

The Fraud Examiner



Pacific Northwest Chapter

Inside this issue:

Chapter Members in the News	1
ACFE Hubbard Award	2
PNW Chapter Training Events	3, 5 - 6
Free ACFE CPE with Webinars	3
CPE Compliance for CFEs	3,11
Additional Training Opportunities	4
Chapter Incentive Award Program	5
2018 Chapter Fraud Conference	6
The Tidbit	7-9
Chapter Dues	9
Fraud Law	10
Chapter Annual Payment Option	10
Student Scholarship Programs	11
Chapter Membership & Board of Officers Benefits	11
Other ACFE and Chapter Training Opportunities	12
Chapter Board of Officers	12

September/October 2017 Issue

Message from the President

Pacific Northwest Chapter/ACFE Annual Fraud Conference

The Chapter will conduct its Annual Fraud Conference in Tacoma on May 7, 2018! There will be 8 hours of CPE, including 2 hours of ACFE Ethics training, available for all those that attend this event. Registration fees will be \$150 for registration and payment received on or before April 16, 2018, \$175 April 17 through April 30, 2018, and \$200 after April 30, 2018. Chapter Members, Associate Members and Affiliates of the Chapter will receive a \$50 discount from these rates, provided that they have paid their 2018 Chapter dues. There will also be a special discounted rate of \$25 for the first ten Student Members that register on or before April 16, 2018, and ten registration fee scholarships awarded for the first ten Student Members that apply and meet eligibility requirements. See also page 6.

2017 Chapter Incentive Award Program

Are you an Associate Member of the Chapter or are you interested in becoming one? If so, and if you are interested in obtaining the CFE Credential by December 31, 2017, then I encourage you to apply for the Chapter Incentive Award Program. Each calendar year the Board of Officers grants one \$500 award to help defray an individual's unreimbursed costs of obtaining the CFE professional credential. See also page 5 and the Chapter website.

Chapter and ACFE Student Scholarship Programs

The Chapter offers one annual \$1,000 scholarship, and the ACFE Foundation also offers a robust scholarship program. Applications for the 2018-2019 academic year are due by late January 2018 for the ACFE Foundation program, and by March 31, 2018, for the Chapter program. See also page 11 and the Chapter website.

Robert A. Goehring/Chapter President/(253) 856-5262/President@fraud-examiners.org.

Chapter Members In The News

The following Chapter Members have been active in our community outreach programs and other Chapter activities as follows:

(1) Chapter Member Dr. Robert Holtfreter, CFE, CPA, Distinguished Professor of Accounting and Research at the Central Washington University's College of Business, was awarded the ACFE 2017

Hubbard Award. See also page 2.

(2) Chapter Member Gordon Craig, CPA, CFE, Audit Manager, U.S. Army Audit Agency, spoke to the undergraduate forensic accounting class at the UW-Tacoma on July 6, 2017, about two fraud investigations he supported as a member of the U.S. Army Audit Agency. There were seven students who

attended the event, all of which asked questions and stayed engaged throughout the presentation.

Other Chapter members are encouraged to notify President Robert Goehring (President@fraud-examiners.org) about their recent or future presentations or publications so that these events can be publicized in the newsletter.

ACFE 2017 Hubbard Award — Robert Holtfreter, CFE, CPA



Pictured above is ACFE President James Ratley, CFE (right) presenting the award to Dr. Robert Holtfreter, CFE, CPA (left).

The ACFE has honored Central Washington University's Dr. Robert Holtfreter, College of Business Distinguished Professor of Accounting and Research, with its 2017 Hubbard Award. Holtfreter, along with his co-author Adrian Harrington, earned the award after being judged to have produced the best feature article in the ACFE's peer-reviewed journal *Fraud Magazine* by members of the ACFE editorial advisory committee.

The three-part series pertained to a new model that identified five internal and four external data breach causal factors. Harrington, of Yakima, is a former student of Holtfreter, having

taken his CWU fraud examination course.

"This competitive award is especially important to me because it comes from an organization that is strongly committed to detecting and preventing fraud," Holtfreter said. "In addition, having a student like Adrian as a co-author is even more satisfying because it gives me great pleasure in seeing a former student continue to excel in this way."

Holtfreter and Harrington received their award during the ACFE's Annual Conference in Nashville, Tennessee June 18 - 23, 2017. Holtfreter was previously named the ACFE's Educator of the Year in 2006 and received their Outstanding Achievement in Accounting Award in 2005.

Since he joined CWU, he has published more than 90 articles, most of which have been published in various peer-reviewed academic and professional journals. He has also been routinely recognized for his efforts to provide continued education pertaining to fraudulent practices, identity theft, and security breaches.

For his voluntary executive leadership efforts with an assortment of academic, civic, and professional organizations, he has received 15 significant leadership service awards. They include the Phi Kappa Phi Ray Sylvester Distinguished Service Award for 2016-2018, for which he was in competition against faculty from more than 300 university chapters nationwide.

