WHITE-COLLAR CRIME FIGHTER

www.wccfighter.com

YOUR SECRET WEAPON IN THE WAR ON FRAUD

VOLUME 11 NO. 10
DECEMBER 2009

IN THE NEWS

If the SEC and DoJ Don't Get You...

The early-December corruption charges against a UK-based executive of the *Fortune 500* company Johnson & Johnson are significant in that they prove that the recent reports of heightened enforcement activity by the SEC and DoJ are not occurring in a global vacuum.

Details: After responding to referral of its investigation of Robert John Dougall by the US Department of Justice, Britain's Serious Fraud Office charged Dougall, a former executive of Johnson & Johnson subsidiary DePuy International of Leeds with overseas corruption.

Dougall is accused of making corrupt payments to medical professionals in the Greek public healthcare system in order to sell orthopaedic products. The illegal activities allegedly occurred between February 2002 and December 2005.

The UK charged Dougall with conspiracy to corrupt in violation of the UK Criminal Law Act 1977.

Important: The SFO said it began working on the case in March 2008. It remains to be seen whether additional foreign agencies sign on to enhance global anti-corruption activity.

White-Collar Crime Fighter sources: UK Serious Frauds Office (SFO), www.sfo.gov.uk and reliable news sources.

IN THIS ISSUE

Paul McCormack, CFE, *Innovar*

"I Did It"

Traps and Opportunities When Guilty Employees Confess to Fraud

Once an employee has confessed to committing fraud he or she may display a wide range of emotions. Some are distraught, others are aggressive. Still others are fearful or depressed.

More often than not, employees are embarrassed and in a surprising number of cases, relieved that they have been caught. For employees who appear relieved, now is the time for management to use this vulnerable state of mind to its advantage.

Aim: To obtain the clearest possible picture of how your organization left itself open to the crime and how to optimize preventive measures.

Key: The relieved employee has just confessed to a deeply held secret that has most likely caused him or her significant stress. The individual may want to talk about the fraud. Ironically, some internal fraudsters want to make amends for the fraud by helping the organization stop similar incidents from happening in the future.

Regardless of the employee's motivations, consider asking the following types of questions:

•When did you decide to commit fraud against the organization?

•How did you rationalize the fact that you were committing fraud?

vWhen did you figure out that the fraud would be easy to perpetrate?

•Which internal control(s) did you bypass, ignore or circumvent to commit the fraud? How much time and effort did it take you to come up with a scheme to bypass these controls?

•How did you keep the fraud hidden from your colleagues and manager(s)?

•Does anyone else in the company know about the fraud? If so, were they part of the scheme?

•What would you do to prevent this type of fraud from happening in the future?

•How long did you expect it would take for management to detect the fraud?

SURPRISING REVELATIONS

Not all employees will cooperate to the extent that you might like, but the information provided by those who do can be exceptionally valuable. Some of the answers you receive may be very surprising.

Real life examples of information received during the post confession phase:

•When asked why they committed fraud, an employee responded that "It was too easy. I couldn't help it. You didn't know how much money we had in the office. What did it matter if I took some cash here and there? The company would not miss the money because you had no clue there was so much readily available cash in the first place! Besides, I really needed it. I spent all of it and kept on taking more. I needed to be stopped."

•Another employee who had hidden a complex fraud for over five years gave the following response when asked how he kept the fraud hidden for so long: "I knew the procedures better than anyone else in the company. In fact, when you sent the auditor to my location, I had to tell him how to do the audit! He was clueless and

I know that he earned more than I did. It made me even angrier and motivated me to take more money. But one day I took $25,000. I was too angry and greedy that time. That's when you caught me. You would never have caught me if I had not taken so much at one time."

•An employee with less than 12 months with the company could hardly contain his excitement when describing how he stole over $250,000 in the course of nine months. "No one in the office had a clue what I was doing. I worked with a bunch of idiots. I enjoyed stealing the money from right under their noses. This job was so far beneath me, I had to do something to make it worth my while to be here. I created all of the fake invoices on my computer. I also used the office copiers and file folders. I then paid all of the invoices myself. Everything I needed to commit fraud was in the office just lying around. The whole thing was far too easy, especially for someone like me who was looking for some excitement."

