

# WHITE-COLLAR CRIME

## FIGHTER

www.wccfighter.com

VOLUME 10 NO. 9  
OCTOBER 2008

### YOUR SECRET WEAPON IN THE WAR ON FRAUD

#### IN THE NEWS

##### Beware of Information Insecurity While Traveling

As soon as you log onto a hotel's Wi-Fi or cable Internet service you may unknowingly be making your organization's confidential data vulnerable to cyber-thieves.

That's the finding of Cornell University's Center for Hospitality Research.

**Details:** The researchers discovered that 20% of US hotels still use antiquated Internet service systems that are highly vulnerable to hacking. Moreover, while over 90% of hotels offer wireless Internet service, such service is too often insecure. For example only 15% of hotels surveyed use encryption on guest-used Internet services.

**Tips for travelers:** Avoid sending sensitive business data over a hotel Internet service unless you know the network to be encrypted.

Whenever possible, use virtual private network (VPN) connections from hotels. If your company does not supply a VPN connection, use an on-line service such as <http://www.hotspotvpn.com>.

**White-Collar Crime Fighter source:** *Hotel Network Security: A Study of Computer Networks in U.S. Hotels* by Josh Ogle, Erica L. Wagner and Mark P. Talbert, Center for Hospitality Research, Cornell University School of Hotel Administration, [www.hotelschool.cornell.edu/research/chr/](http://www.hotelschool.cornell.edu/research/chr/).

#### IN THIS ISSUE

- **FIGHTING FRAUD**  
Unique strategy for large and small organizations..... 3
- **FUTURE FRAUD**  
Prepare for widening fraud threat... 4
- **PAYMENTS FRAUD**  
Internal controls for the disbursement process..... 5
- **THE CON'S LATEST PLOY**  
Law-enforcement successes from around the country..... 7

Glenn M. Pomerantz, CPA, *BDO Consulting*

## Common Management Mistakes in Employee Fraud Prevention



Over the past few years I have found myself involved in a disturbingly large number of fraud investigations involving internal perpetrators. In retrospect it is clear that many of these cases could have been prevented had management avoided some costly mistakes. **Examples:**

• **Bad background checks.** I am continually surprised that many of the internal fraud cases I conduct involve ex-felons in positions of trust in which they handled cash and other valuable assets, authorized large-dollar transactions or maintained key financial books and records.

**Important:** Some organizations intentionally give prior felons "a second chance." This can actually work out well for both the employee and the employer. The problem arises when organizations unknowingly hire, promote or partner with individuals with criminal backgrounds.

Making such uninformed decisions is especially astonishing since all of the information you need to thoroughly examine the background of just about anyone is literally at your fingertips.

**Key:** Investigative due diligence ("IDD"), background checks, credit and criminal checks are all terms used to describe the process of gathering information about the people and organizations you are considering hiring or partnering with. Many companies forego the process entirely. Others settle for credit checks without searching for criminal

records...or vice versa. Still others look for the least costly background-checking option just to comply with their own policies and procedures.

**Danger:** All of these "drive-by" background checks can result in costly internal frauds...as can similarly incomplete background checks conducted when an employee is promoted to a position of trust or when a business relationship is expanded.

**Better way:** Thorough, "high-level" investigative due diligence on candidates for positions of trust should include:

- Criminal history, encompassing all jurisdictions where the individual has recently resided.
- Credit history.
- Civil litigation.
- Bankruptcies, liens and judgments.
- Confirmation of educational and professional credentials.
- Media search.
- National and state sex offender registries.
- For individuals with a financial services industry background, searches of financial regulators such as the SEC and FINRA.
- Reference checks of past employment.

**Important:** Investing in such thorough probes—while a bit more costly than the average background check—can provide your organization with a competitive advantage. By screening for the "cleanest" candidates, you eliminate

the costly process of replacing people who, after being trained and tested, end up stealing from you.

**•Poor segregation of duties (SoD).** The opportunity component of the Fraud Triangle exists when an employee possesses the tools to execute a fraud and there is an absence of fraud deterrence, prevention or detection mechanisms.

**Problem:** Segregation of duties (SoD), while proven to be among the most effective controls for minimizing fraud opportunities (see page 5), is still overlooked or at best implemented “on the fly” by many organizations.