Upcoming Training

Type:
Bi-Monthly Chapter Fraud Seminar

Date:
December 6, 2017

Time:
2:30—4:30 p.m.

Topic:
Annual Review of Recent Local and National Securities Fraud Cases

Speaker:
John J. Tollefsen, J.D., LL.M., CFE, CCS

Where:
Downtown Seattle at 1000 Second Avenue in the Training Room on the 28th Floor of the Washington State Housing Finance Commission's offices. The building is located across the street and one block North of the Jackson Federal Building (corner of Second Avenue and Spring Street).

Price:
The seminar fee is \$20 for Members and \$25 for non-members. Student Members may attend this event at no cost.

Registration:
Register and pay the Chapter at the door or online at the Chapter website (www.fraud-examiners.org). Pre-registration is not required for this event.

December 6, 2017 Chapter Fraud Seminar in Seattle - Annual Review of Recent Local and National Securities Fraud Cases

December 6, 2017, is the date of our next Chapter fraud training seminar at our downtown Seattle training facility. There are 2 hours of Continuing Professional Education available to all who attend this event.

The cost of this fraud seminar is \$20 for Members and \$25 for non-members. Student members may attend this event at no cost.

Pre-registration is not required. Attendees can pre-register and pay at the Chapter website (www.fraudexaminers.org/training.shtml) or do so at the door.

The speaker will be John J. Tollefsen, J.D., LL.M., Founder of Tollefsen Law, PLLC, an attorney, Certified Fraud Examiner, and Certified Controls Specialist. He is a semi-retired international business finance lawyer and litigator with multiple post-graduate degrees from both U.S. and European schools.

Over the years, John has developed a passion for helping victims of financial fraud through the civil law. He serves as a member of the Board of Officers as the Training Director/Director-at-Large for the Chapter, and is a regular contributor to the Chapter's Bi-Monthly Newsletter column of

articles on the topic of "Fraud Law".

The topic will be, "Annual Review of Recent Local and National Securities Fraud Cases". This session will examine selective recent discipline cases from the Securities and Exchange Commission and other regulatory agency files with a special emphasis on ethics. In addition, the speaker will present critical information concerning ethics that will be helpful to all who attend this session.

This session qualifies for ACFE approved ethics CPE credits.

Free ACFE Webinars by Logging on to Your ACFE Membership Account

For dues paying Members of the global ACFE organization, the ACFE offers free training. The webinars are typically 60 minutes in length and are equal to 1 credit hour of ACFE approved CPE credits.

Archived webinars are available for a limited time and new content is periodically uploaded. More information can be found by logging in to the ACFE

website as a member, clicking on "My Account" in the upper right corner, and then clicking on the link in the paragraph in the right column which says "Access archived webinars."

Currently available free webinars include:

- Trends and Best Practices in Global Procurement Fraud
- The Value of a Self-

Contained Compliance Program

- Fraud Detection for SWIFT Payments
- Navigating Beneficial Ownership and Financial Transparency
- A Focused Approach: Best Practices for Uncovering Hidden Risk and Minimizing Exposure

CPE Compliance for Certified Fraud Examiners

When you renew your annual dues you must certify your CPE compliance. You are required to earn 20 hours of CPE each year, **10 of which must be fraud related, and 2 of which must be on ethics.**

Report your CPE Compliance to the ACFE in your anniversary month (online or by phone).

If a CFE has earned more than 20 CPE hours of CPE in any year, he/she may

carry forward up to 10 of these extra hours to meet their future CPE requirements.

Now you can find all your CPE

(Continued on page 11)

Joint Chapter/ACFE Fraud Training Class October 16-17, 2017— Hilton Seattle Airport & Conference Center—SeaTac, WA

October 16-17, 2017, are the dates of our joint Chapter and ACFE Annual Fraud Training Class. This event will be held at the Hilton Seattle Airport, 17620 International Blvd., SeaTac, WA. Registration begins at 7:30 a.m. each day.

The class is entitled, “Using Data Analytics to Detect Fraud”. The ACFE course leader is Allen E. Brown, CFE, CPA, Former Assistant Legislative Auditor for the Louisiana Legislative Auditor’s Office.

Allen Brown spent 21 years with the Legislative Auditor’s Office and participated in more than 250 investigative audits. The results of those audits included felony convictions of four sheriffs, three of whom went to prison. As a result of an investigative audit of the Department of Elections, the statewide elected Commissioner of Elections was also convicted of felony charges and was sentenced to prison, and more than 25 others were indicted and convicted, including vendors from New Jersey, Florida, and Alabama. Subsequent to this project, the department was eliminated by the state legislature.

There are 16 hours of Continuing Professional Education available to all who attend this class.