More often than not, employees are embarrassed and in a surprising number of cases, relieved that they have been caught

•An employee with 25 years at the company provided an answer that revealed a troubled personal life which resulted in the motivation to steal. "About a year ago, my husband had an affair. It's over now, but he told me that he did not want to be married anymore. I thought if we could pay off some debts and take a vacation that our marriage would get better.

"I took a couple of blank checks from the stack in my manager's desk, made them out to "cash" and cashed them. I then waited for someone to become suspicious and ask about them. When no one did, I wrote five more checks, enough to buy my husband a new set of golf clubs. After, that my husband wanted me to buy him more presents. I took more and more checks, to pay for his gifts as well and to pay some bills. I meant to pay it back, but I never could figure out how to do that. I know I took a lot of money, but I tried not to think about it."

PUT THE INFORMATION TO USE

Often, information like this, gathered directly from fraudsters from within your own organization, carries more weight with senior management than recommendations from auditors or anti-fraud experts that are based on perceived internal control weaknesses that have yet to result in fraud.

Key: Revelations like those in the above examples allow management to understand the mind of a fraudster as he or she contemplates, and then commits fraud. Such information can be used to convince management to make changes that dramatically reduce the probability of a similar crime occurring in the future. *From the above confessions, it should be readily evident that for the victim companies, one or more of the following essential anti-fraud controls was not in place:*

•All cash receipts and disbursements should be reported on a daily basis using at least two employees to compile the report.

•Bank statements should be reconciled on a monthly basis to amounts claimed on the daily cash reports.

•Employees should be rotated frequently through different job functions to ensure that fraud can be discovered quickly.

•Auditors must have adequate training and experience to conduct fraud audits. If employees perceive that auditors are highly trained, they may be less likely to commit fraud in the first place.

•Blank check stock should be stored in a locked cabinet that few employees have access to. Each check issued must be recorded in the check register. Each month, the bank statement should be reconciled to ensure that checks written against the account were properly authorized and signed.

•Payment of invoices should be made by a centralized department with the appropriate controls in place. Dollar thresholds for senior management approval should be established and enforced. Vendor payments should be randomly sampled to verify that both the vendor and invoice were authorized and paid using the appropriate process.

•An employee hotline should be activated to provide employees who learn

Preventing and Detecting Fraud in Accounts Payable

By Peter Goldmann

This book provides invaluable insight into how fraudsters exploit AP and how to stop them! Visit *www.iappnet.org.*

WHITE-COLLAR CRIME FIGHTER

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

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

Mission Statement

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

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

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

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

of wrongdoing by one or more of their co-workers with a confidential channel for blowing the whistle.

Bottom line: Next time an employee confesses to fraud, consider pushing the interrogation as far as you can. As the results above show, it can be well worth the effort.

***White-Collar Crime Fighter* source:**
Paul McCormack, CFE, a partner at Innovar where he leads the firms' fraud practice. Paul is also former vice president of Fraud Detection for SunTrust Banks in Georgia. He can be reached at pmccormack@innovarpartners.com.

Cooking the Accounts Receivable Books

Companies typically maintain "allowance" accounts—sometimes called "Allowance for Doubtful Accounts" to cover receivables that ultimately become uncollectible and must be written off. When the company writes off receivables at their actual realizable value, the result is a decrease in receivables, current assets and net income.

Fraud risk: Accountants can abuse this function to embellish the company's financials by falsely underestimating the uncollectible portion of receivables, thus making total collectible receivables appear greater than they actually are. This in turn keeps uncollectible receivables on the books as current assets.

Similarly, dishonest accountants can cover up a credit issued to a customer without reducing the receivable. This is achieved by simply keeping the full receivable on the books to falsely bolster sales totals, but hiding the credit memo to avoid having to make the appropriate downward adjustment in receivables.

Example: A customer receives a shipment of $100 worth of goods. The vendor records the $100 sale as revenue and increases receivables by $100. The customer then complains that half of the goods were defective and says he's only going to pay $50. To avoid having to take the $50 "hit" on sales, the vendor issues a credit memo to the customer's account, but leaves the $100 receivable unchanged.

