WHITE-COLLAR CRIME FIGHTER

YOUR *SECRET WEAPON* IN THE WAR ON FRAUD

www.wccfighter.com

Vol.17 No.4
July-August, 2015

Kevin E Doyle, CPA, CFE, CFF, CGMA

How to Develop and Implement Effective Anti-Fraud Training in Your Organization

The importance of anti-fraud training cannot be overstated. Based on the recent Association of Certified Fraud Examiners (ACFE) *2014 Report to the Nations on Occupational Fraud and Abuse*, less than 50% of respondents say they provide anti-fraud training to their employees, yet companies lose an average of 5% of their top line revenue to fraud – *every year!*

These two statistics appear to be counterintuitive. Typical companies lose money to fraud, yet more than one-half of the surveyed companies don't provide necessary training to help minimize or prevent such losses.

Employees are, however, by far the best asset to wage the fight against fraud. *Educated* employees enhance that impact. We accountants are notorious for wanting more and more review, additional levels of approval, multiple signatures, etc. Yet such recommendations must be balanced against head count, payroll costs and the like.

Key: Just think of the positive impact your company will get by having many more pairs of eyes supporting the company's need to minimize its business risk of fraud. It's a win, win; additional control with little incremental cost…a viable investment in the workforce.

Caution: This is not to suggest that training will arm employees to be fraud investigators but it can enable them to identify a possible issue and then have the wherewithal to properly report it.

IN THIS ISSUE

Caution: Your training should make it clear that should an employee witness a possible violation of law or company policy, they must *not* act on it other than to report it. Too often I have been involved in investigations where the proper reporting protocols were not followed which led to evidence spoilage, interference and other complications.

BE ADAPTABLE

As you can imagine no single training platform can work for every organization. The determination of an effective program must be the result of an exhaustive collaborative process that considers management goals and objectives, culture (corporate and geographic), industry, risk vulnerabilities, cost benefit, etc.

Helpful: The American Institute of Certified Public Accountants, The Institute of Internal Auditors and the ACFE have developed a guidance paper called *Managing the Business Risk of Fraud: A Practical Guide*. The paper provides general guidance on establishing an environment to effectively manage an organization's fraud risk. I encourage you to use it as a resource. It has tools, outlines and other information that discusses effective fraud risk mitigation processes including anti-fraud training.

When it comes to training, the adage "what gets written, gets done" is very appropriate. Fraud and/or ethics training should be included as part of overall corporate training and tailored to address roles and responsibilities. *This achieves important objectives:*

- It advises employees about the investment the company is making in doing the right thing.
- It reinforces the "tone at the top" – based on an anti-fraud culture.

Recommended: A change in employee status should include training to reflect his or her new duties. Another effective measure is to include fraud/ethics training as part of employee annual goal setting. Consideration should be given to requiring employees take a post-session quiz, questionnaire etc. and achieve a "passing" score that measures desired comprehension goals.

Essential: Fraud/ethics training must be required for all new hires. Other elements of new hire training should include code of conduct, policies and procedures, their role within the internal control framework and fraud prevention and detection, whistleblower policy etc.

White-Collar Crime *FIGHTER*

Editor
Peter Goldmann, MSc, CFE

Consulting Editor
Jane Y.Kusic

Managing Editor
Juliann Lutinski

Senior Contributing Editor
David Simpson

Associate Editor
Barbara Wohler

Design & Art Direction
Ray Holland, Holland Design

Panel of Advisers

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 Inc.

Corporate Integrity and Compliance
Martin Biegelman, Deloitte

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 Internet Fraud
Richard Cuscarino, CIA, CISM, CRM Richard Cuscarino & Associates

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

LEGAL GUIDELINE

Part B, Chapter 8 of the U.S. Sentencing Guidelines (Guidelines) lay out prescriptive steps that an organization must consider to prevent and detect criminal conduct. One such step is as follows:

> *Communicate the program's standards and procedures throughout the organization, including training that is tailored to members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and applicable agents of the organization.*

Accordingly, in many corporations, an effective training program is not only a good idea, but required.