According to the ACFE’s 2016 Report to the Nations on Occupational Fraud and Abuse, proactive data monitoring and analysis is among the most effective anti-fraud controls. Organizations which undertake proactive data analysis techniques experience frauds that are 54% less costly and 50% shorter than organizations that do not monitor and analyze data for signs of fraud.

“Using Data Analytics to Detect Fraud” will introduce you to the basic techniques of uncovering fraud through data analysis. Taking a software-independent approach, this 2-day course provides numerous data analytics tests that can be used to detect various fraud schemes. You will also discover how to examine and interpret the results of those tests to identify the red flags of fraud.

You will learn how to:

- Recognize the types of data and available tools that can be used to look for signs of fraud.
- Implement the full data analytics process from determining which data to acquire to evaluating the results.
- Apply numerous fundamental, advanced and non-traditional data

analysis techniques.

- Analyze non-numeric data, such as text and non-traditional timelines, for signs of fraud.
- Identify anomalies and recognize common red flags of fraud that appear in the data.
- Use data analytics tests to detect various asset misappropriation, corruption and financial statement fraud schemes.

Registration for this fraud class is directly with the ACFE. To register, contact the ACFE at (800) 245-3321, or at www.ACFE.com.

The cost of this class is \$695 for ACFE Members and \$845 for non-members. There is a \$95 discount for early registration (deadline—September 15, 2017).

Contact the ACFE for registration procedures. Pre-registration for this class is required.

Parking is available at the hotel at a discounted rate of \$12 for each day of this class.

Additional Training Opportunities—John Reid & Associates

John E. Reid and Associates, Incorporated, Chicago, Illinois, announces the following training classes on “The Reid Technique of Interviewing and Interrogation” for the state of Washington in 2017:

- November 14 - 17, 2017, Seattle, WA (Crown Plaza Hotel - Seattle, 1113 6th Avenue) \$795

These are the standard per-person rates and do not reflect the RPGA discounts or discounts available for more than one participant for the same registration.

Prior to registering, be sure to contact Chapter President Robert Goehring (president@fraud-examiners.org) to obtain the Chapter’s RPGA Discount Code. This discount is only available for Chapter members and may not be transferred to non-Chapter members.

Call 1-800-255-5747, Ext. 14 or 24, to register for any of these classes, or visit Reid’s website at www.reid.com.

Learn how to assess the credibility of statements; how to structure the flow of the interview to maximize the flow of information; how to use behavior

provoking questions in the interview process; how to persuade a suspect to tell the truth about their involvement in criminal activity; and, how to develop interrogation themes, handle denials, overcome objections, and use alternative questions.

In the Advanced Program, learn how to psychologically profile suspects for interrogation, develop specialized tactics for juvenile interrogations, and more.

The training manual includes specialized information on interview and interrogation techniques for domestic terrorist activities.

Highlights of the August 9, 2017, Chapter Fraud Seminar in Seattle - Fraud and Technology: The Good, the Bad and the Ugly

August 9, 2017, was the date of the most recent Chapter fraud training seminar, which was held at our downtown Seattle training facility. There were 2 hours of Continuing Professional Education available to all who attended this event.

There were 11 Chapter Members, two Chapter Student Members, and four non-members that attended this event.

The cost of this fraud seminar was \$20 for Members and \$25 for non-members. Student members attended this event at no cost.

Pre-registration was not required. Attendees could pre-register and pay at the Chapter website or did so at the door.

The speaker was Gina St. George, CPA, CFE. Gina is the controller at Ilani, a new casino resort in Ridgefield, Washington, developed by the Cowlitz Indian Tribe in collaboration with Salishan-Mohegan LLC. She oversees financial accounting and revenue auditing which includes compliance with

gaming regulations.

Prior to joining Ilani, Gina served as a senior manager with Moss Adams LLP in its Tribal and Gaming Services Group. She amassed more than a decade of experience in public accounting serving tribal gaming properties across the U.S., by conducting financial statement and gaming compliance audits. Her expertise in fraud prevention and anti-money laundering compliance extends to performing internal and external investigations and assessments, developing policies and procedures, and presenting at industry group conferences and other trainings.

Gina is a member of the Association of Certified Fraud Examiners, the American Institute of Certified Public Accountants, the Institute of Internal Auditors - Gaming Audit Group, and Hospitality Financial and Technical Professionals. She earned a Bachelor of Science in Accounting from Central Washington University.

The topic was, "Fraud and Technology:

The Good, the Bad and the Ugly".

Technology has changed the way we live and work in so many ways.

Technology has also changed the fraud environment and transformed the skill sets needed to be an effective "fraud fighter". The speaker shared her experiences with the good, the bad and the ugly of technology as it relates to fraud taken from her own cases of internal fraud as well as the external threats that companies face in their fight against fraud. In this session, participants:

- Gained an awareness of the negative and positive consequences of technological advances as it relates to internal and external fraud threats.
- Learned controls to combat fraud, tools to detect fraud, and resources to gather evidence.
- Discussed the approach to conducting and investigation when technology is a key component.