**Key:** Properly implemented SoD eliminates fraud opportunities in the key business process areas of...

- Custody of assets.
- Record-keeping.
- Authorization.
- Reconciliation.

The most basic SoD requirement is separation of responsibilities for items one and two—custody of assets and record-keeping.

**Details:** Time and time again, we encounter frauds in which checks are received by an employee who also has the ability to write-off receivables or post fraudulent accounting entries.

**Additional example:** When employees have only a limited role in either custody of assets or record-keeping. An employee who handles returned merchandise and processes credits to the customer’s account has a “golden opportunity” to either credit his or her own account or fail to record the return and steal the merchandise.

**Key:** These and many other basic SoD requirements are sometimes overlooked in even the most sophisticated organizations.

By contrast, when the organization adequately separates these functions among its employees—and ensures that it does not deviate from the procedure—it puts into place some of the best possible deterrents to employee fraud.

This is also true in cases involving collusion.

**Example:** When two or more employees are in positions of trust and have direct responsibilities for financial processes or procedures, it is often easy for them to come up with collusive schemes that can be well concealed. Effective segregation of duties in such situations may require additional controls such as rotation of employees among key financial positions and an independent review and reconciliation function.

**ELECTRONIC SoD**

With most accounting and finance functions now fully automated, segregation of duties has taken on a whole new electronic dimension. It is easy for inadequately trained IT staff to set up automated accounting systems and applications without access restrictions that are critical to eliminating opportunities for accounting, finance and audit personnel to fraudulently manipulate financial documents.

**Self-defense:**

- Regular review of system access.
- Audits of system approvals. This is critical for preventing collusion where an authorized employee tries to enable unauthorized access for a colleague.

**Also important:** Eliminating system access for employees as they change positions in the organization and take on different responsibilities with different access authorizations.

**FRAUD AND HUMAN ERROR**

Unfortunately, even sound internal controls, including appropriate SoD and meticulous background checks, can’t protect organizations against fraud

**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 © 2008 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.

*White-Collar Crime Fighter* and **FraudAware®**  
Proudly Sponsor  
**INTERNATIONAL FRAUD AWARENESS WEEK**  
November 9-15, 2008  
Sponsored by the Association of Certified Fraud Examiners  
INCREASE AWARENESS. REDUCE RISK.

*White-Collar Crime Fighter* and the leading fraud awareness training program, *FraudAware* are proud to sponsor Fraud Awareness Week. *In observance of Fraud Awareness Week FraudAware is pleased to offer FREE one-day on-site fraud awareness workshops. Topics include...*

- How fraud that affects your organization affects all of your employees
- How to train employees to detect red flags of fraud
- How to increase tips to your Fraud Hotline
- How to reduce fraud losses by up to 50%

To reserve a date for your organization’s Free Fraud Awareness Workshop, call us at 1-800-400-2261. (A limited number of dates are available. Dates will be allocated on a first come-first served basis)

caused by honest human error.

**Example:** An accounts payable clerk repeatedly fails to match receiving reports to approved invoices and authorized purchase orders. This gives a dishonest insider the opportunity to divert assets for personal use.

**Key:** What appears to be an innocent shortcut to an accounts payable clerk may defeat a key internal control in the organization's Procure to Pay function.

**Self-defense:**


- Regularly test compliance with key internal controls.
- Establish monitoring controls to verify that the underlying internal controls are functioning. Monitoring controls can best be defined as "controls over controls" and may include independent review of exception reports, analytical review and automated identification of unusual transactions.
- Review training and education programs to ensure that employees understand the significance of internal controls for which they are responsible.
- Establish compensating controls where underlying controls are particularly susceptible to human error.

**TRAINING IS KEY**

As the examples above indicate, companies often underestimate the importance of educating employees about their role in fraud prevention, detection and reporting.

An employee who has been trained to understand the significance of his or her role will be more likely to perform critical procedures as designed...and report fraudulent or suspicious activity to the organization's hotline.

Additionally, organizations should manage training and education as a continuous process.

**Important:** Recognize that changes to the company's strategy, methodologies and tools, competitive environment, products and services and a host of other inputs may require updated employee training on internal controls. Mergers and acquisitions as well as promotions to positions of trust should also be obvious triggers for fresh employee training. 