In closing here are a couple of additional training suggestions:

- Fraud topics to consider covering in your fraud training:
  - ✓ FCPA and UK Bribery Act (US-based companies operating in a foreign country must be particularly sensitive about local business practices/cultures which may be in conflict with US laws and regulations.)
  - ✓ Commercial bribery
  - ✓ Expense report schemes
  - ✓ Time and billing schemes
  - ✓ Money laundering
- Tailor the content based on industry, regulatory environment, legal standards, ect.
- Formalize a reporting protocol for employees who observe a possible violation of law or company policy.
- Consider live and on-line training; balance cost/benefit
- Include fraud professionals to provide training
- Compile and measure effectiveness of training

***White-Collar Crime Fighter* source:**
Kevin E Doyle, CPA, CFE, CFF, CGMA, independent fraud investigation consultant and former senior internal auditor at a leading international hotel and resort company.

Payroll Fraud: Best Prevention Practices

■ **Segregate payroll duties.** The new hire "onboarding" process comes with a unique set of fraud risks.

Example: Personal and banking information may be exposed as a new hire provides personal data online and/or on paper.

Recommended: Have validation of employee information conducted by individuals outside the payroll function.

Key: The objective of segregating duties is not to add cost or work but to identify where an opportunity for fraud may exist—and neutralize it. The focus should be on segregation of duties between individuals— not functions. Segregation of duties and regular rotations of individuals in key functions prevents the potential for collusion.

- **Inspect payroll offices and computers regularly.** On one of my first audit assignments, my manager had a sign on her desk that read "People rarely do what you expect, but often what you inspect."

  Lesson: Experience has taught me this is more than just a simple parable. Regular inspections of the payroll office and the payroll records by someone outside of the payroll department are valuable to help reduce exposures to loss.

  Hardware and software used to record new employee data should be regularly reviewed to ensure they are free from electronic devices such as key loggers or other hidden "malware" programs that surreptitiously gather data.

- **Audit the communication path.** When money and records are exchanged between the payroll provider and the employer, there is a shared exposure to loss.

  Self defense: At all points of the communication path, the technology team must ensure the link that they oversee is protected from exposure and is regularly audited for unintended content that could alter or compromise data. Whenever possible, a closed loop communication is preferable.

- **Avoid complacency.** The repetitive nature of the payroll process lends itself to potential complacency on the part of those in charge of the process.

  Result: Regular oversight and vigilance remain critical aspects of payroll fraud prevention. Understanding the mutual security practices and technology offerings of both the payroll provider and employer is critical when transferring data and money.

- **Perform exception reporting.** Exception reporting that highlights certain aspects of payroll transactions is helpful in reducing fraud risk.

  Examples: Changes made to employee bank accounts … anomalies in check amounts … differences in frequencies of pay … and withholding changes are all transactions worthy of exception oversight.

  The key to good exception reporting is developing data reports based on anomalies in such a manner that reviews can be done efficiently without a high degree of false positives. Efficient exception reporting not only helps in identifying potential fraud but also heightens awareness and enhances the perception of detection.

White-Collar Crime Fighter* source*:
Paul Cogswell, JD, CFE, CPP, Senior Managing Director, McGovern & Greene LLP, www.mcgoverngreene.com

How to Protect Your Computer System

Any computer system can collect event logs, but most security operations do a poor job of filtering them to find evidence of malicious activity. *Here's where to start…*

Most event logs are primarily useless "noise" that obscures the entries most defenders should be analyzing.

Better: "Less is more" event logging, where thoughtful filtering significantly improves the value of your logs. When I hear a security event log team buying petabytes of disk storage for their event logs, I know they're inefficient.

Worse: Most companies lack a clear understanding of what logs they have — or should be collecting — especially which types of malicious events these logs might possibly detect.

Over the last year I've seen many organizations creating matrices — usually in spreadsheets— that detail every log that the company's assets are either generating or could generate. It includes a list of every computer device (and sometimes written logs to capture physical attacks), as well as workstations, mobile devices, servers, routers, firewalls, proxies, switches, antimalware software, application logs, and more. Many of these devices generate dozens of logs.

Example: A Microsoft Windows server. Nearly everyone has worked with the basic Windows event logs — Application, Security, and System — for years. But ever since Windows Vista and Windows Server 2008, Windows event logs have included dozens of filter logs, each detailing a particular application or process. Examples include AppLocker, Authentication, BitLocker, Bluetooth, Code Integrity, Group Policy, NTFS, Task Scheduler, UAC-FileVirtualization, and WER-Diagnostics.