Key: This fraudulent manipulation of earnings will only be spotted if the receivable eventually ages to the point of write-off, and the auditor discovers the $50 discrepancy between sales and written-off receivables.

***White-Collar Crime Fighter* source:**
Scott Langlinais, CPA, head of Langlinais Fraud Audit and Advisory Services, a Fort Worth, TX-based consultancy specializing in fraud prevention, detection, and response. He can be reached at www.scottlan glinais.com.

BETTER INVESTIGATIONS

R.W. (Andy) Wilson, CFE, CPP, *Wilson-Turner Incorporated*

Responding to the Fraud Allegation: Now What!

The initial response to a fraud allegation against your organization is the most important step in the investigation process. Unless the investigator properly assesses the allegation, an investigation may never take place, allowing the fraudster to go undetected.

Critical investigative goal: Quick assessment of complex fraud indicators and providing sufficient information to assist management in making the right decision to move forward.

HOW TO USE TIPS

According to the Association of Certified Fraud Examiners' *2008 Report to the Nation on Occupational Fraud & Abuse,* fraud is discovered by a "tip" nearly half of the time, with the majority coming from employees.

- **Resist overreacting.** Fraud investigators must understand that allegations of fraud and other forms of misconduct come as a shock to management. As the victimization of fraud sets-in, the shock often turns to disbelief, panic and alarm.

Trap: Allowing this disbelief to press too hard and too fast for confirmation of the suspicions. This often alerts the criminals to the detection of their misdeeds, leading them to destroy potentially valuable evidence.

- **Avoid making spontaneous allegations which are often inaccurate and reckless.** Sometimes, managers even convene meetings with confidants who are later identified as accomplices in the scheme. In other cases, bosses may fire the fraudster before gathering vital information through interrogation (see also page 1).
- **Make all efforts to investigate.** Management may believe that doing nothing is better than doing anything. This results in the offender(s) getting away with their crimes and sends the message that crime pays.

Better: A four-phase Plan of Action for responding to tips about potential fraud:

- Pre-investigation
- Investigation planning
- Investigation
- Post-investigation.

Caution: Just because someone has a degree or special certification (i.e. CPA, CFE, CIA) does not mean that they are ready to conduct a fraud investigation. Instead, fraud investigators should "know what they know and know what they don't," before undertaking a fraud assignment.

PHASE 1: PRE-INVESTIGATION

When providing information, tipsters often supply the name of the fraudster and the fraud type, leaving the investigator to determine the "how" and "why." Sometimes the information reveals what is occurring, and the investigator must determine "who" and "how."

Either way, the pre-investigation is the starting point and should focus on proving or disproving the allegation. *Critical investigative guideline:*

"To prove that a fraud has occurred, one must endeavor to prove it has not; and to prove it has not occurred, one must endeavor to prove that it has."

If the fraudster is still employed, the process should be conducted covertly under the auspices of a management review or other non-threatening business practice. The pre-investigation process must develop an understanding of the suspect's position and the opportunities that may exist for him or

Continued on pg. 4

CYBER-CRIME FIGHTER

How E-Merchants Can Improve Manual Credit Card Anti-Fraud Review

As on-line retail merchants know all too well, most credit card orders that do not pass automated order screening must be held for manual review. In this stage, additional information is collected to determine if orders should be accepted or rejected based on the level of fraud risk.

Problem: Manual review is costly and puts great pressure on already slim profit margins. It also limits scalability, and potentially compromises customer satisfaction.

Approximately one of every three on-line credit card orders are still screened manually for fraud

Result: A trend toward investing in state-of-the-art automated fraud detection software for on-line transactions.

However, approximately one of every three on-line credit card orders are still manually screened for fraud. This means that existing automated tools are not yet sophisticated or cheap enough to enable merchants to cut back on manual review.

Key: One consequence of using more automated fraud detection tools is a greater chance of one or more flags being raised on E-commerce purchases, resulting in more orders being flagged for manual review.