2017 Chapter Incentive Award Program

Each calendar year the Board of Officers recognizes one Associate Member who becomes a Certified Fraud Examiner during that year and meets other requirements, by granting him/her an award of \$500 to help defray the costs of obtaining the CFE professional credential.

See the Chapter website (http://www.fraud-examiners.org/PNW_Chapter_Incentive_Award.shtml) for specific information concerning eligibility and the selection process.

Key items (Not All-Inclusive):

- Deadline for fulfilling all of the requirements—**Dec 31, 2017**
- Applicant must be an Associate Member of the Chapter and provide written notice of intent to the Board to apply for this award
- Applicant must pass the CFE Examination and obtain the CFE Credential in 2017
- Applicant must attend at least two

of the Chapter's Fraud Training events

- Applicant must incur eligible expenses that are not reimbursed by his/her employer or other party

The winner will be determined through a drawing, if more than one person meets the eligibility requirements. The winner will be announced at the February 2018 Chapter Fraud Seminar.

There were no applicants for the 2016 Award.

May 7, 2018—Pacific Northwest Chapter Annual Fraud Conference— La Quinta Inn & Suites—Tacoma, WA

Monday, May 7, 2018, is the date of our Chapter's 4th Annual Fraud Conference. Registration begins at 7:30 a.m. and a continental breakfast will be provided. The conference begins at 8:00 a.m. and ends at 4:20 p.m. Lunch will be provided from 11:45 a.m. to 12:30 p.m.

The conference will again be held at the La Quinta Inn & Suites (1425 East 27th Street), Tacoma, WA. There is no charge for parking at the hotel.

There are 8 hours of Continuing Professional Education available to all who attend this event. **This will include 2 hours of training that meets the ACFE annual ethics requirement for Certified Fraud Examiners.**

The Conference Coordinator is Chapter Board Member-at-Large Pete Miller, CFE, CPA. Pete Miller and Chapter President Robert Goehring, CFE, CPA will serve as Conference Co-Chairs.

Registration Information:

Participants can register online through the Chapter website (www.fraud-examiners.org) effective December 1, 2017.

Registration fee:

- On or before April 16, 2018 - \$150
- April 17 through April 30, 2018 - \$175
- After April 30, 2018 - \$200

Pacific Northwest Chapter Members, Associate Members, Retired Members, and Affiliates of the Chapter will receive a \$50 discount from these rates. Calendar year 2018 Chapter dues must be paid prior to receiving this discount.

Pre-registration for this fraud conference is recommended. A limited number of same day registrations will be available provided that payment is made on the day of the conference.

Participants that cancel in writing on or before April 16, 2018, will be given a full refund. Participants that cancel in writing after April 16, 2018, will be given the option of transferring their registration to another person, or applying their registration fee to the 2019 Annual Fraud Conference. No refunds or credit will be given for "no shows".

Chapter Student Member Registration:

There are a maximum of 20 Chapter Student Member registrations available on a first-come first-serve basis. The cost of ten of these registrations is \$25, and there are 100% registration fee scholarships available for the other ten Student Member registrations.

Participants must be Student Members of the Chapter prior to registration for this conference (see Chapter website for eligibility requirements).

Student Member Scholarships:

Student Members applying for the Registration scholarship must apply by e-mail to Chapter Director-at-Large Nancy Pasternack, CFE, CPA, CIA (Boardmal3@fraud-examiners.org), and meet the following eligibility requirements:

- Must be a full-time student in a graduate or undergraduate program at a State of Washington higher education institution
- Minimum 3.0 GPA on a 4.0 scale (or equivalent)
- Enrolled in a degree program related to fraud examination such as accounting, law, or criminal justice
- Must submit an essay of not more

than 500 words including the above information and addressing the following question: "Why is education in the disciplines of fraud examination important to you and to the community?"

Speakers and Topics:

The speakers and topics for this conference will be announced on the Chapter website and through the Chapter newsletter as this information becomes available.

Drawing for ACFE CFE Exam Prep

Course CD:

Attention Chapter Associate Members or those thinking about becoming Associate Members! There will be a drawing for a FREE ACFE CFE Exam Course CD. Those participating must be Associate Members of the Pacific Northwest Chapter/ACFE prior to the date of the conference. Further, the Prep Course CD is not transferrable to another party.

See the Chapter website for Associate Membership eligibility requirements, including being members in good standing with the ACFE.

This is a great opportunity to obtain the CFE Credential at significant savings and join your fellow CFE's in the world of fraud prevention, detection, investigation and/or prosecution.