**White-Collar Crime Fighter source:**

Glenn M. Pomerantz, Partner in the New York office of BDO Consulting, a division of BDO Seidman, LLP, [www.bdoconsulting.com](http://www.bdoconsulting.com). Glenn directs BDO Consulting's Critical Anti-Fraud Program (CAP), which advises clients on fighting and preventing corporate fraud. He can be reached at [gpomerantz@bdo.com](mailto:gpomerantz@bdo.com).

**FIGHTING FRAUD ON ALL FRONTS**

Mike Freiling, PhD, and Wesley K. Wilhelm, MS

# Unique Fraud-Prevention Strategy For Large & Small Organizations



**F**or top management, trying to manage fraud across the entire enterprise presents difficult challenges because there are countless ways to implement anti-fraud programs ...and determining which one provides the biggest bang for the buck can be a complex task.

Fortunately, there is a way to streamline the process. We call it The Fraud Management Lifecycle (FML). It gives top management a way to organize necessary components of an anti-fraud program by breaking them down according to their specific roles.

**Key:** There are eight stages of an effective anti-fraud program—six defensive components and two offensive ones. They are described below.

**Objective:** To optimize the effectiveness of all eight stages. To accomplish that, you must measure how effectively they're being implemented.

**DEFENSIVE STAGES**

*Critical components of effective fraud defense...*

- Deterrence—ensuring that fraud is not attempted.
- Prevention—ensuring that attempted frauds do not succeed.
- Detection—being prepared to discover fraud if it is in progress.
- Mitigation—minimizing losses if a fraud is attempted or carried out successfully.
- Investigation—having the professional and financial resources to discover the "who, why and how" of a fraud incident.
- Prosecution—demonstrating the organization's "zero tolerance" stan-

dard toward fraud by holding perpetrators accountable for their actions.

**OFFENSIVE STAGES**

- Analysis—developing fraud detection models, performing root cause analysis and prediction of the likelihood of a fraud incident.
- Policies—developing clear procedures, processes and "best practices"...as well as proactively implementing internal controls designed to prevent specific types of fraud.

**MEASURING EFFECTIVENESS**

Each defensive stage in the FML has twin goals—to reduce the number of fraud incidents as well as the financial loss from each incident as it is handled in that stage.

**Important:** "Exposure" in this context means the average projected loss from a single fraud incident. You can measure exposure by tracking the loss associated with each incident, and the stage at which it is first discovered.

**Example:** A bank adopted a new prevention initiative that reduced fraud incidents from 5,000 per month to 4,000 by implementing more stringent customer identification and authentication on "high-risk" transactions and by monitoring for adherence to these controls.

**Result:** Exposure per incident dropped from \$6,000 to \$5,000. Total savings were \$10 million—\$6 million from incidents that were prevented, and \$4 million from reduced exposure due to incidents that still occurred.

**Key:** When you can define the savings associated with each stage, you can tell which stages are doing their

*Continued on pg. 4*

**FUTURE FRAUD**

Blake Coppotelli, JD, *Kroll*

## Fraud Ahead: Prepare for the Widening Fraud Threat Now

**K**roll's latest research paints a sobering picture about the current and future threat of fraud for organizations throughout the world.

**Specifics:** Nearly all companies surveyed experienced at least one incident of fraud in the past three years—85% to be exact, with 90% of large organizations indicating they suffered from fraud in that period. That's up by five percentage points since our last survey.

### **WHY CREATE YOUR OWN FRAUD PROBLEM?**

Among the most compelling findings of our recent survey is that more and more companies are causing their own fraud risk. While unintentional, this is a direct result of accelerating entry into high-risk business deals in high-risk geographical areas.

**Details:** Driven by intensifying pressure to meet investor expectations in an increasingly difficult global economic climate, companies are entering into business relationships in industries and geographical areas they are unfamiliar with—without adequate preparation.

We are seeing more and more companies doing deals faster than usual and with less legal and regulatory review and without establishing adequate anti-fraud controls.

**Result:** Pursuing these riskier business "opportunities" often results in doing business in a weakened control structure—which can expose the organization to a host of costly frauds in such high-risk geographical locations as China, India, the Middle East and Africa.

