how scams occur because we assume everyone is watching out for a business's best interests when, in fact, they're not

out. (A clear example of management's failure to impose accountability!)

We began to monitor the cashier's cage to see who was cashing in the tick-

ets and soon learned that employees of the Keno department were winning most of the cash awards.

We soon learned that one of the keno employees found that if you held a ticket over a light you could see what was on the card. With that knowledge all the employee had to do was hold each ticket over a light, find the winning tickets, and set them aside. This employee passed the scheme on to co-workers and the free-for-all was on. The employees removed the tickets with the largest cash value and, generously enough, left the lowest cash values for the players.

Fraud prevention lessons learned:

- Ensure that promotional items such as coupons, tickets and gifts are treated as controlled items and as potential cash transactions.

- Anti-fraud accountability must be built into the entire organization. If some-

Continued on page 6

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE



Heartland Breach—Solving the Puzzle

Separating the speculation from what's been reported as fact about the recent Heartland Payment Systems breach leaves some puzzle pieces that are starting to look like a bad picture. *What we know so far:*

- The breach was on-going for more than weeks (the exact number of weeks remains unknown).

- Heartland was unaware of the breach until it was alerted by Visa.
- Heartland processes 100 million transactions a month.
- Data from credit and debit card magnetic strips was compromised.

Problem: These facts lead to the almost inevitable conclusion that a lot of card data was compromised but any numbers would be pure guesses.

A few technical facts offer some perspective...

- The breach was a direct attack on the weakest link—the brief time when card data was being transmitted to the issuers.

- The attack was caused by malware.

- The malware was hidden in an unallocated portion of a disk.

Problem: Security consultants agree that hiding malware in unallocated disk space can happen in two ways. Either the operating system was altered or some device driver software was altered. But even this doesn't tell the whole story. Some portion of the malware needs to be executed, and this can't happen randomly from data bits in unallocated storage space. There must be something resident in memory that accessed the hidden malware in order for the breach to succeed.

Heartland did tell us that the malware was not functioning at the time it was found, but obviously at some point it was.

Key questions: How did the malware get there and how was it able to load into memory and siphon off huge quantities of data without detection?

No matter how it all worked, this points to a big hole in PCI.

Advice to merchants, issuers and acquirers: Keep a very close eye on developments in this case, as you will inevitably be required to make additional security adjustments to mitigate the "Heartland risk" once it has been fully analyzed.

White-Collar Crime Fighter source: Tom Mahoney, founder and director of Merchant 911.org, a leading Internet information exchange for E-merchants seeking to prevent on-line fraud against themselves and their customers, www.merchants911.org.

T&E Fraud Deterrent

One way employees with expense accounts frequently "supplement" their incomes is by fudging their expense reimbursement reports. They may submit "doctored" receipts, receipts for expenses that are not business-related, or receipts for goods or services pre-paid by your organization.

Solution: Make the approving manager financially accountable for the reports he or she approves.

Even better: Start with a policy of zero-tolerance for fraud and then, when you discover a T&E scam, both the crooked employee and the manager who approved the report are fired. (See also page 3.)

For some organizations, this may be too drastic. However, in times like these, when employees are more likely than usual to steal, and when high-profile frauds have eroded public confidence in corporate management, there is more reason than ever to force responsible managers to stand behind their actions.

Potential alternative: Require dual approval of T&E expense reports over a certain amount. The second approval comes from the manager of the first approver.

Key: When the initial approving manager knows his or her boss is also going to review the report, he or she may take the approving responsibility more seriously.

White-Collar Crime Fighter source: e-AP News, E-newsletter from Crystallus Inc., publishers of Accounts Payable Now and Tomorrow newsletter, www.ap-now.com.

Continued from page 5

thing goes wrong you must be able to identify where it is going wrong...and who is in charge of the targeted department so that he or she can be trained, re-trained or disciplined.

Important: For accountability to effectively reduce fraud, your organization must be aggressive in ensuring that the necessary anti-fraud controls are in place to begin with so that department heads and other accountable individuals can't use the excuse that they didn't know what the company's policy was.

CASE STUDY #2

The next case made me realize how much damage can be done by an employee working in collusion with outsiders.

As in many businesses, casinos use loyalty programs much like the airlines' frequent flier programs. Depending on how much time and money patrons spend, they can earn enough points for complimentary meals, beverages, rooms, and can even redeem points for cash. Casinos pour immense amounts of money into these programs to attract and retain big-spending players.

This scam was discovered through a combination of loss prevention techniques and luck.