Post-Event Networking Opportunity:

Immediately after the conference, there will be an informal no-host cash bar opportunity at the hotel for attendees to network with each other. This is a great opportunity to meet members of the Board of Directors to ask questions about the Chapter, including membership and training opportunities, as well as networking with colleagues in our common fight against fraud.

"Be honorable yourself if you wish to associate with honorable people" - Welsh Proverb

The Tidbit: Scam Alerts— (1) The New Predators; and (2) Who’s That Knocking?

Scam No. 1. This information was paraphrased from the January-February 2016 issue of AARP Bulletin/Real Possibilities by Joe Kita.

The New Predators. Senior citizens are criminally defrauded by \$12.76 billion annually, including identity theft and all those other scams you hear about but think will never work on you. Do you consider yourself friendly? Thrifty? Financially sophisticated? If so, you are more likely to be defrauded because you may give complete strangers the benefit of the doubt, be enticed by bargains, and are comfortable by even moving large amounts of money around. The next scam victim could be you.

Here’s what you need to know to watch out for and to protect yourself.

- **Technical support.** Microsoft reported that 3.3 million people, many of them senior citizens, were victimized by a technical support con in 2015 with losses of \$1.5 billion. That’s one individual duped out of an average of \$454 almost every ten seconds, perhaps the biggest consumer scam in the U.S. right now.

Here’s how this scam typically works. You receive an unsolicited telephone call from someone claiming to be with Microsoft or Windows technical support who says that viruses have been detected on your computer. In order to protect yourself, this individual prompts you to call a certain web-site and follow its instructions. A “dummy” screen may even appear that

shows viruses being detected and eliminated. However, the program is really installing malware on your computer which allows the scammer to steal your usernames and passwords, hold your data for ransom, or even use the web-cam to spy on you.

Your Response. Hang up the telephone! Neither Microsoft or their partners make unsolicited telephone calls. And, don’t click on any links in unsolicited e-mails from “Microsoft” or in pop-up advertising promising to speed up your computer. Best Buy’s Geek Squad says that if you haven’t downloaded Windows 10 or the latest version of OS X, do it now. Each update is free, and has lots of new security built in. The same applies to other software programs you use.

- **Silent Call.** When you answer your telephone and no one is there, you’ve received a robo-call. This is an automated computer system which makes telephone calls strictly for the purpose of building a list of people to target for theft. This is the first step to opening you up to many telephone scams.

Your Response. If you haven’t already done so, ask your telephone company to put “caller ID” on your landline. Then simply screen your calls, and ignore any telephone number which you don’t recognize.

- **Internal Revenue Service (IRS) Impostor.** This is one of the most common scams right now. In fact, it’s even getting more sophisticated over time. Here’s how it works.

Someone claiming to be from the IRS either calls you on the telephone or leaves a voice message on your recorder indicating that you owe back taxes. They even threaten to arrest you or take other legal action against you unless funds are wired to them immediately. A variation of this scam is that the caller tells you that you have a refund waiting and that all they need to do is verify your personal information before they send you the money. They’re very convincing and often use aggressive language. In addition, scammers are getting more devious. Sometimes “IRS” appears on your caller ID (spoofing), and con artists may know the last four numbers of your Social Security number.

Your Response. Do not return a telephone call from anyone claiming to be with the IRS. The real IRS begins any communication with a taxpayer only by using the U.S. Postal Service. If you’re ever in doubt about a caller, contact the agency directly by calling (800) 820-1040.

- **Cancer Rip-Off.** In Spring 2015, the Federal Trade Commission charged four national cancer charities (the Cancer Fund of America, Cancer Support Services, the Children’s Cancer Fund of America, and the Breast Cancer Society) with defrauding citizens out of \$187 million. In August 2015, a reigning beauty queen (Miss Pennsylvania U.S. International) was arrested for allegedly claiming she had cancer, thereby swindling funds from unsuspecting sympathetic

(Continued on page 8)

Scam Alert

Summaries:

(1) “Today’s scam artists are everywhere -- on the telephone, at your door, and on-line. Be careful.”

(2) “Deception acts like a door to door salesman during the Autumn months of the year. Don’t fall for it!”

The Tidbit—Continued

(Continued from page 7)
supporters. She even shaved her head and ran fundraisers.

Your Response. Before you contribute to any charity, check out its rating on “charitynavigator.org”. Instead of donating cash to door-to-door solicitors or giving your credit card number to those who call you on the telephone, ask for more information about the charity (i.e.; brochures, web-sites, etc.) so that you can investigate the cause more thoroughly. Also be wary of popular on-line giving sites such as “gofundme.com”. According to experts, the best thing you can do to protect yourself against scams is to be skeptical. Ask questions, and trust your gut.