Key: These individual filtered logs are a great way to focus your forensics.

A STEP FURTHER

Beyond built-in (or custom-created) Windows event logs, a typical Windows computer may also have a handful to dozens of other logs. Search on *.log to see what I mean. Web servers have Web server logs. If you're using Windows Firewall, events are usually saved to a file called pfirewall.log. You'll find install logs, Windows Update logs, patch logs, diagnostic logs, VPN logs, and usually dozens of application logs. Non-Windows computers will have many, many log files as well. Even your antimalware systems and devices have multiple log files.

HOW SHOULD YOU DEAL WITH THIS GLUT OF DATA?

Start with these two steps:

1) **Do an inventory.** List all devices that have log files, the purpose of the log file, the names and locations of the log files, log formats, possible events, current and maximum log file sizes, and anything else that might prove useful (rotation method, backup method, retention period, and so on).

2) **Determine which type of malicious events your log files can detect.** Create a matrix along the other axis of the spreadsheet, then highlight the strengths, gaps, and weaknesses. I often see companies use colored shading (such as red, yellow, and green) to quickly highlight the conclusion.

Even though your event log matrix is likely to result in dozens of rows and columns, in one place you'll quickly be able to note your areas of vulnerability. You can fine-tune your event log collection process or buy additional tools along the way. But without creating this type of matrix, you'll never be aware of your strengths and weaknesses — at least, not at a glance.

UNKNOWN SYNERGIES

My favorite part of the process is finding areas of synergy that you never knew you had.

Example: I've been pushing my customers to enable application control programs to generate events whenever a new, unexpected program or process is executed. Whenever a new malicious program or process is noted (and hopefully stopped) by your anti-malware software, the detection can be compared to when the program or event first appeared.

The difference between those two events is the real risk horizon for that malicious event. I call it mean time to detection. The more you can shorten this metric, the better job your anti-malware software will perform, and the lower the risk you have (from that particular scenario).

Bottom line: Effective malicious event management isn't easy. But without an accurate event log matrix you won't have a solid understanding of what you have and what needs to be fixed…let alone what you need to look for in a cyber-security investigation.

White-Collar Crime Fighter **sources:**

- "Enter the Matrix: Track Down Hacks with Log Files", article by Roger Grimes, leading computer security expert, writing at InfoWorld.com, www.infoworld.com
- "Spotting the Adversary with Windows Event Log Monitoring," by National Security Agency/ Central Security Service, https://www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf
- "An Analysis of Microsoft Event Logs", by Michelle Mullinix, Utica College, http://programs.online.utica.edu/pdf/Mullinix_4_Gonnella_An_Analysis_of_Microsoft_Event_Logs_December_2013.pdf

How to Beat Cyber-Criminals at their Own Game

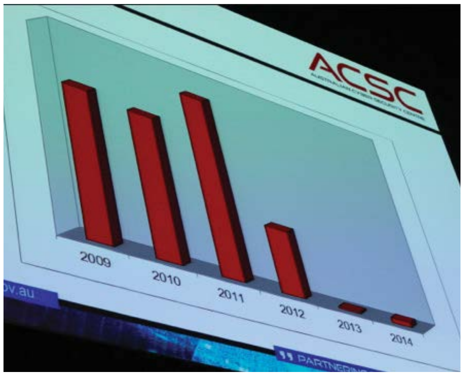
Australian Signals Directorate (ASD) deputy director, Steve Day says hackers have failed to extract any sensitive information from Federal Government agencies for the last two years despite successfully breaching several networks. (The ASD is Australian Signals Directorate—a unit of the Defense Department. It is the unit bearing primary responsibility for government information security).

Day attributes the success to agencies following the so-called **"Top 4 security controls"** developed by ASD Cybersecurity Technical Director, Steve McLeod and colleagues. *The "Top 4" are:*

- Application whitelisting
- Patching applications regularly
- Patching operating systems regularly
- Minimizing admin privileges.

Day said thanks to the top four strategies having been consistently implemented, "There were no compromises of Australia Government agencies between mid-2013 to mid-2015."