Details: For those who are not gamblers, casino table games personnel rate players based on the average amount of their wagers, their skill level, how long they play, and the type of game they play (Blackjack, Craps, etc.). These ratings determine a player's "worth" to the casino and establishes the value of "complimentaries" (comps) that players will receive.

We had on previous occasions detected false rating scams—where a casino employee rates a player at a higher wager level than he or she actually played, or rates a player for a longer time period than was actually played, etc. Hence, I assigned an investigator to monitor for indicators of this fraud.

While the investigator didn't detect any indications of fraud on the part of the floor employee, he happened to look over at another employee—the pit clerk. The pit clerk's role is to enter into a computer the player rating information compiled by floor personnel. The investigator noticed two things: the clerk was working on a slot machine

Continued on page 7

Continued from page 6

account, rather than a table game account, and she was typing her name into the account owner field. As the investigator continued to watch, the clerk called up other accounts and into each she replaced the name of the account owner with her own.

Further investigation revealed that the clerk had obtained her supervisor's system password and used them to access the "edit" function which allowed her to alter player accounts.

The clerk used her access to identify older accounts of players located out of state—because there was less chance of being noticed by a returning player who had a lot of points. Again, she removed the names and added hers. She then used the players' points as her own.

It was ultimately determined that the scam had gone on for at least 18 months and cost the casino well into six figures.

Fraud prevention lessons learned:

- Every function in a business is critical to the overall operation and must be continuously monitored for adherence to anti-fraud controls, policies and procedures.

- Protect computer passwords at all times. In the above case, the clerk was given her supervisor's password to use while the supervisor was on vacation. Needless to say, the password was not changed upon her return.

- Regularly review employee computer access levels. Fraud is often committed by employees through the use of a higher level of computer access than authorized.

- If applicable, review all exception reports on a daily basis.

The bottom line: It is a mistake to underestimate the cost of fraud in any organization. The financial and human resources you invest in fraud prevention can easily cut those losses to a degree that more than pays for the investment. And making fraud prevention a priority enables management to project an image of integrity and ethical conduct that can only help it in dealings with customers, shareholders, regulators and other stakeholders. 📌

White-Collar Crime Fighter source:

Derk Boss, CFE, CPP, CSP, President, DJ Boss & Associates, a domestic and international gaming protection and loss prevention firm. Prior to starting his own firm, Derk was Corporate VP, Surveillance and Compliance at American Casino & Entertainment Properties, LLC, owners of the Stratosphere Casino and Hotel in Las Vegas. Derk can be reached at djboss49@gmail.com.



THE CON'S LATEST PLOY...

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

Stockton, CA

Top drug maker nailed on massive kickback scheme. Louis Anthony Contreras, a one-time high school football star, was arrested on eight counts of theft and falsifying bookkeeping.

According to San Joaquin County (CA) Sheriff's Detective Michael Alagna, Contreras worked since 1995 for Tracy Material Recovery Inc., a local waste recovery company owned by Mike Repetto. Contreras is the brother of Repetto's wife, Anna.

Contreras worked on the weigh scale and accepted payments after customers dumped loads of refuse at the transfer station. Many of these payments were made with cash.

The charges: Prosecutors originally accused Contreras of stealing portions of the cash payments—an average of \$410 a day over the 12 years he worked for Repetto. That would indicate a total misappropriation of \$1.8 million. However, court documents indicate that the total loss was considerably less. The actual amount remains undetermined.

How he did it: Alagna alleges that Contreras would void tickets purchased by customers to permit dumping loads of refuse...add up receipts from the cash he planned to steal, and then take that amount from the register to conceal the theft from company bookkeepers.

The bust: Apparently, a co-worker noticed that Contreras failed to follow the rules on some cash transactions and told his bosses, who ultimately alerted the sheriff's office. According to grand jury testimony, Mike Repetto then installed surveillance cameras to monitor Contreras' activities while on duty. The cameras allegedly recorded Contreras ripping up receipts for customer payments, removing cash from the register and stuffing it into a

backpack.

Contreras ultimately confessed to the fraud and in a written statement admitted to stealing \$100,000 to \$150,000 a year while working the scales at the waste recovery facility. He revealed in his confession that he would spend the stolen cash on "five-star hotels," "girls" and "fancy dinners."

Tacoma, WA

"Phantom logs" yield \$2.5 million in dirty money.

Brett Smith, who worked for Manke Lumber Company, pleaded guilty along with seven other defendants to a scheme involving diverting funds that should have gone to individuals who sold logs from their property to the lumber company.

Details: Smith worked as a scaler for Manke starting in 2004. This job involves weighing, measuring and inspecting logs delivered to the mill to determine their grade and value. Scalers then enter the information about each log into a handheld computer which transmits the data directly to Manke's offices where processing for payment to the seller is completed.