BALANCING ACT

In today's tough economy, E-merchants expecting increased on-line sales will need to take at least one of the following actions:

- Dedicate more staff time to the order review process.
- Hire more review staff.
- Allow more time to process orders and ship good ones.
- Improve accuracy of initial automated sorting and make the subsequent review process more efficient.

USING CASE MANAGEMENT SYSTEMS

Currently one out of three merchants reports using a case management system that supports their manual review process by prioritizing flagged transactions by degree of fraud risk and other efficiency-promoting factors.

Main manual screening factors:

- Gathering all relevant transaction data to initiate the review.
- Analyzing transaction data characteristics to identify suspicious elements.
- Reviewing customer's historical purchase activity.
- Contacting third-party data sources to validate customer provided billing and/or shipping information.
- Contacting the card issuing bank to validate billing information.
- Contacting the customer to verify that the purchase was authorized.
- Documenting the procedures performed during the review process.
- Resolving the order—deciding to "accept" or "reject" the transaction.
- Telephone number validation / reverse lookup.

Benefits: Merchants using a case management system are better able to track fraud rates on orders that have gone through manual review. Seventy-four percent of merchants using case management systems report tracking fraud rates for manually reviewed orders compared with only 42% being able to do so when not using a case management system. Being able to track fraud rates and patterns enables the merchant to fine-tune manual review training and thereby improve efficiency.

Bottom line: The indispensability of these manual anti-fraud measures is not abating. E-merchants should carefully assess the cost-benefit ratio of bringing on additional manual review personnel in the ongoing battle against growing on-line credit and debit card fraud.

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

- *CyberSource 10th Annual Online Fraud Report, CyberSource,* www.cybersource.com and credit card industry anti-fraud experts.
- *"Proven Strategies for Combating Card Not Present Fraud: What is Needed Today to Protect Your Business,"* white paper from Accertify, merchant fraud prevention solutions provider, www.accertify.com.
- Tom Mahoney, founder and president, Merchant 911.org, a Web-based resource for on-line retailers seeking information to help protect themselves from credit card fraud. Tom can be reached at admin@merchant911.org.

Continued from page 3

her to commit fraud. The process should also focus on identifying the symptoms of fraud surrounding the allegation. *Examples:*

- **Document irregularities.** Look for missing, altered or photocopied documents…errors involving duplicate payments…invoice sequences that are not logical…excessive voids or credits… aging receivables or payables…and bank reconciliations that contain old or increasing items, to name a few.
- **Other accounting anomalies** such as inaccuracies in the organization's journals and ledgers…increased scrap claims when production is on a decline…paying excessive rates to vendors with little or no documentation…unusually numerous debit or credit memos…over-rings or voids.

Critical: These symptoms must be documented and secured. More than half of all fraud investigations fail because essential documentation was not obtained at the first instance.

Important: Once evidence is discovered in support of the allegation, "predication" exists. Predication refers to circumstances which, when taken as a whole, lead a reasonable, prudent professional to believe that a fraud has occurred, is occurring or will occur.

PHASE 2: SHREWD PLANNING

With initial evidence supporting the allegation of fraud in hand and an on-site evaluation of the business unit having been conducted, the investigator should be able to make informed planning decisions, designed to establish proof that a fraud has occurred. *In designing the plan, focus should be centered on proving three fraud elements:*

- Theft of cash or other assets including tangible inventory or information.
- Concealment—most commonly manifested in "cooking the books," which is where the fraudster falsely records financial information in order to eliminate the "paper trail."
- Conversion—exchanging stolen assets for cash. Among other methods, this can be done by selling the assets, taking inventory or cashing checks.

Important: Explain the investigation plan to management and provide an estimate of how long it will take to execute, at what cost and the chances of recovering stolen assets.

Reason: Management will almost certainly have goals and objectives for

Continued on page 5

Continued from page 4

the probe. If these are known in advance, they should be included in the plan to allow the investigation to move forward efficiently.

PHASE 3: INVESTIGATION

Helpful: Most fraud investigations require the cooperative effort of a multi-disciplinary team which may include fraud examiners, accountants, professional investigators, attorneys and others including the personnel department and operations team. Some of these specialists may work directly for the organization, while others may be outside contractors.