**Example:** While an attractive manufacturing opportunity in Asia may seem prudent and potentially profitable, failing to adequately screen prospective local employees for criminal records...conduct

due diligence on local suppliers...and thoroughly investigate the legal and regulatory pitfalls of adopting local business "procedures"—such as bribing regulatory officials to obtain required permits and licenses—can result in devastating fraud-related repercussions.

If nothing else, such a foray into uncharted business "territory" can easily land your organization in hot water with the US Department of Justice, which in recent years has ramped up its enforcement of the Foreign Corrupt Practices Act (FCPA).

Other frauds victimizing companies in these difficult economic times include fraudulent financial reporting, breach of fiduciary duties, management conflict of interest, theft of confidential information and money laundering.

**Kroll's latest research paints a sobering picture about the current and future threat of fraud throughout the world**

### **URGENT SELF-DEFENSE MEASURES**

*To avoid subjecting the organization to undue risk of fraud as it ventures into business and geographical areas it is not familiar with...*

- Develop internal policies that are effective geographically and across business sectors, and that strictly prohibit violations of anti-fraud based regulations. Train all employees who will be interfacing with overseas business entities about the anti-fraud rules.

- Implement aggressive investigative due diligence procedures covering all prospective business partners, employees, vendors, etc.

- Modify your internal controls framework and legal resources in a way that incorporates anti-fraud measures that can be applied in new types of business relationships in new areas and jurisdictions.

- Require audit rights in all contracts with third parties, including agents and consultants, wherever situated.

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

• Blake Coppotelli, JD, Senior Managing Director of Business Intelligence & Investigations and head of Real Estate Integrity services based in the New York office of Kroll. He can be reached at bcoppotelli@Kroll.com.

*Continued from page 3*

job and which aren't.

### **ARE THEY DOING THE RIGHT JOB?**

It's also important to know if each stage is doing its anti-fraud job efficiently. *Efficiency can be measured in many ways...*

- **Cost/benefit.** This is the cost of each dollar of fraud savings. To measure this, track the savings in each offensive and defensive stage (see above) and the budgetary cost of all anti-fraud activities in that stage.

- **Latency.** Latency is a measure of how quickly an individual case is handled in a particular stage of the FML.

**Important:** Handling a case can involve numerous activities, depending on which stage of the life cycle is being addressed.

**Examples:** For the detection stage, latency is measured from the start of the fraud attempt to the time the attempt is detected. For the investigation stage, latency is measured from the time the case is assigned for investigation to the time all aspects of the investigation are concluded.

- **Support.** Support measures the degree to which a stage helps or hinders anti-fraud efforts at other stages.

**Example:** A bank concerned with employee fraud discovered that its laxity in the prosecution stage hindered deterrence efforts, because employees did not believe the bank was serious about punishing offenders. By beefing up its prosecution efforts, the bank significantly improved the effectiveness of its deterrence stage.

- **Benchmarking.** Benchmarking is a technique for comparing your organization's anti-fraud capabilities against anti-fraud best practices. *You can benchmark your organization against:*

- A comparable organization willing to disclose its fraud experiences and the techniques and strategies that have succeeded in minimizing fraud risk.

- Industry best practices in fraud-risk reduction.

- Prevailing anti-fraud regulatory guidelines and recommendations.

**Example:** The FACT Fair and Accurate Credit Transaction Act was recently amended to require financial institutions to implement broad-ranging programs to minimize the risk of identity theft and fraud. The Federal Trade Commission and the five federal financial institution regulatory agencies issued specific guidance for the detection stage of identity theft. With compliance required by November 1, 2008, financial institutions must now benchmark their anti-identity theft policies and procedures against these regula-

*Continued on page 5*

Continued from page 4

tory standards.

**RETURN ON INVESTMENT**

To invest effectively in fraud reduction, you must know which stages of the FML are achieving their potential, and which need improvement.


**Essential:** Determining which employees and teams are functioning optimally to minimize fraud risk.

**Case study #1:** A telecommunications company recently discovered that its prevention stage was more effective than its downstream stages such as detection, mitigation and investigation and decided to make further investments in this stage.

Evaluation revealed a trained and motivated staff capable of fielding new fraud prevention initiatives quickly and cost-effectively. It was also determined that further improvements in incident reduction in the prevention stage reduced workload in all downstream stages, allowing them to improve their own performance within existing budgets.

