CFE UPDATE
November-December 2000

Chapter Fraud Seminar Training and Meeting Dates

Future fraud training events for the remainder of the year 2000 and for calendar year 2001 are as follows:

December 12, 2000 - Joint Chapter and WSCPA Fraud Conference, Marriott Hotel, SeaTac.

February 28, 2001 - Chapter Fraud Seminar, Seattle.

April 25, 2001 - Chapter Fraud Seminar, Seattle.

June 27, 2001 - Chapter Fraud Seminar, Seattle.

August 29, 2001 - Chapter Fraud Seminar and Annual Business Meeting, Best Western Southcenter, Tukwila.

November 1-2, 2001 (dates not yet firm) - Joint Chapter and Association of CFE's Fraud Conference, Hilton Hotel, SeaTac.

December 11, 2001 (date not yet firm) – Joint Chapter and WSCPA Fraud Conference, Marriott Hotel, SeaTac.

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

Annual One-Day Fraud Conference With the WSCPA

Our next Chapter training event is the Annual Fraud Conference we jointly sponsor with the Washington Society of CPA's. It will be held at the Marriott Hotel, SeaTac. This fine hotel facility is just up the hill a couple of blocks from the Hilton Hotel where the 2-day Fraud Conference was held jointly with the Association of CFE's.We have both outstanding topics and speakers lined-up to fill your day with fraud facts that will help you do a better job. And, technology is a part of the program. So, plan to attend. The Washington Society of CPA's has prepared a "flyer" on this Conference that contains additional details for your information. You can obtain it directly from them if you so desire. The topics and speakers for this year's conference are as follows:

(1) E-Commerce and Computer Forensics in the State of Washington, presented by Jim Brittain and Peter Donnell from the Washington State Auditor's Office.

(2) Documenting Fraud Risk, presented by Mark Gibson from Arthur Andersen.

(3) Counterfeit Currency and Fraud Schemes Investigated by the Secret Service, presented by Michael Levin from the U.S. Secret Service.

(4) Interviewing Techniques presented by Ray Lauer from the Federal Bureau of Investigation.

This will be another fine training opportunity for your consideration. Your Chapter Board of Officers has worked hard to bring you the latest and greatest information from the finest instructors. Tell them how much you appreciate their efforts when you see them at the conference. Chapter President, Norm Gierlasinski, and Vice-President, Joe Dervaes, are the Co-Chairpersons for the Annual Fraud Conference.

All registrations will be handled directly by the WSCPA, not the Chapter. So, contact the WSCPA at 1-800-644-4800 to register for this conference. The earlier you register the better. This will give the WSCPA some help in planning the conference and making all of the necessary arrangements with the hotel.

Another Training Opportunity

Internet Crimes, Inc. is hosting the Cyber Crime 2001 National Conference and Exhibition, a three-day conference on computer crimes, during the period January 21-23, 2001, at the Foxwoods Resort and Casino in Southeastern Connecticut. The organization is dedicated to providing information and resources necessary to combat the rapidly expanding realm of computer crime. It has assembled an outstanding panel of experts to provide training and discussion on topics including Economic Espionage, Identity and Credit Card Fraud, Hacking, and much more. Over 400 attendees are expected at this educational event. To obtain additional information about this training opportunity, contact their web site at www.internetcrimes.com, or call them at 800-213-4326.

Graduate-Level Fraud Course

The Dean of the Business School at the University of Texas, Austin has contacted the Association about sponsoring a graduate level fraud examination course during Summer 2001. Chairman Joe Wells has sent out the call for the world's best volunteer instructors to teach the course using materials provided by the Association. Chapter Vice-President Joe Dervaes responded affirmatively and has agreed to teach one of the 13 three-hour blocks of material in the course. Final instructor selections have not yet been made.

New CFE Examination Preparatory Course

The 500-question Uniform CFE Examination, the test that all candidates must pass to obtain the Certified Fraud Examiner designation, has proven to be rigorous. Fewer than one in five candidates pass all sections of the Uniform CFE Examination on the first attempt.

To help candidates better prepare for the Uniform CFE Examination, the Association is developing a "new and improved" CFE Examination Preparation Course. The Association is so confident of the new course's ability to prepare you for the Uniform CFE Examination that it guarantees you will pass on your first attempt. If not, the Association will refund your money or let you retake sections of the examination at no charge.