Key: If the suspect is still in position, keeping the investigation covert is essential. Investigators should work rapidly to obtain evidence as long as the suspect is unaware that he or she is a suspect.

PHASE 4: POST INVESTIGATION

The investigator should assess the evidence at every stage of the investigation, but once the process is complete, it is time to document the findings.

If the evidence supports the allegations, organizations have many options ranging from doing nothing, to dismissal of the suspect or perpetrator to filing a commercial crime insurance claim, civil litigation and/or criminal referral. The fraud investigator should assist management in understanding what is involved in each process.

Regardless of the decision, the primary purpose of documenting the findings is to report the facts. The report should be a true and accurate record of what has been learned; discussed in a brief, objective and neutral manner.

Most reports include the following areas: Introduction, summary of the investigation, allegations, relevant policies or procedures, chronology/timeline, key factual findings, conclusions and recommendations (depending on the purpose of the report) and exhibits.

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

R. A. (Andy) Wilson, CFE, CPP, co-founder and Managing Director of Wilson & Turner Incorporated, an investigative consulting firm in Memphis, TN. Andy specializes in the prevention, identification, investigation and resolution of employee crime. In addition to his anti-fraud practice, he serves on the adjunct faculty at The University of Memphis and Utica College, where he teaches fraud examination classes at the undergraduate and graduate levels. He can be reached at raw@wilson.turner.com.

IN THE TRENCHES

Unsung Fraud-Fighters: Your Accounts Payable Team

The Orlando, FL-based International Accounts Payable Professionals (IAPP) helps its members (who are exactly what the name of the organization says they are—accounts payable professionals) gain recognition as critical organizational employees.

Key: In promoting the role of AP professionals, this relatively obscure trade association emphasizes that these people represent a potentially critical collective impediment to dozens of types of fraud.

Problem: AP, while critical to the anti-fraud defenses of the organization, is on no one's radar. They're just there in the back office doing their thing—processing invoices and paying the vendors.

Because they are located in the epicenter of everything financial, it stands to reason that AP employees are in positions to detect and prevent any number of potential frauds

Now, however, this stigma of second-class organizational citizenship may be starting to change. And today's growing risks of fraud have a lot to do with it.

CENTRAL FUNCTION

AP managers and staff sit at the frontlines of any organization's financial systems and in one way or more, impact the efficiency of purchasing and procurement, supply chain operations, manufacturing operations, financial operations, legal, human resources, compliance and, of course, payments and disbursements.

Result: When the AP function runs smoothly, virtually every other function in the organization does as well. More importantly from an anti-fraud perspective, if your AP team is trained in the numerous types of fraud that can occur in these functions, they are able to detect and often prevent many of these crimes.

THE AP FRAUD FACTOR

As mentioned above, because they are located at the epicenter of everything financial, it stands to reason that AP employees are in positions to detect and prevent any number of potential frauds. *Examples…*

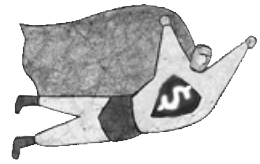
- **Internally perpetrated billing schemes.**
- **Externally perpetrated billing schemes.**
- **Tampering with the Vendor Master File** to add phony vendors, change legitimate vendors' addresses, alter vendor bank account information, etc.
- **T&E fraud.**
- **Purchasing card (P-card) fraud.** (Remember Tom Coughlin, the former Wal-Mart co-chairman who charged $500,000 of personal expenses including a $5,000 pair of alligator cowboy boots to his corporate P-card?)
- **Payroll fraud** (such as "ghost" employee schemes).
- **Check fraud.** Stealing blank company checks, forging endorsements, forging signatures, counterfeiting the organization's checks. The list goes on and on.

Additional risks:

- **Collusive AP-related frauds** such as kickback schemes and bribery. In many organizations, AP staffers can't or aren't in a position to take bribes or kickbacks due to effective segregation of duties. However, your procurement department is a different

Continued on page 6

FRAUD-FIGHTERS' NEED-TO-KNOW HOT LINE



Latest On-Line Banking Fraud Alert: ACH Hacking

The Federal Deposit Insurance Corporation (FDIC) and other organizations have issued warnings to banks and their commercial customers about a new variety of phishing attack based on fraudulent ACH transfers.