- **Chip Card.** Banks and credit card companies are updating their systems by issuing customers new “chip” cards. Your data is protected in an integrated circuit, rather than in a magnetic strip as before, and there’s a dynamic code that resets after each use. These new cards are almost impossible to counterfeit. But, here’s the scam. Con artists are impersonating card issuers and sending e-mails requesting personal and financial information, or asking that you click on a malware-laced link before being issued a new card. Fraudsters are sending e-mails purporting to be from companies such as American Express that use the company’s logo and color scheme. They even have footer links such as “View Our Privacy Policy” and “Contact Us”.

Your Response. No credit card company will send you an e-mail or call you on the telephone to verify your personal information that it already has on file before mailing you a new card. You might receive a letter, however, indicating that your new card will soon be arriving in the mail. If you’re ever in doubt about what is happening, call the telephone number on the back of your credit card (not the one supplied in the e-mail), and ask the company if it’s trying to contact you.

- **Faith-Based Dating.** Traditionally on-

line dating deceptions have involved con artists stealing the hearts of unsuspecting singles (many of them senior citizens) and then using various ploys to steal money. Scammers are now targeting faith-based sites like BigChurch, ChristianMingle, JDate, and others. Many people are more likely to fall for scams on these sites because they can’t believe that somebody of their own faith is a con artist.

Your Response. Before you become involved with anyone on-line, use Google or Spokeo.com to research the person, and even view his or her address on Google Maps. Finding “no results” is a red flag. Do a Google Image search for a profile picture. Keep in mind that people who are legitimately looking for love won’t ask for money (unless they’re your kids).

- **Medical Identity Theft.** When most people hear about identity theft, they usually think about someone stealing their credit card information and then going on a buying spree. Remember that you can’t be held liable for fraudulent purchases such as a big screen television. However, medical identity theft is different. You can be required to cover the cost for health care services you never received. These can include tests, prescription drugs, and even operations.

Your Response. Never give your Social Security, Medicare, or health insurance number to anyone you don’t know and trust. Be particularly wary about free health checks offered at shopping malls, fitness clubs, and retirement homes (so called rolling labs). If anyone asks to photocopy your cards or even sign a blank insurance claim form, don’t do it! After all, if the service is supposed to be free, why would they even need this information? In addition, you should review all statements you receive from your insurance provider. If you spot any charges that you don’t understand, call them immediately. And, if you shop on-line for prescription drugs or other health-related items, remember that if the price of anything seems too good to

be true, it probably is!

- **Counterfeit Apps.** In September 2015, Apple disclosed that it’s normally secure app store had been compromised. Some developers had evidently used a fake version of Xcode (now dubbed Xcode Ghost) to build their apps, not knowing it contained malware designed to steal passwords and do other devious things.

Your Response. Apple said that it has purged its store of these malicious apps, but that doesn’t mean that it won’t happen again in the future. Some experts recommend you read an app’s reviews before downloading. Choose a proven and popular app. In addition, remember that you can limit an app’s access to your location by adjusting your device’s privacy settings. This will reduce the chance of being spied upon.

- **Grieving Widow.** The goal of every scammer is to put you under “emotional ether”. This is when you’re not thinking cognitively, but emotionally. People are always more vulnerable after the loss of a loved one, and con artists know that. Scammers scan obituaries for their prey, and then pretend to be a bank official to trick people out of their money.

Your Response. Ask a trusted family member to temporarily manage your financial responsibilities while you’re grieving. That person should follow-up on any suspicious telephone calls or e-mails. And, remember that while you’re grieving, you may be more vulnerable to fraud tactics that play on your emotions.

- **Gift Voucher.** This rip-off involves you getting an unsolicited e-mail from McDonald’s, Subway, or other popular restaurant or retailer offering a free gift card. All you have to do is click on a link to activate it. This may seem like the thing to do, but it’s a phishing scam, meaning that the perpetrator is either trying to install malware on your computer or get your personal information by having you complete an on-line questionnaire.

Continued on page 9)

The Tidbit—Continued

(Continued from page 8)

Your Response. Never click on a link in an unsolicited e-mail or give your personal information either for that matter, no matter how enticing the offer may appear to be. Do a Google search and see if any warnings appear. In most cases, they will.

How Scammers Find You.

Have you ever wondered how scammers obtain your telephone number, mailing address, or e-mail address? Experts say that sometimes it's random, and sometimes there's a science to the targeting. It's just like playing roulette. Sometimes your unlucky number just comes up, and you get the messages. But, experts also cite three additional reasons.

- **Data Purchases.** Scammers buy telephone numbers from companies that sell data. They use the same methods legitimate marketing companies do, but for nefarious purposes.
- **Sucker Lists.** Con artists network too. So, if you've been a victim of a fraud or scam in the past, you're put on a "sucker list". These lists are bought, sold, traded, and stolen among scammers because names on these lists are perceived as potential gold mines. Scammers usually target the victims with a "recovery" or "reload" scam. They pretend to be from a consumer group or law enforcement agency to trick you into thinking they'll help you get your money back – for a fee.
- **Volunteered Information.** This is personal information that you willingly gave out by entering giveaways and sweepstakes, or when completing surveys. Scammers use all of this information to create profiles of those they wish to target in the future. They often target senior citizens who they perceive as holding the majority of the wealth in this country.

