

Chapter Board of Officers

President: Linda L. Saunders, CFE, CPA, CGFM
Owner, Forensic Accounting Consulting (206) 842-4809
forensicCPA@compuserve.com
Bainbridge Island, Washington

Vice-President: Norman J. Gierlasinski, PhD, CFE, CPA, CIA
Professor, Central Washington University (206) 439-3800, Extension 3825
normang@cwu.edu
SeaTac, Washington

Secretary-Treasurer: Joseph R. Dervaes, CFE, CIA (360) 710-1545
Association of Certified Fraud Examiners Fellow
Chairman of the Board of Regents, Association of Certified Fraud Examiners
Audit Manager for Special Investigations, Washington State Auditor's Office
dervaesj@sao.wa.gov
Port Orchard, Washington

Director-At-Large: Roger B. Gulliver, CFE, CPA, CISA, CBA
Owner, Robert B. Gulliver, CPA (253) 735-2392
RBG@halcyon.com
Auburn, Washington

Director-At-Large: Bernadette McBride, CFE, CPA
Investigator, Medicaid Fraud Control Unit, Attorney General's Office (360) 697-3342
bernadette7@sprintmail.com
Poulsbo, Washington

Chapter Training and Meeting Dates

Future fraud training events for **calendar year 2001** are as follows:

December 4, 2001: Joint Chapter and WSCPA Annual Fraud Conference, Marriott Hotel, SeaTac. **Register directly with the WSCPA by calling 1-800-272-8273 (Bellevue, WA).** The cost of the conference is \$175, and includes continuing professional education for six hours of Technical and two hours of Accounting and Auditing. The course registration form can also be obtained from the WSCPA's web site at "www: wscpa.org/wscpa/CPEVcrity/cpe". However, you must call the WSCPA to actually register for the conference. Ask for Lisa Chin-Itawa in the Education Department.

Future fraud training events for **calendar year 2002** are as follows:

February 27, 2002: Chapter Fraud Training Seminar on Gypsy Con-Games and Crimes presented by Rob Floberg, a Pierce County Sheriff's Department Detective; Downtown Seattle. **(NOTE)**

April 25-26, 2002: Joint Chapter and Association of CFE's two-day Fraud Conference; Doubletree Inn, SeaTac. **Register directly with the Association of CFE's by calling 1-800-245-3321 (Austin, TX).** The cost of last years conference was \$225 for one day and \$350 for both days. Ask for Diane Neill at conference registrations for all the details and the current cost. Or, you may also register on-line at the Association's web site: "[www: marketplace.cfenet.com/register/SeminarDetail](http://www.marketplace.cfenet.com/register/SeminarDetail)".

June 26, 2002: Annual Chapter Business Luncheon Meeting and Fraud Training Seminar; Best Western Hotel Southcenter; Tukwila. Topic and speaker to be determined.

August 4-9, 2002: 13th Annual Fraud Conference, Association of Certified Fraud Examiners; Renaissance Hollywood Hotel; Los Angeles, CA. **Register directly with the Association of CFE's by calling 1-800-245-3321 (Austin, TX).** The cost of last years conference was \$350 for the one-day pre-conference (4th), \$895 for the 2.5 day annual fraud conference (5th-7th), and, \$595 for the two-day post-conference (8th-9th). Ask for Diane Neill at conference registrations for all the details and the current cost. Or, you may also register on-line at the Association's web site: "[www: fraudconference.com](http://www.fraudconference.com)".

August 28, 2002: Chapter Fraud Training Seminar; Downtown Seattle. Topic and speaker to be determined. . **(NOTE)**

October 30, 2002: Chapter Fraud Training Seminar; Downtown Seattle. Topic and speaker to be determined. . **(NOTE)**

December 3, 2002: Joint Chapter and WSCPA Annual Fraud Conference, Marriott Hotel, SeaTac. **Register directly with the WSCPA by calling 1-800-272-8273 (Bellevue, WA).** The cost of the conference should be \$175, and includes continuing professional education for six hours of Technical and two hours of Accounting and Auditing. The course registration form can also be obtained from the WSCPA's web site at "www: wscpa.org/wscpa/CPEVcrity/cpe". However, you must call the WSCPA to actually register for the conference. Ask for Lisa Chin-Itawa in the Education Department.

(NOTE): Please note our new starting time for Chapter Fraud Training Seminars in our downtown Seattle location. The meetings will begin at 2:30 p.m., have a one-half hour networking session in the middle, and end at 5:00 p.m. for 2 hours of CPE.

Be sure to mark these important dates on your training schedule and plan to attend.