Who should take this course? Candidates for the Uniform CFE Examination. Professionals who wish to seek the CFE designation, including Associate Members of the Association, fraud examiners, attorneys, internal and external auditors, accountants, law enforcement personnel, security and loss prevention specialists, and managers and executives with anti-fraud responsibilities.

How will the CFE Examination Preparation Course benefit you? It guarantees you will pass the Uniform CFE Examination on the first attempt; helps you develop a specific study plan; lets you study at your own pace; allows you the flexibility to work on multiple computers; creates a non-intimidating study environment; provides answers with detailed explanations; guides you to reference material; gives you exposure to study questions similar to those on the actual Uniform CFE Examination; evaluates your strengths and weaknesses; and, assesses your preparedness for the Uniform CFE Examination.

What will your receive? The Uniform CFE Examination Preparation Course on CD-ROM or diskettes; Fraud Examiners Manual, Third Edition on CD-ROM; and, User's manual and technical support telephone numbers.

The new course is now available for use. The current price for the course is $695 and will be honored until the end of this year. Effective January 1, 2001, the price will increase to $795. So, if you're considering purchasing the CFE Examination Preparation Course, now would be a good time to do so.

You must be an Associate Member of the Association to take the Uniform CFE Examination. To find out more about the course, or to order your copy, contact the Association at 800-245-3321 or visit their web site to purchase it online at: (http://marketplace.cfenet.com/ProductDetail2.asp?ProdID=158)

New Discussion Group Now Available

A new online forum is now available to Associate Members of the Association of CFE's who are studying to become Certified Fraud Examiners. If you are a candidate for the CFE designation, you may use this interactive forum as often as you like to post questions, make comments, get advice, or just "lurk and learn" about the CFE Examination Preparation Course and the Uniform CFE Examination. If you are already a CFE, you are encouraged to participate in the discussions and to help mentor other CFE candidates.

To access the new discussion group for CFE candidates, visit the Members Only section of the Association's web site at: http://www.cfenet.com/membersonly.

Happy Holidays

Well, the Thanksgiving Holiday is now behind us. Your Chapter Board of Officers hopes you had a wonderful time either visiting or receiving relatives at this festive time of the year. Enjoy the family. It's what life is all about.

Now, all we have to do is survive the upcoming holidays of Christmas and New Years. Your Chapter Board of Officers wishes each and every one of you a happy holiday, even if these are not the ones you celebrate. Be careful out there, and drive safely. We look forward to seeing you at a future Chapter Fraud Seminar in the new year.

This is the season for too much food. So, take it easy out there. Otherwise, some rough and tough new year resolutions might be in order. Be healthy!

Twenty Ways to Detect Fraud

The following information is reprinted from the September/October 2000 newsletter of the Oregon Chapter of CFE's by permission. The source of the information is quoted in the text of the article. The article follows:

Successful white-collar crooks know how to work within-and around-your company's internal controls. Moreover, they understand the "form and substance" of traditional audit procedures as well as you do. So, how do you catch them? A better question still: How do you prevent them from embezzling, skimming, or benefiting from bribes and corrupt transactions with outsiders?

First, internal auditors need to look beyond procedures to see how fraud succeeds despite a strong internal control environment.

Second, internal auditors should contemplate the many ways the successful crook can camouflage the signs of fraudulent activity.

And finally, internal auditors must maintain their professional skepticism without becoming "gotcha" auditors.

Simple admonitions? Even obvious? As a practical matter, this can be difficult to remember under the pressure of budget limitations, time constraints, and lack of internal audit department resources.

Are embezzlers more lucky than skilled? The fact that many inside jobs take years to uncover may lead some to think crooks are just plain lucky, that their luck will run out, and that the company's checks and balances will eventually expose their misdeeds.

Actually, the accounting and auditing procedures can be the crooks' greatest ally. All too often, the ability of the typical auditing standard of "sampling and testing" records requires more luck to uncover fraudulent schemes than the embezzlers need to get away with the fraud.

Moreover, many internal audits focus on compliance auditing wherein the emphasis is placed on whether the company's internal control procedures are being followed. The problem: The records themselves. The auditor may be relying on the information provided by the employee or manager who is actually lapping accounts receivable.

For instance, a standard "compliance" audit program might call for an internal audit to check a sample of recorded cash receipts and verify discounts taken by customers to ensure that they have received proper approval in conformance with official policy. Or, the assignment might call for a sample of shipping orders to be traced to recorded sales invoices. In both instances, if the procedures assume that the transactions are accurate, they will not detect skimming by a skilled embezzler.