The company then used this information to mail checks to people as compensation for the logs they had had delivered to Manke. This process was abused by Smith and his co-conspirators to fraudulently divert funds from Manke.

Details: Between November 2004 and July 2006 Brett Smith and several co-conspirators, including his brother Bryan M. Smith, Elaine Turner, who was Bryan Smith's girlfriend, Jeffrey Ogburn, another Manke employee, and several others, created phony records of log deliveries that resulted

in Manke unknowingly sending checks to people involved in the conspiracy for logs that were never delivered.

Four of the defendants, including Bryan Smith, pleaded guilty to several fraud and money laundering charges and to having recruited others to accept fraudulently obtained checks for non-existent logs that were falsely recorded as having been sold to Manke.

The recruits received and cashed or deposited the checks from Manke Lumber, keeping 10% to 25% of the proceeds and returning the rest to Brett Smith and his co-conspirators. This financial activity constitutes conspiracy to commit money laundering in the indictment filed in US District Court in Tacoma.

Big numbers: In his plea agreement Brett Smith admitted that he submitted false paperwork for more than 1,500 loads of logs worth a total of more than \$2.5 million. In all, he submitted bogus log documentation in 20 different names.

The case was investigated by the Tacoma Police Department and the Internal Revenue Service Criminal Investigations (IRS-CI).

Las Vegas, NV

Energy company financial professional applies his skills to a four-year embezzlement spree. A former

business analyst and financial planner for Nevada Power, a unit of Las Vegas-based utility company, NV Energy Inc., who stole almost \$2 million from a company bank account, was sentenced to two years in prison and ordered to pay \$1.8 million in restitution.

Background: Kyle Roher pleaded guilty several months earlier to two counts of wire fraud in connection with an alleged scheme in which he exploited his authority as a senior business analyst and financial planner at Nevada Power to steal money from a Nevada Power charitable account and a “general spending” bank account by preparing forged wire transfer forms which authorized disbursements from the Nevada Power bank accounts to two bank accounts that Roher controlled at Bank of America. One of those accounts was named NPC Foundation Account.

Details: Roher was a signatory to a Nevada Power account at Well Fargo Bank called Nevada Power/CAL Foundation Account which was intended specifically for disbursing charitable donations.

Roher also had limited authority to use a general Nevada Power account for making business-related disbursements. However to initiate payments from this account, Roher was required to fill out and receive approval of a wire transfer form along with the signature of an authorized Nevada Power manager.

Between August 2001, Roher forged a letter from Nevada Power to Wells Fargo directing Wells Fargo to close the Nevada Power/Call Foundation account and have all funds wire transferred to his NPC Foundation Account at Bank of America. The total transferred was \$91,400.

Approximately six months later, Roher opened a second account at Bank of America, this time in his own name. Several months later and over a period of about two years, Roher created seven false wire transfer authorization forms and forged the necessary signatures in order to fraudulently transfer approximately \$550,000 from the Nevada Power general account to his NPC Foundation account.

Emboldened by the success of this fraud, Roher opened yet another account which he named CAL Foundation. Though similar in name to the closed Nevada Power charitable account, this new account was owned and controlled by Roher. For approximately two and a half years, Roher perpetrated a similar fraudulent wire transfer scheme, initiating a total of 12 bogus transfers from the Nevada Power general account to his CAL Foundation account totaling about \$1.1 million.

In October 2006—after nearly four years—Roher’s fraudulent scheme was finally discovered by Bank of America which froze disbursements to Roher’s accounts including a final \$100,000 wire transfer which Roher had fraudulently authorized.

Lessons for all: Segregation of duties in all financial transactions does matter. Positive pay at your bank does matter. Reviewing your disbursements and wire transfer records at least once a year does matter. ☺



YES! I want to save \$50 on a one-year subscription to **WHITE-COLLAR CRIME FIGHTER!** By subscribing now, I'll get the money-saving introductory subscription rate of \$245. **That's \$50 off the regular subscription price of \$295!**

Plus, send me—for **FREE**—THREE Special Reports on how to prevent, detect and investigate fraud threatening MY organization.

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

Card # _____ Expiration date _____

Signature _____

Name _____

Affiliation _____

Address _____

City _____ State _____ Zip _____

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

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

COMING SOON IN

White-Collar Crime Fighter...

- **Essentials of accounts payable fraud prevention**
- **Latest anti-identity fraud—best practices**
- **Cyber-security insights from top experts**
- **Secrets of successful forensic data-mining**
- **Why not to cut anti-fraud budgets in tough times**