Web Site Under Construction

The Chapter's web site is currently under construction. Webmaster Ken Hansen is working hard to make this a reality. We anticipate that the site will be operational by the end of the calendar year. In addition to joining the technology world, the web site will give us the capability to deliver the bi-monthly Chapter newsletter to you electronically. As soon as the site is activated, we will stop mailing the newsletter to those inside and outside of our Chapter who have been interested in our activities. This action will save the Chapter about \$2,000 per year.

What to do if you Lose Your Wallet or Purse

You probably already know all this... but it's a good reminder. A anonymous corporate attorney sent this out to the employees in his company. It is now passed along to you for information purposes. The Chapter Board of Officers hopes you find the information useful. We sincerely hope you do not experience this situation up close and personal. If you do, your life can be altered significantly for a long period of time. Similar nightmares abound everywhere. Beware!

We've all heard horror stories about fraud that's committed in your name, address, Social Security number, credit, etc. Unfortunately, I (the author of this piece who happens to be an attorney) have firsthand knowledge because my wallet was stolen last month and within a week the thief(ves) ordered an expensive monthly cell phone package, applied for a VISA credit card and had a credit line approved to buy a Gateway computer.

But here's some critical information to limit the damage in case this happens to you or someone you know. As everyone always advises, cancel your credit cards immediately. The key is having the toll-free numbers and your card numbers handy so you know whom to call. Keep this information where you can find it easily. File a police report immediately in the jurisdiction where it was stolen. This proves to credit providers you were diligent, and is a first step toward an investigation (if there ever is one).

But here's what is perhaps most important (I never ever thought to do this). Call the three national credit reporting organizations immediately to place a fraud alert on your name and Social Security number. I had never heard of doing that until advised by a bank that called to tell me an application for credit was made over the Internet in my name. The alert means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit. By the time I was advised to do this, almost two weeks after the theft, all the damage had been done.

There are records of all the credit checks initiated by the thieves' purchases, none of which I knew about before placing the alert. Since then, no additional damage has been done, and the thieves threw my wallet away this weekend (someone turned it in). It seems to have stopped them in their tracks. The numbers are:

Equifax: 800-525-6285
Experian (formerly TRW): 888-397-3742
Trans Union: 800-680-7289
Social Security Administration (fraud line): 800-269-0271

Additional information provided by another source on this issue follows. Do not carry your Social Security card in your wallet or purse. Also, make a copy of everything you carry in your wallet or purse so that you have a record of what was in there and can make the necessary calls.

The Chapter Board of Officers recommends you share this important information with your fellow colleagues and professionals.

Fraud Tips

By: Joseph R. Dervaes, CFE, CIA
Association of Certified Fraud Examiners Fellow
Chairman, Board of Regents, Association of Certified Fraud Examiners
Audit Manager for Special Investigations
Washington State Auditor's Office

Segregation of Duties

D.H. was the custodian of two checking accounts at a large school district. She was able to conceal the theft of \$188,300 from a wide variety of miscellaneous revenue streams over a five-year period because she controlled all aspects of the checking accounts. Then she issued checks to herself and paid for her own personal bills directly from the accounts. The bank reconciliation wasn't reviewed by an independent party.

Why did D.H. embezzle \$188,300 over a five-year period? There is no easy answer to this question, because fraud isn't caused by just one factor. Witness the time-honored Fraud Triangle originated by renowned fraud researcher, Dr. Donald R. Cressey. One leg of the triangle represents a perceived non-sharable financial need. The second leg is perceived opportunity. And, the third leg is rationalization (Wells, Joseph T. *Occupational Fraud and Abuse*. Austin, Texas: Obsidian Publishing Company Inc., 1997.)

Even though Cressey's theory is 50 years old and may not be applicable in all situations, I've observed in my position that the second leg of the triangle, perceived opportunity, is often caused by a lack of internal controls. And the number one internal control weakness cited in the fraud reports from my office is inadequate segregation of duties. All activities and functions within every organization are at risk from this internal control defect.

As the audit manager for special investigations for the Washington State Auditor's Office, I'm responsible for managing the agency's Fraud Program, one of our agency's highest priority functions. The Constitution of the state of Washington established the State Auditor's Office as the auditor of all public accounts. This means we audit all state agencies (approximately 170) and all local governments (approximately 35 different types and 2400 units of government). Because we are one of only a few states that have this broad audit authority, we detect and report more fraud in government than any other state. Another reason for the top statistics is because we concentrate on the area of greatest risk for fraud in our industry -- the misappropriation of public resources by employees. For example, in the last 14 years, we reported 408 cases of fraud totaling \$8,355,440 in losses.