Added defense measures: Day says hackers failed to steal data thanks to the education regime behind the top four controls push, coupled with regular audits of Federal Government agencies forced to implement the controls.



Day points to a chart illustrating the number of network intrusions into Federal Government agencies since 2009. Prior to that date the agency lacked insight into government agency breaches. "We had some pretty bad years", Day said.

Important: Day said the time it took ASD to discover breaches has fallen from about nine months “a few years ago” to a matter of weeks.

Next steps: Day also announced that the Federal Government’s Cyber Security Center will house representatives from seven telecommunications organizations to develop information sharing mechanisms, although he did not put a deadline on the initiative.

He says he would envision for the future that the Cyber Center will have “footprints” in each capital city to build face-to-face industry relationships.

***White-Collar Crime Fighter* source:**
Major General Steve Day, deputy director, Australian Signals Directorate, quoted in *The Register,* www.theregister.co.uk

Avoid Legal Traps in Managing Whistleblowers

The Securities and Exchange Commission (SEC) recently announced its first enforcement action against a company for using excessively restrictive language in confidentiality agreements that can potentially stifle the whistleblowing process.

Details: The SEC charged Houston-based technology and engineering firm, KBR Inc. with violating whistleblower protection Rule 21F-17 enacted under the Dodd-Frank Act.

KBR required witnesses in certain internal investigations interviews to sign confidentiality statements with language warning that they could face discipline and even be fired if they discussed the matters with outside parties without the prior approval of KBR’s legal department. Since these investigations included allegations of possible securities law violations, the SEC found that these terms violated Rule 21F-17, which prohibits companies from taking any action that could impede whistleblowers from reporting possible securities violations to the SEC.

Result: KBR was fined $130,000 to settle the SEC’s charges and the company voluntarily amended its confidentiality statement by adding language making clear that employees are free to report possible violations to the SEC and other federal agencies without KBR approval or fear of retaliation.

From Andrew J. Ceresney, Director of the SEC’s Division of Enforcement: “By requiring its employees and former employees to sign confidentiality agreements imposing pre-notification requirements before contacting the SEC, KBR potentially discouraged employees from reporting securities violations to us. SEC rules prohibit employers from taking measures through confidentiality, employment, severance, or other type of agreements that may silence potential whistleblowers before they can reach out to the SEC. We will vigorously enforce this provision.”

Important legal detail: According to the SEC’s order instituting a settled administrative proceeding, there are no apparent instances in which KBR specifically prevented employees from communicating with the SEC about specific securities law violations. However, according to the Commission, *any company’s blanket prohibition against witnesses discussing the substance of the interview has a potential “chilling effect” on whistleblowers’ willingness to report illegal conduct to the SEC.*

Upshot: KBR changed its agreements to make clear that its current and former employees will *not* have to fear retaliation or seek approval from company lawyers before contacting the SEC.

Recommended by Sean McKessy, Chief of the SEC's Office of the Whistleblower. "Other employers should similarly review and amend existing and historical agreements that in word or effect stop their employees from reporting potential violations to the SEC."

***White-Collar Crime Fighter* source:**
Securities and Exchange Commission (SEC), www.sec.gov

THE CON'S LATEST PLOY…

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

New York, NY.

Blow the whistle and the government just might listen. The Federal Government reached a $60 million settlement of a civil fraud lawsuit against specialty pharmaceutical services provider, Accredo Health Group ("Accredo") concerning a kickback scheme with industry giant, Novartis Pharmaceuticals Corp. ("Novartis") involving the prescription drug Exjade.

And there's more: In addition to filing a Notice of Intervention against and Stipulation and Order of Settlement and Dismissal with Accredo, the Government elected to intervene against Novartis over the same misconduct previously reported by a whistleblower.

Allegation: Novartis provided kickbacks, in the form of patient referrals and related benefits, to Accredo in exchange for Accredo's recommending refills to Exjade patients. In connection with the scheme, the defendants understated the serious and potentially life-threatening side effects of Exjade when promoting the drug's benefits to patients.