**Case study #2:** An E-commerce startup similarly discovered that its prevention stage was much more effective than downstream stages. Evaluation revealed that prevention was largely automated via the use of third-party anti-fraud tools, and did not offer much potential for short-term improvement, whereas the detection stage, which was not yet automated, had the potential for greater savings if detection activities were automated.

**THE BOTTOM LINE**

The Fraud Management Lifecycle can help management determine the specific anti-fraud activities each job function should be doing...how well they are doing the job, and where investment in anti-fraud activities will be most effectively applied. 

**White-Collar Crime Fighter sources:**

•Mike Freiling is Director of Professional Services for the Fraud Management Institute. Mike holds a PhD in Applied Mathematics from MIT, and was named a Henry Luce Scholar at Kyoto University in Japan. Mike can be reached at Mike@toFMI.com.

•Wesley K. Wilhelm, Vice President of Consumer Deposit Risk Management for WaMu. Wesley earned his Masters of Science in Economic Crime Management from Utica College, where he serves as an adjunct professor. He is also a Certified Financial Crimes Investigator. Wesley can be reached at wkwilhelm@comcast.net.

For more information on the Fraud Management Institute, visit <http://www.fraudmanagementinstitute.com>.

**PAYMENTS FRAUD PREVENTION**

Christine Doxey, CAPP, CCSA, *Business Strategy Inc.*

**Do You Know Where Your Disbursements Are Going?**



**Internal Controls for the Shared Services Disbursements Process**

**T**here is little dispute that when the economy is in turmoil, fraud becomes a greater threat than ever. But *what kind* of fraud is most likely to worsen in this environment? From past experience it's clear that one of the areas in which anti-fraud controls may need to be tightened is disbursements.

**LEADING TYPES OF DISBURSEMENT CRIME...**

•**Forged check signatures.** Criminals steal legitimate blank checks, forge the authorized payer signature on the signature line and then forge the endorsements.

**Note:** Forged check endorsements are also a growing problem with valid company checks that have been legitimately signed.

•**Counterfeit checks.** This is the biggest form of check fraud.

•**Altered checks.** This occurs when insiders steal company check stock and alter certain fields.

•**Electronic check fraud.** As ACH transactions increase, companies must ensure that they are not victims of the newest type of fraud—unauthorized ACH transactions

•**Fraudulent manipulation of accounting records** or changing master file records to conceal a “ghost” employee or vendor.

•**Falsifying T&E reimbursement claims** with bogus receipts or claiming personal travel as business travel.

•**Submitting T&E claims twice** through company and personnel credit cards.

•**Manipulating payroll programs**

to increase pay rates.

**SHARED SERVICES FRAUD ISSUES**

Shared services disbursement systems combine the payments processes for accounts payable (A/P), payroll and travel and entertainment (T&E) into a single function. The above list represents a sampling of disbursement frauds that fall into at least one of those areas. Perpetrators can be employees, outsiders or a collusive pair of each.

**ANTI-FRAUD CONTROLS**

To minimize the organization's risk of disbursements fraud in a shared ser-

vices system—especially during difficult economic times—start by implementing these basic controls...

•**Segregation of duties (SoD)** of all planning/initiation, authorization, custody of assets, and recording or reporting of transactions.

**Important:** SoD in a modern information system environment requires separation of on-line approval of transactions, master file initiation, master file maintenance, user access rights and review of transactions.

No individual should have access rights that permit him or her to enter, approve and review transactions.

•**Delegation of authority (DoA).** A company-wide policy that establishes signature authority by level or position within the organization—with officers and employees who delegate their authority remaining responsible for monitoring and reviewing the actions of those to whom authority

Continued on page 6

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



### Fraud Risk Assessments Simplified

With fraud risk assessments (FRA) becoming a top anti-fraud priority for more and more organizations, the guidance paper, *Managing the Business Risk of Fraud*, recently released by the Association of Certified Fraud Examiners, the Institute of Internal Auditors and the American Institute of Certified Public Accountants offers a helpful introduction to the basics of FRAs.

**Background:** According to the guidance, because successful anti-fraud tactics require attempts to outsmart potential fraudsters with a skeptical mindset, the FRA must initially involve asking such questions as:

- How could a fraud perpetrator exploit weaknesses in the system of controls?
- How could a perpetrator override or circumvent controls?
- What could a fraudster do to conceal a fraud?