Scam No. 2. Paraphrased from the September 2016 issue of AARP.Com Bulletin by Sid Kirchheimer.

Who's That Knocking?

The end of Summer brings the nice, cool, and crisp weather of Fall. It also brings con artists right to your front door!

Elections will soon be upon us. So, you can expect campaign workers to arrive at your door step, as well as pollsters and all kinds of people offering to update your voter registration information. Legitimate folks canvassing your neighborhood will leave their literature behind, or give you donation and registration forms that you can later mail. Real pollsters won't delve deeper than your opinions of candidates and issues important to the times. But, never provide your Social Security number, income level, birth date, or hometown to people performing this type of work. It's all useful information for identity thieves.

Also, don't allow entry to your home by unexpected utility employees who say they need to inspect your furnace or water heater. Utility companies don't dispatch workers to go inside your home without first notifying you about

the event. You can automatically assume that unsolicited offers for a free energy audit will only lead to a hard sell for possibly unnecessary, but expensive, improvements in your home. Stick with the legitimate programs offered through your utility provider, and then only by appointment. Never pay a utility worker for a house call. Remember that your utility company will bill you for any legitimate services they perform for you.

With school back in session, local children may go door to door to raise money for team uniforms or school-sponsored charities. Support those organizations you recognize. Strangers could be scammers or employees of crooked vendors seeking your cash, checks, or credit card numbers. Also beware of charities that you've never heard about. These organizations may be claiming to raise money for victims of a recent disaster, wounded veterans, police and fire department activities, or even sick kids. All of these causes may tug at your heart-strings. But, always be cautious.

Finally, be on the lookout for couriers who arrive at your front door with an unexpected package to be delivered to you. In one of the more recent and popular schemes, these folks show up unannounced (or following a telephone call about a supposed package) and ask for a nominal "verification fee" to be paid to them with a credit card in order for you to receive the package.

Visit www.aarp.org/fraudwatchnetwork to learn more about identity theft and how to avoid scams.

2017 Annual Chapter Dues

Annual Chapter Dues were due in January 2017 for calendar year 2017 membership. The dues/fees are as follows: \$24 for CFE Members; \$30 for Associate Members; \$36 for Affiliates of the Chapter (non-members); and \$-0-

for Retired Members and Student Members. Information about how to pay is available on the Chapter website (www.fraud-examiners.org/membership.shtml).

The Chapter Board of Officers thanks you for your prompt attention to this matter, and appreciates your support of our Chapter's fraud training mission.

Fraud Law—September 2017—By John J. Tollefsen, JD, CFE, LLM, CCS

Alleged Embezzlement by Washington State Bar President

Not helping the public reputation of lawyers, the current president of the Washington State Bar Association, Robin Haynes, resigned recently (June 2017) after a search warrant was filed in Spokane alleged embezzlement during her employment with two law firms. According to the Spokane Spokesman-Review, her attorney wrote, "Ms. Haynes has done nothing wrong and looks forward to clearing her name in a fair tribunal." The WSBA is currently investigating whether she may also have embezzled from it during her tenure.

Sentenced, Bellevue, Washington EB-5 Fraud

On August 4, 2017, Lobsang Dargey, 43, was sentenced to four years in prison, followed by three years of supervised release for EB-5 immigration fraud involving around 280 investors [see article in a previous edition of this column].

Federal Government Not Liable for Misrepresentation

For more than 20 years, Kenneth Wayne McLeod, 48, gave seminars explaining how to get the most out of government retirement benefits, drawing rave reviews from the FBI, Drug Enforcement Administration, Immigration and Customs Enforcement, and U.S. Customs and Border Protection employees he was hired to teach. Thousands of agents heard the pitch, often at the beginning and end of their careers, when their financial decisions mattered the most. The U.S.

government gave tacit approval to McLeod's credentials; he contracted with agencies, including the Homeland Security Dept. and the IRS, and some paid him as much as \$15,000 per seminar. According to his marketing materials, McLeod's benefits company gave 250 presentations to law enforcement agencies since 2006. In recent years, as federal budgets got tight, McLeod gave them for free. [from Bloomberg Businessweek]

Beginning in 1988, McLeod solicited clients, including many DEA employees to invest in a the FEBG Bond Fund, described as a confidential fund backed by long-term government securities that offered guaranteed, tax-free annual returns of 8 to 10 percent. McLeod used investor funds to pay for, among other things, Super Bowl trips for his friends and clients, including seven DEA employees. McLeod also made large donations to the DEA Survivors Benefit Fund contributing at least \$209,994. In June 2010, the SEC began a "cause examination" of one of McLeod's companies. During an interview with SEC investigators, McLeod admitted that the FEBG Bond Fund was a Ponzi scheme. He committed suicide on June 22, 2010. [from DOJ report]

Many federal employees lost their life savings. A legal action (Alvarez et al v. United States of America) was filed in Florida. The Eleventh Circuit upheld its dismissal on July 17, 2017.