Important: Simultaneous with the filing of the Notice of Intervention against Accredo, U.S. District Judge Colleen McMahon approved a settlement to resolve the United States' claims against Accredo. Under that settlement, Accredo agreed to pay $45,060,598.87 to the United States … admitted numerous facts concerning its relationship with Novartis … and agreed to cooperate with the United States in the prosecution of the claims against Novartis. Accredo also agreed to pay $14,939,401.13 to a group of states to settle the states' claims based on the same alleged conduct.

Background from Manhattan U.S. Attorney Preet Bharara: "As alleged in our intervention papers, Novartis used Accredo to promote refills under the guise of purported 'counseling' and 'education,' and in doing so, Novartis caused patients to receive one-sided advice that did not discuss Exjade's serious, potentially life-threatening, side effects. This settlement with Accredo restores to the public tens of millions of dollars paid out for kickback-tainted drugs."

As alleged in the Government's second amended Complaint, Novartis markets and manufactures Exjade, a drug approved for use by patients with iron overload resulting from blood transfusions. For approximately five years until 2012, Novartis ran a scheme whereby it offered kickbacks, in the form of patient referrals and other benefits to certain specialty pharmacies, including Accredo and Bioscrip, in exchange for increasing their Exjade refills through biased recommendations to patients. Accredo and Bioscrip were part of a Novartis-created exclusive distribution network for Exjade called the Exjade Patient Assistance and Support Services ("EPASS"), and through this network Novartis was able to refer Exjade patients to particular pharmacies within the network.

Key details: The Government elected to intervene in a related complaint with respect to its allegations concerning Novartis and Accredo's participation in an Exjade patient referral allocation scheme. Through the alleged scheme, Novartis gave Accredo additional patient referrals and related benefits in return for Accredo achieving the highest refill percentage for Exjade patients as compared to the refill percentages among Exjade patients at the other two pharmacies in the closed distribution network that Novartis had established for Exjade.

As part of its settlement with the United States, Accredo made extensive factual admissions, including that:

- Accredo was one of three specialty pharmacies permitted to dispense Exjade as part of EP-ASS, Novartis's distribution network for Exjade.
- Novartis controlled how many of the patient prescriptions received by EPASS were distributed among Accredo and the other two EPASS pharmacies.

Keeping score: In June 2007, Novartis began issuing monthly "Exjade Scorecards" to the EPASS pharmacies that measured, among other things, the pharmacies' "adherence" scores. Based on discussions with Novartis, Accredo knew that the "adherence" scores in the Exjade Scorecards were designed to show how long Accredo's Exjade patients continued to order refills. Accredo also knew that, in calculating the adherence scores, Novartis did not exclude patients who stopped ordering refills due to side effects or patients who were directed to stop therapy by their physicians.

In late 2007 and early 2008, Novartis indicated to Accredo that Novartis was dissatisfied with Accredo's performance in terms of its "adherence" scores in the Exjade Scorecards. Novartis executives asked Accredo executives to implement an Exjade adherence improvement plan that involved additional nurse intervention. Novartis executives also told Accredo that Accredo could lose undesignated patient referrals from EPASS if it continued to lag behind other EPASS pharmacies in the Exjade Scorecards.

At a meeting in March 2008 with Accredo, a Novartis executive underscored the importance to Novartis of Accredo's adherence performance. Later that month, Novartis told Accredo that Novartis was formulating a plan to allocate undesignated patient referrals to the EPASS pharmacies based on their rankings in the Exjade Scorecards. Specifically, the EPASS pharmacy with the top adherence score in the Exjade Scorecards would receive a larger share of the undesignated patient referrals as compared to the other EPASS pharmacies. In addition, between April and June 2008, Novartis managers told Accredo that Accredo's performance in the Exjade Scorecards was below Novartis's expectation and this affected Novartis's ability to meet its sales targets for Exjade.

In July 2008, Novartis executives reiterated in statements to Accredo that Novartis was dissatisfied with Accredo's performance in relation to Exjade. Later that month, Accredo hired a new nurse for Exjade and assigned that nurse to make a sequence of calls to each Exjade patient.

In making calls to Exjade patients, the nurse at Accredo was supposed to follow a set of call protocols that Accredo had developed. Accredo's 2008 call protocols directed the nurse to tell patients that compliance with Exjade therapy regimen is extremely important and that, if untreated, iron overload could result in arthritis, liver or heart problems, high blood sugar, persistent abdominal pain, severe fatigue, and skin discoloration. With regard to adverse reactions, Accredo's 2008 Exjade call protocols directed the nurse to advise patients about Exjade's common adverse reactions, including diarrhea, abdominal pain, fever, and rash, but not the less common, but more severe, adverse reactions like renal or hepatic impairment.