*With that mindset, the guidance recommends building a FRA on three elements:*

- Identify inherent fraud risk. Gather information to obtain the array of fraud risks that could apply to the organization. Include in this process careful consideration of all types of fraud schemes and scenarios...incentives...pressures...opportunities to commit fraud...and IT fraud risks specific to the organization.

- Assess the likelihood and significance of inherent fraud risk. Assess the probability and potential impact of identified fraud risks based on historical information, known fraud schemes and interviews with staff, including business process owners.

- Respond to likely and significant inherent and residual fraud risks. Determine the proper response to fraud risks and perform a cost-benefit analysis of priorities for implementation of preventive controls or specific fraud detection procedures.

**White-Collar Crime Fighter source:** *Managing the Risk of Fraud: A Practical Guide*, available from the AICPA, www.aicpa.org, the IIA, www.iaa.org or the ACFE, www.acfe.com.

### Disturbing Data on the High Cost of Fraud

A new study by a prominent global consulting firm examined the opinions of partners and other senior executives at 100 US private equity firms regarding their perceptions of the seriousness of fraud among US companies...the risk of fraud to their investments...how important anti-fraud measures are to them...and which measures they consider most effective in preventing fraud.

**Key findings:** 37% of top executives at leading US private equity firms have been exposed to corporate fraud through their investments and 40% said the impact on their investment return was significant. In fact, 59% of the firms have been hit by incidents of fraud of \$1 million or more.

**Significant:** Nearly one-third (29%) indicated they would be willing to pay a higher price (a median of 5% more) for a company that had a comprehensive anti-fraud program in place.

**Also important:** Only 22% of partners and senior executives at private equity firms believe that a company in compliance with Sarbanes-Oxley, including Section 404 of the Act, is adequately protected from fraud. But 66% say that a comprehensive anti-fraud program would be at least somewhat effective in fighting fraud.

**Leading prevention methods:** Private equity investors tend to focus on common and traditional anti-fraud techniques. *They place the highest value on...*

- Conducting criminal and other background checks on potential employees (72%).
- Maintaining a Board and Audit Committee with oversight responsibilities for preventing and detecting fraud (62%).
- Monitoring and updating anti-fraud controls (60%).
- Timely and well-communicated policies regarding appropriate behavior (56%).

**White-Collar Crime Fighter source:** *BDO Consulting Corporate Anti-Fraud Study* by research firm, OSR Group on behalf of BDO Consulting LLP, a provider of litigation, investigation, restructuring and risk advisory services to major corporations, law firms, insurance companies, financial services entities and government entities, www.bdoconsulting.com.

Continued from page 5  
has been granted.

**Helpful:** Some organizations also have a finance manager approve expenditures for amounts above an operational manager's approval level. This anti-fraud control is referred to as the "double key" method.

- Positive pay and payee positive pay.** Positive pay is a widely used service offered by most banks as a means of reconciling accounts and reducing exposure to fraud. It matches checks being presented for payment against those authorized by the paying organization.

**Effective variation:** Payee positive pay allows you to include payees as additional points of comparison between checks presented and the authorized payment file.

- Check controls.** Common anti-fraud controls for A/P, payroll and T&E consist of both built-in system features and manual procedures that help ensure the accuracy and integrity of cash disbursements. *Key controls...*

- Physical controls. In an ideal world, eliminating physical checks would prevent many frauds. However, since checks are still needed for the disbursement process, unprinted check stock should be stored in a locked filing cabinet under dual control.

- Control unopened check stock. Safeguarding of unopened boxes is just as important as control over checks in use.

- Enforce check limits. The system's limitation of the maximum amount of any check can serve as an overall stop-loss control over cash disbursement.

- ACH controls.**

- ACH blocks and filters. A debit block keeps all ACH debits from posting to accounts. Debit filters allow ACH debits from only approved trading partners.

#### SPECIFIC CONTROLS

- Accounts payable controls.** These center around vendor verification controls which include requiring a W-9 with TIN matching for all new vendors...periodic vendor master file clean-up to flag duplicate vendors...screening new vendors against the OFAC file...establishing vendor coding standards... reviewing vendors with the same name operating from multiple addresses...reviewing employees and vendors at the same address and with the same TIN/SSN... reviewing all

Continued on page 7

Continued from page 6

non-PO transactions.