Details: Hackers are reported to send Emails to corporate customers of banks, luring them to fake bank Web sites where they enter their login information to access accounts and initiate funds transfers from accounts used by customers to make ACH payments.

Example: One New England retail fuel company had its bank account compromised when an employee fell for a phishing attack that resulted in hackers located in Eastern Europe obtaining the username and password to the bank account to which fuel customers send ACH payments. The hackers fraudulently transferred $150,000 from the account and obtained access to an unspecified number of customer bank account information.

Some attacks also plant sophisticated Trojan horse "crimeware" on bank customer computers to enable hackers to access the customer bank accounts used to make ACH transfers to the bank accounts of vendors with whom they have commercial accounts.

Self-defense: Banks that accept ACH payments from customers should warn these patrons about clicking on links in Emails from senders purporting to be from their financial institutions. In addition, customers should immediately implement ACH debit blocks. These block any ACH payment that is not pre-scheduled with the bank.

Also effective: Small- and medium-sized businesses should use a dedicated computer for all on-line banking. This should eliminate the opportunity for authorized users to click on risky links or browse the Internet to sites that could inadvertently result in downloading of Trojan horses and other malicious applications.

White-Collar Crime Fighter *sources:*

- Linda McGlasson, Managing Editor, *BankInfoSecurity,* www.bankinfosecurity.com.
- Federal Deposit Insurance Corporation (FDIC) Special Alert, www.fdic.gov/news/news/SpecialAlert/2009/sa09147.html.

Latest Phishing Attack Attempts to Steal Consumers' Data Via Bogus Live-Chat Support

A new, unique type of phishing attack targeting on-line banking customers was recently discovered by the prominent security services provider, RSA. RSA has dubbed this new version of on-line fraud the "Chat-in-the-Middle" (CITM) phishing attack.

Key characteristic: A CITM attack is first executed through "routine" phishing methods but instead of being redirected to the next page of the phishing scheme, victims are presented with a social engineering phase of on-line fraud.

Example: The attack may dupe bank customers into entering their usernames and passwords into an ordinary phishing site but this triggers opening of a bogus live chat support window where a "live" fraudster posing as a bank employee can obtain even more personal information for later use in committing identify fraud.

Latest finding: In the live chat session, the fraudster poses as a representative of the bank's fraud department and attempts to trick customers who are on-line into divulging sensitive information—such as answers to secret questions that are used for the ostensible purpose of "on-line customer authentication." This is achieved by falsely but convincingly stating that the bank is "now requiring each on-line customer to validate their accounts."

White-Collar Crime Fighter *source:* RSA, Security Division of EMC, providers of secure data, compliance, PCI, consumer identity, consulting, other Internet security services, www.rsa.com.

Continued from page 5

story. And when a vendor pays off a purchasing manager to award him a piece of business he might otherwise not get or to submit invoices with prices in excess of what he'd normally charge, who ends up processing the payments? Right, AP.

• Customer-perpetrated frauds. In tough times companies need every single customer they can get and hold on to. But don't lose sight of the forest for the trees. Not all of your customers are perfect models of integrity. Whether it's a retail or a commercial customer, given the extreme financial pressure they're under, if you give them an opportunity to scam you chances are they'll find a way to justify doing it.

Essential: Segregation of duties for processing customer refunds. That means refunds should not be processed by anyone who is involved with customer data input or billing activities. And, before issuing any customer refund checks ensure that 1) the customer is legitimate; and 2) all supporting documentation about the reason for the refund is valid and accurate.

FIGHTING FRAUD ON THE FRONT LINE

With your AP managers and staff occupying such key positions to detect, prevent and report a wide variety of internal, external and collusive frauds, you can support their fraud-fighting efforts by:

- Paying them at a rate commensurate with the significant responsibility they have for maintaining the organization's financial security.
- Training them in the many types of fraud that they may encounter in their day-to-day duties.
- Incorporating into the organization's Tone at the Top the message that Accounts Payable is among the organization's most critical centers of corporate ethics and integrity and must be treated with the same respect that operations, finance, purchasing and human resources are.