In October 2008, Novartis informed Accredo about, and Accredo agreed to, a new patient referral allocation plan that Novartis had formulated. Under that plan, Novartis would allocate 60 percent of all undesignated patient referrals to the EPASS pharmacy with the top "adherence" scores in the Exjade Scorecards and allocate 20 percent of the undesignated patient referrals to each of the other two EPASS pharmacies.

In February 2009, an Exjade executive from Novartis visited Accredo and met with the Exjade nurse at Accredo. During that meeting with the Novartis executive, the Exjade nurse at Accredo described how she handled calls with Exjade patients.

In January 2010, the FDA required Novartis to add a "black box warning" to the Exjade label to highlight that Exjade may cause renal impairment (including renal failure), hepatic impairment (including hepatic failure), and gastrointestinal hemorrhage. The FDA-mandated warning also stated that these reactions were fatal in some reported cases.

After January 2010, no representative of Novartis asked or suggested to Accredo that its Exjade call protocols should be revised to require the Exjade nurses to discuss the serious risks listed in Exjade's "black box warning" when they called patients to discuss Exjade therapy.

In February 2010, Accredo updated its Exjade call protocols. In terms of the adverse reactions for Exjade, the February 2010 Accredo Exjade call protocols continued to direct the Exjade nurses to advise patients about the common adverse reactions, such as diarrhea and rash, but not the less common, but more severe, adverse reactions discussed in the "black box warning," such as renal or hepatic failure. As revised, the February 2010 Exjade call protocols directed the nurses to tell Exjade patients that "compliance with Exjade is very important in order to prevent the following complications that result from untreated iron overload: arthritis, high blood sugar, persistent abdominal pain, severe fatigue, skin discoloration, stroke, or death."

Critical detail: The allegations of fraud stated in the Complaint were first brought to the attention of federal law enforcement by David Kester, the whistle-blower who filed a lawsuit under the False Claims Act. The False Claims Act permits the Government to recover up to three times the amount of damages incurred by the United States, plus civil penalties ranging from $5,500 to $11,000 per violation. Private parties who have knowledge of fraud committed against the Government may file suit on behalf of the Government and share in any recovery. The United States may then intervene and file its own lawsuit for treble damages and penalties, as it did in this case.

Chicago, IL.

Veteran "big beer" marketing executive exploited control loopholes to the tune of $7 million. Former MillerCoors marketing executive, David Colletti was indicted along with seven others for allegedly perpetrating a scheme to defraud the Chicago-based brewing company of at least $7 million.

The alleged scheme: Submitting false invoices and falsely billing MillerCoors for fictitious promotional events and inflating prices for other events held to market and promote the company's products. The indictment alleges Colletti, who oversaw the marketing and sale of beer to restaurants and bars, approved several of the false invoices, for which MillerCoors paid more than $7 million to third-party bogus companies controlled by the other defendants. Colletti in turn allegedly received a portion of those payments.

Colletti, who worked for the brewing company from 1982 to 2013, and the other defendants then used the money to pay for personal expenses, collectible firearms, international golf trips, hunting trips, investments in a hotel and bar and an arena football team, according to the indictment.

It gets worse: MillerCoors separately filed suit against Colletti and another former marketing executive, Paul Edwards, along with several other people and 15 companies in multiple states. That suit alleges the defendants embezzled more than $10 million from MillerCoors through fake invoices and other undelivered services over more than a decade.

Control failure: That suit claimed Colletti's scheme avoided detection until 2013 because he directed the payments from an internal MillerCoors budget he controlled. The lawsuit states Colletti was the sales director for national on-premise chain accounts from 1992 to 2001 and was promoted in 2002 to senior director of the division. His office moved to Chicago from Milwaukee in 2009 after Miller Brewing entered into the MillerCoors joint venture. It alleged he and his wife, Pamela, created a shell company to hold the embezzled funds.

The Milwaukee County case has been stayed pending the outcome of the criminal investigation.