- **Payroll controls.** Screen for ghost employees by performing an annual review where employees sign for live checks or direct deposit slips ...review the gross to net payroll reconciliation process and ensure there are no variances...ensure that all withholding taxes are properly recorded and disbursed to the correct taxation agency...where possible, implement job-rotation in the payroll department.

- **T&E controls.** Review all transactions to ensure that receipts are complete and legitimate...ensure that all approvals are within established DoA policy...screen for travel that is not for business purposes, for repeat submission of expense claims and for exceptions to corporate travel policy.


**Critical:** For all three elements of shared systems disbursements, reconcile all bank account statements within 30 days of receipt. All discrepancies should be investigated immediately.

**PERIOD-END CONTROLS**

All well-structured shared services systems have anti-fraud controls that are exercised during period-end. These controls are designed to help identify errors or irregularities that might have occurred during the prior period. They serve as key internal controls over the accuracy of automated A/P records. *Generally, period end balancing includes three types of balancing and reconciliation:*

- **Balancing the A/P master file with a manual log of control totals.** To verify that the A/P master file was correctly carried forward from the beginning of the period and that activity was correctly posted during the period, a simple reconciliation should be performed at the end of each period.

- **Reconciling the A/P master file to the general ledger (G/L).** As part of the period end process, an accountant will also reconcile the total open vouchers from the open voucher report to the G/L accounts payable liability account. This procedure helps ensure that the interface to the G/L is working properly and that all journal entries shown in the G/L distribution have been properly posted to G/L accounts.

- **Period-end bank reconciliation** (discussed above). 

**White-Collar Crime Fighter source:**

Christine Doxey, CAPP, CCSA, vice president of business development, Business Strategy Inc., a Grand Rapids, MI-based transaction control and payment/procurement consulting firm, www.businessstrategy.com.



# THE CON'S LATEST PLOY...

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

**San Diego, CA**

**Barter fraud, false revenue recognition and other brazen acts of financial crime.** The Securities and Exchange Commission (SEC) filed securities fraud charges against Retail Pro, Inc. (formerly known as Island Pacific, Inc.), and two former CEOs and a former CFO for their alleged roles in an accounting fraud scheme designed to falsely inflate Island Pacific's revenues.

**Details:** In *Securities and Exchange Commission versus Retail Pro, Inc. (fka Island Pacific, Inc.)*, Barry M. Schechter, Ran H. Furman and Harvey Braun, the SEC alleged that Barry Schechter, the former CEO...Ron Furman, the former CFO...and Harvey Braun, another former CEO, misstated \$3.9 million of Island Pacific revenue from a barter transaction.

According to the SEC complaint, the barter transaction—with an Australian software company called QQQ Systems Pty Limited—was a sham orchestrated only to artificially inflate Island Pacific's revenues.

**Added charges:** As a result of improperly recognizing and reporting the \$3.9 million as revenue, Island Pacific overstated its revenues by 140% for the second quarter of 2004, 29% for the nine months ending the third quarter of 2004, and 22% for the 2004 fiscal year. In addition, Island Pacific reported a small profit instead of a massive loss for the second quarter of 2004.

**The "deal":** Schechter concluded a software license agreement between Island Pacific and QQQ one day before the close of a quarter, granting QQQ rights to distribute Island Pacific's "Host" software in Australia and New Zealand. As part of the "arrangement," QQQ agreed to pay Island Pacific, at QQQ's option, either: \$3.25 million in two equal installments of \$1.625 million...or 0% of QQQ's net sub-licensing

fees to a maximum of \$4 million.

Pursuant to that agreement, on the last day of the quarter, Island Pacific shipped software to QQQ.

**Key detail:** Just prior to signing the license agreement, QQQ's CEO received a side letter from Island Pacific, signed by Braun at Schechter's direction, confirming that, in addition to the license agreement, Island Pacific and QQQ were simultaneously negotiating, among other things, Island Pacific's purchase of QQQ's "Pyramid" software.

The side letter also stated that the payment terms extended to QQQ in the first license agreement would be changed to coincide with the closing date of the second transactions described in the side letter.

One month later, Schechter and Furman allegedly caused Island Pacific to recognize the \$3.25 million in revenue from the License Agreement and to record on Island Pacific's books a \$3.25 million account receivable from QQQ.