Think like a crook, not an accountant. This is often the advice given by experienced fraud examiners. Don't trust the obvious, and question, question, question. Whether you are conducting a routine audit of revenue cycle activities or physical inventory controls, consider how a disloyal, disgruntled, or dishonest employee might beat the system. For example, ask yourself: "If I were skimming the cash receipts, what records would I need to change? How could I change them?"

The following list comes courtesy of Stephen Getzoff, CFE and founder of Business Fraud Detection Services, investigation specialists. It is based on BFD Services' 20 years of experience in assisting clients with fraud detection, investigation, and prevention. A review of these 20 indicators will help you maintain your professional skepticism and remain alert to the potential for fraudulent activity within your organization.

1. Unusual Behavior: The perpetrator will often display behavior that signals a problem – for instance, never taking vacations or sick days for fear of being caught. He or she may not assign out work even when overloaded. Other symptoms may be changes in behavior such as increased drinking, smoking, defensiveness, and unusual irritability and paranoia.

2. Complaints: Frequent tips or complaints will be received that indicate a fraudulent action is going on. Complaints have been known to be some of the best leads about fraud and should be taken seriously. Even if the motives of the complainant are suspect, the allegations can have merit and thus warrant investigation.

3. Stale items in reconciliation: Deposits or checks not included in the bank reconciliation could indicate theft. Missing deposits could mean the perpetrator has absconded with the funds; missing checks could indicate one was made out to a bogus payee.

4. Excessive voids: Voided sales slips could mean that the sale was rung up, the payment diverted to the perpetrator, and the sales slip voided to cover the theft.

5. Missing documents: Documents that cannot be located are often a red flag for fraud. Although it is expected that some documents will be misplaced, the auditors should look for explanations as to why the documents are missing and see what steps were taken to locate the requested items. All too often, the auditors will select an alternate item or allow the auditee to select an alternate without determining whether a problem exists.

6. Excessive credit memos: Similar to excessive voids, this techniques can be used to cover theft of cash. A credit memo to a phony customer is written-out to make the cash total balance.

7. Common names and addresses for refunds: Sales employees frequently make bogus refunds to customers for merchandise. The address shown for the refund is then made to the employee's address, or to the address of a friend or co-worker.

8. Increasing reconciliation items: Stolen deposits or bogus checks are frequently not removed, or covered, from the reconciliation. Hence, over a period of time, the reconciling items tend to increase.

9. General ledger out-of-balance: When funds, merchandise, or assets are stolen and not covered by a fictitious entry, the general ledger will be out of balance. An inventory of the merchandise or cash is needed to confirm the existence of the missing assets.

10. Adjustments to receivables or payables: In cases where customer payments are misappropriated, adjustments to receivables can be made to cover the shortage. Where payables are adjusted, the perpetrator can use a phony billing scheme to convert cash to his or her own use.

11. Excess purchases: These can be used to cover fraud in two ways. Fictitious payees can be used to convert funds, and excessive purchases to actual payees may indicate a possible payoff of the purchasing agent.

12. Duplicate payments: These are sometimes converted for use by an employee. He or she may notice the duplicate payment and falsify an endorsement on the check.

13. Ghost employees: Such schemes are frequently uncovered when an auditor, fraud examiner, or other individual distributes paychecks to employees. Missing or otherwise unaccounted-for employees could indicate the existence of a ghost employee scheme.

14. Employee expense accounts: Employees frequently conceal fraud in their individual expense account reimbursements. These should be scrutinized for reasonableness and trends, especially in the area of cash transactions.

15. Inventory shortages: Normal shrinkage over a period of time can be computed through historical analysis. Excessive shrinkage could explain a host of fraudulent activity, from embezzlement to theft of inventory.

16. Increased scrap: In the manufacturing process, an increased amount of scrap could indicate a scheme to steal and resell this material. Scrap is a favorite target of embezzlers because it is usually subject to less scrutiny than regular inventory.

17. Large payments to individuals: These may indicate instances of fraudulent disbursement.

18. Employee overtime: Here, employees are paid for overtime hours not worked by altering time sheets before or after management approval.

19. Write-off of accounts receivable: Comparing the write-off of receivables by customers may lead to information indicating that the employee has absconded with customers' payments.

Post office boxes as shipping addresses: This may indicate that an employee is shipping to a bogus purchaser.