AP FRAUD AT THE TOP

On a more costly and disturbing note, management's authority to override AP anti-fraud controls can

Continued on page 7

Continued from page 6

be abused to commit crimes that are both far costlier than those committed by AP or procurement staff or customers.

Example: "Fraud by intimidation." A senior executive instructs an AP manager to cut a check made out to cash or to "XYZ Corporation" for a significant six-figure amount.

The rules say that any check request for more than $10,000 requires the written approval of two senior managers as well as full documentation of the payment (an invoice, purchase order, charitable gift documentation, etc.).

The AP manager, concerned about being hauled on the carpet for insubordination musters the courage to meekly inform the executive that the rules require documentation prior to cutting the check. Unsurprisingly, the executive barks at the AP manager to mind his own business and just cut the check and deliver it to his desk within an hour.

Management's authority to override AP anti-fraud controls can be abused to commit crimes that are both far costlier than those committed by AP or procurement staff or customers

Unfortunately, most AP managers deal with this problem by reluctantly complying with their bosses' orders. In a high-unemployment economy, it is understandable for such victims of abuse to justify their actions by saying, "What could I do? I needed my job."

SELF-DEFENSE

Management-perpetrated fraud such as this can be reduced if the rest of the management team—and the Board—realize how critical AP is to the fraud prevention process. They would then implement policies encouraging AP staff to blow the whistle on incidents of management override, and would repeatedly emphasize that doing so would in no way jeopardize a whistleblower's job security.

***White-Collar Crime Fighter* source:**
Peter Goldmann, editor, *White-Collar Crime Fighter,* www.wccfighter.com.

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

THE CON'S LATEST PLOY...

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

Iowa City, IA

Kosher meat merchant may be anything but. Sholom Rubashkin, former manager of the kosher meatpacker, Agriprocessors, was charged with money laundering, bank fraud, destroying evidence and violations of federal meat processing laws.

Background: Agriprocessors filed for Chapter 11 bankruptcy protection in November 2008 and was subsequently purchased by a group headed by a Canadian businessman, Hershey Friedman. The plant has been the subject of nationwide scrutiny since federal agents raided it in May 2008 and arrested hundreds of immigrant workers who were in the country illegally. The raid led to criminal charges against most of the workers and 72 immigration-related charges against Rubashkin. The fraud charges make a total of 91 against Rubashkin.

Regarding the fraud charges, prosecutors accuse Rubashkin of engineering a scheme to divert about $26 million in customer payments away from First Bank Business Capital with which Agriprocessors had a $35 million line of credit. Specifically, Agriprocessors was required to deposit all customer payments in a special account that served as collateral for the line of credit. Instead Rubashkin allegedly funneled the money to a separate account. According to the indictment, he then used various third parties including a Torah education program and a kosher grocery outlet to launder portions of the funds. This was allegedly executed by having Agriprocessor checks sent to these outside entities and then having checks from the entities deposited in the collateral account, thereby disguising them as customer payments, as required by the loan agreement.

However, a substantial portion of the customer revenue channeled through this method was essentially skimmed by Rubashkin. To conceal the fraud, Rubashkin had Agriprocessors' accounting department neglect to record many of the received customer payments as revenue, making it appear as though the payments had not yet been received and thus falsely inflating the company's accounts receivable. He then had the accountants maintain a second set of books showing receipt of the customer payments that were deposited into an account other than the one designated by the bank as collateral for the credit line. The difference between what was deposited in the collateral account and what wasn't—approximately $6 million—presumably represented funds that were misappropriated by Rubashkin.

Rubashkin will be tried on the fraud charges before he is tried on the immigration charges.

Fairfax, VA

Yet another food stamp fraud prevention attempt. The US Department of Agriculture will spend $25 on a new technology aimed at nailing food stamp fraudsters. The federal food stamp program, now referred to as SNAP for Supplemental Nutrition Assistance Program, has been a source of dirty money for retail food suppliers for years, despite numerous attempts to foil them.