**Insult to injury:** Without QQQ's knowledge, Schechter and Furman allegedly changed three key terms of the initial license agreement—what was being sold, the price and the payment terms. They modified the agreement to grant QQQ a license to distribute two Island Pacific programs, "Host" and "Direct," and to state that QQQ agreed to pay Island Pacific \$3.25 million for Host and \$650,000 for Direct, payable in two equal installments, plus 10% of QQQ's net sub-licensing fees.

**Result:** Schechter and Furman recorded an *additional* \$650,000 in Island Pacific revenue and accounts receivable, for a total of \$3.9 million in bogus revenue.

**The cover-up:** The SEC charges that Schechter and Furman concealed the fraud from Island Pacific's outside auditors and the public by creating

forged and backdated documents in an attempt to show that recognizing revenue from the transaction was proper. In addition, the complaint alleges that Schechter sold 637,750 shares of Island Pacific stock for more than \$1.5 million during the fraudulent scheme.

**New York, NY**

**R**evue recognition case #2: SEC **R**nails a “big fish.” General Electric Co. said the US Securities and Exchange Commission plans to recommend a civil complaint against the company in a three-year-old probe that includes the way it recognizes revenue and presents cash flow.

The SEC issued a so-called Wells notice Sept. 4, GE said in a regulatory filing after the close of US markets. Wells notices typically give the recipient an opportunity to dissuade the agency from proceeding. GE is reportedly in preliminary settlement discussions on the details of the case with the SEC.

However, the SEC probe and internal corporate investigations have spanned the company’s finance, aviation, health-care and energy units and led to the firing of “a few” workers at the locomotive unit.

The investigations led to restatements that the company has said

reduced its profit by a net \$297 million, or 3 cents a share, out of about \$118 billion from 2001 to 2007.

The SEC may seek to impose fines, an order barring further violations, and “other relief within the Commission’s authority,” GE said in the filing.

**Background:** The investigation started in January 2005 and is one of the key, albeit less publicized, business problems that has been weighing on GE’s share price ever since.

GE has restated net income twice as part of the investigation and its internal investigation. The company made adjustments in the past year including in January, when it moved some profit for 2002 to subsequent years.

That disclosure, made the day GE announced fourth-quarter 2007 results in January, stemmed from accounting errors regarding profits from long-term service contracts, including those for its aviation spare-parts unit. The restatement cut per-share profit for 2002 by \$770 million, or about 8 cents a share, with most moved into subsequent years.

Among other steps, GE has hired law firms to help with the SEC and audit issues.

**Detroit, MI**

**M**ortgage fraud: Case demonstrates how even the “good


guys” were in on the bonanza in home loan fraud. A former Detroit cop and a City of Detroit property appraiser were indicted in a \$2.1 million mortgage fraud case.

**Details:** According to the Detroit U.S. Attorney’s office, former police officer Pierre Greene, city appraiser Jacque Miller, and Sandy Robinson of Detroit were named in an 11-count indictment charging them in a property-flipping scheme.

The indictment states that from January 2004 to December 2006, the three obtained fraudulent mortgage loans on more than 35 properties in Detroit. They allegedly bought run-down properties for a few thousand dollars, obtained inflated appraisals claiming the properties were worth as much as 10 times the actual value, and paid people to act as straw buyers to apply for mortgages.

After getting the mortgages, they simply walked away from the payments, leaving mortgage companies on the hook for largely worthless property. Three banks, all based elsewhere, were the biggest losers in the scheme, authorities said.

Court papers noted that the defendants provided the straw buyers with phony credit and personal financial documents to make them appear creditworthy.

**Lesson:** These schemes are known to have been perpetrated by the thousands, if not tens of thousands in recent years, when banks were approving virtually anyone for mortgages whether they could afford them or not. However, it is noteworthy that this situation—which prevailed during the late 1990s and early 2000s—created such a tempting promise of “easy money” that even fundamentally honest, law-abiding individuals succumbed to the temptation to break the law. 

**COMING SOON IN**

**White-Collar Crime Fighter...**

- Lessons from the role of fraud in the latest financial crisis
- Audit committee, board and management team: Clarifying the fraud role confusion
- Protecting against the growing threat of industrial espionage
- Secrets of successful forensic data-mining



**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](http://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](mailto:subscribe@wccfighter.com)