My personal specialty is employee embezzlement fraud in the workplace because this is what most employees do once they decide to steal money from their employer in government. There is room for all of us to learn from these experiences, because the same frauds that happen to us in government also occur in the private sector. In addition, additional frauds happen in the private sector that do not occur in government. These will not be further considered in this article.

While monitoring fraud cases throughout the state, we've gathered important information about fraud. We've decided that learning from the past is one of the best ways to affect our future. So watching what the fraud perpetrators actually do, and listening to what they say, pays big dividends. For example, we use the information we obtain from the cases to develop internal fraud training courses for auditors and to present external fraud training seminars to the units of government we audit. I'd like to share some of these tips with you. I believe it's important for us to start where the problem often enters the organization -- segregation of duties.

Internal Control Weakness. While we often concentrate on internal controls in major systems and functions, fraud perpetrators do the opposite by concentrating on the obscure processes in which no one expects fraud to occur. These devious employees know exactly what managers do and don't do, and they know exactly what auditors do and don't do. Once they realize where the weaknesses are in the review and audit process, they capitalize on them to commit their crimes. They simply commit the fraud that's allowed by their particular access and in the area they can control. It's these special domains of control that allow them to not only process irregular transactions, but also to conceal them from view, normally for months or even for years.

The problem is that one employee has total control over a transaction from beginning to end.

The solution is to hire two or more employees to appropriately segregate the duties so no one employee has total control. That may sound obvious, but not many of the organizations we audit have the funds or desire to hire extra employees for this purpose. Since most organizations are doing more with less these days, we expect to see even fewer employees these days than in the past. In fact, as organizations down-size or right-size due to economic pressures, the internal control structure, or key portions thereof, often self-destructs in the process. As an aside, the internal control structure also self-destructs on breaks and lunch as relief personnel with incompatible duties take over operations from the primary employees performing these critical tasks. Under these conditions, the need for internal controls actually increases, rather than decreases, as the total number of employees decline over time. And this is the prime time for something to go wrong with segregation of duties for key employees.

So how do we encourage managers to deal with this dilemma even when they might not want to do so? First of all, we must communicate that failing to implement this internal control **will ultimately** lead to one thing: fraud. It's only a matter of time; the issue is simply "when," not "if." I've found that managers will act to correct this weakness when they finally realize their employees are tempted beyond their ability to handle the situation, and their employees' careers, (and possibly their own) are at tremendous risk if fraud occurs.

Also, when it's not possible to hire more employees, **the next best solution** is for managers to find ways to segregate employee duties without spending more money. The most common method to do this is to require that employees with similar tasks regularly switch specific duties to achieve the proper level of internal control.

Take the situation in which two employees manage checking accounts within an organization. In far too many cases, we find that only one person handles all aspects of each checking account. That person prepares, signs and issues the checks, and then receives the monthly statement directly from the bank and reconciles the checking account. Even though I think the monthly bank reconciliation is a very important task, supervisors often allocate only a minimal amount of time and effort for their review of the process, which is a major mistake. This is particularly true when check fraud is approaching a \$16 billion industry in the United States this year. In this case, all managers must do is ensure each custodian independently reconciles the bank account maintained by the other employee. While this significantly improves internal controls, it adds no cost to the organization because no new employees are involved.

Finally, when there are no other options available, **the ultimate solution** is for managers to establish a monitoring program for this key employee which effectively accomplishes the segregation of duties without hiring another person to perform the task. Someone in a supervisory position must review the work of the employee to ensure the task is performed correctly, accurately, and without any loss of resources. Re-performing critical tasks is an important fraud deterrent and detection step. This monitoring only needs to be performed periodically in order to achieve the desired results. However, if the review isn't random – if the supervisor reviews the employee's work every Friday like clockwork – then fraud will always occur on Monday through Thursday.

If I had to emphasize only one word in all fraud training, it would be **monitoring** – the key to reducing fraud losses. I find that while managers almost always establish internal controls over critical processes, they often don't monitor these activities to ensure systems operate as designed. Fraud perpetrators either ignore or compromise the internal control structure in order to achieve their goal. Since they simply don't play by the rules, monitoring has to be part of the daily internal control routine in a healthy organization.

Detection: the Primary Mission. Because an inadequate segregation of duties is at the heart of every fraud that exists today, we must operate with the full knowledge that detecting this menace must be the primary mission or objective of managers and fraud examiners. To discover the duties and responsibilities of key employees, we must ask what they do, sign, approve, certify, authorize, supervise, review, reconcile, etc. The answers to these questions should help us determine when an employee has too many or overlapping responsibilities that hinder segregation of duties.

Here's an alarming fact for all to ponder: **Every** active fraud currently exists because there is an inadequate segregation of duties somewhere within the organization. Think about this as you go to work tomorrow. Is it happening in your organization right now? I hope not.