Typical scheme: After an 18-month investigation involving local, state and federal agencies, eight grocery and convenience store owners and employees were charged with federal food stamp fraud.

The eight stores were charged with stealing SNAP benefits through the Electronic Benefits Transfer (EBT) system which is essentially a debit card

system facilitating direct transfer of funds from a SNAP beneficiary's account to that of an approved food retailer, theoretically in payment for food items.

According to court documents, some of the fraudsters were store owners and others recruited SNAP beneficiaries to participate in fraudulently transferring EBT funds to the store owners' accounts in exchange for cash at less than face value.

The eight individuals indicted are charged with having stolen an estimated $2 million.

Latest development: SRA International, Inc., a leading provider of technology and strategic consulting services and solutions to government organizations and commercial clients, was awarded a contract by the U.S. Department of Agriculture's Food and Nutrition Service (FNS), to develop the next generation of the anti-fraud locator using electronic benefits transfer retailer transactions (ALERT) system. The contract has a ceiling of $25 million over a 10-year period.

This expenditure was apparently deemed necessary despite the Agriculture Department's recent statement that "One of the most promising developments in the fight against SNAP fraud has been the increasing use of electronic benefit transfer—EBT—to issue SNAP benefits." Though the US government is not the most nimble at adopting new technology in general, the SNAP problem is yet another example of how difficult it is generally for fraud fighters to get a step ahead of the criminals.

The ALERT system is a fraud-detection, decision-support system designed to monitor and track electronically conducted retail transactions completed by Supplemental Nutrition Assistance Program (SNAP) recipients in authorized meal program and food retailer locations. The ALERT system facilitates management of the program by providing transaction-level information to the federal personnel responsible for SNAP retailer.

SRA stated that it will work with FNS to develop the next-generation ALERT system, to enhance its functionality and modernize its technology.

Memphis, TN

Embezzlement red flag: Fast and furious transactions. In a classic case of fraudster fumbling, Thom Williams, a former "financial analyst" for Verso Paper Corp. was caught after he allegedly embezzled some $2.2 million between March 7, 2009, and July 2009 by making fraudulent ACH transfers from Verso accounts to a joint checking account with his wife and then recording the transactions as payments to vendors.

According to Special Agent Kimberly Moore of the FBI, in an affidavit related to the case, Williams was caught when the company's controller, Bob Wilhelm noticed the "problem" after Williams had allegedly made two fraudulent transfers of $762,000 and $782,000 between September 23, 2009, and October 6, 2009, from Verso's account at Bank of America to Williams's joint account at BankPlus.

The case indicates how fraudsters sometimes fail to realize how easy it is to get caught by failing to think carefully about concealing their crimes. Corporate financial managers should be alert to obvious frauds like these, though most white-collar criminals are more methodical about covering their illegal conduct, requiring financial managers and executives to also familiarize themselves with the more subtle red flags of employee fraud.

Executive Fraud Psychology

In what might help to explain at least some of the financial crime associated with the current financial crisis, two professors have published a report indicating that overly optimistic managers are more likely to commit financial statement fraud than those with more realistic views of their companies' performance.

Details: The researchers argue that "executive overconfidence, defined as having unrealistic (positive) beliefs about future performance, increases a firm's propensity to commit financial reporting fraud... [O]verconfident executives are more likely to 'borrow' from the future to manage earnings thinking it will be sufficient to cover reversals. On average, however, they are wrong."

For the full report, entitled *Executive Overconfidence and the Slippery Slope to Fraud,* by Catherine M. Schrand, PhD, Professor of Accounting, Wharton School of the University of Pennsylvania and Sarah Zechman, PhD, Assistant Professor of Accounting, University of Chicago Booth School of Business, visit http://ssrn.com/abstract= 1265631.

COMING SOON IN White-Collar Crime Fighter...

- **Fraud fighters' role in prosecutions**
- **Automating accounts payable: Essential anti-fraud factors**
- **Critical healthcare anti-fraud measures**
- **Fraud prevention preparation for economic recovery**