In Ponzi fraud cases, there is normally no recovery unless an unrelated "deep pocket" is sued. In this case it was the federal government under negligence

and securities law theories.

Governments are immune from liability unless they agree to be liable. This case was controlled by the Federal Tort Claims Act [28 U.S.C. § 1346(b)(1)] which does not allow "[any claim arising out of . . . , misrepresentation, . . .]" [28 U.S.C. § 2680(h)]

Master Card Escapes U.K. Class Action (July 21, 2017)

Class Actions are new to the U.K. (since 2015). To be effective, the court has to be willing to conclude the class claims are similar enough to one another to be decided in one case. There are always dissimilarities, but U.S. courts have found methods to allow them to go forward. U.K.'s Competition Appeal Tribunal showed it was not going to make Class Actions easy in a £14 billion (\$17.2 billion) consumer antitrust suit against MasterCard over swipe fees, ruling that the fees were too dissimilar among customers to allow the case to proceed.

John J. Tollefsen, J.D., LL.M., is a semi-retired attorney licensed in 6 jurisdictions, Certified Fraud Examiner, and Certified Controls Specialist. His email is John@TollefsenLaw.com. See TollefsenLaw.com for more information regarding fraud law.

Dr. Tollefsen is also the Director-at-Large/ Training Director on the Chapter's Board of Officers, member of the Chapter's Website and Newsletter Committee, and the contributor for all of the information presented in this column.

New for 2018—Annual Dues and Training Payment Option

The Board of Officers is pleased to announce establishment of a new option for Members to pay Chapter dues and Fraud Seminar registration fees!

Effective January 1, 2018, Chapter Members may pay a flat \$94 fee on an

annual calendar year basis that would cover the Member's annual dues and registration fees for all Chapter Fraud Seminars for the entire year.

This fee does not cover registration fees for the Chapter's Annual Fraud

Conference. Further, this fee is non-refundable and cannot be pro-rated for Chapter Fraud Seminars that the member did not attend, nor is this payment transferrable to another person.

2018-2019 Chapter and ACFE Student Scholarship Programs

There are two annual scholarship programs available to full-time university students seeking a major or minor in accounting, business administration, finance, or criminal justice programs in the Pacific Northwest. They are the ACFE Foundation's Ritchie-Jennings Memorial Scholarship Program and the Pacific Northwest Chapter/ACFE Student Scholarship Program.

The Chapter scholarship program is a \$1,000 award to an eligible student attending a qualifying college or university in

the state of Washington. Winners of an ACFE Foundation scholarship are not eligible to receive a Chapter award for the same academic year.

Students interested in applying for the 2018-2019 Scholarship programs are encouraged to visit the Chapter website (www.fraud-examiners.org) or contact any Chapter Board Member to learn more about these programs. The application deadline is **March 31, 2018**.

Applicants must **first** apply directly for the Ritchie-Jennings

Memorial Scholarship Program (expected due date is late January 2018), **then** provide the ACFE Foundation complete application package, including the ACFE's questions and students answers about their interest in the area of fraud, and a resume to Chapter President Robert Goehring via e-mail at President@fraud-examiners.org or by USPS to P.O. Box 215, Auburn, WA 98071-0215.

Unfortunately, there were no eligible applicants for the 2017-2018 Chapter Scholarship Award.

New Chapter Members

Please welcome the new members who joined the Chapter during the period Mid-June 2017 through Mid-August 2017:

CFEs:

- Damon Anderson
- Brian Magbaleta
- Hhu Minh Nguyen
- Anthony Sorbera

Associate Members:

None

Student Members:

- Daniel McManus

Chapter Affiliates:

None

Chapter Membership & Board of Officers Benefits

The Board of Officers recognizes that the Chapter membership is fully aware of the non-financial benefits of being a Chapter Member and serving the Chapter in various capacities including serving on the Board of Officers, serving on the various Chapter committees, and speaking at Chapter training events and other venues. However, did you know that there are very real financial benefits?

Chapter Membership:
Types of Chapter membership and annual dues/fees:

- Chapter Member (\$24)
- Chapter Associate Member (\$30)
- Affiliate of the Chapter

- (\$36)
- Student Member (\$0-)
- Retired Chapter Member (\$0-)

See the Chapter website for eligibility requirements and application process.

Membership Benefits:

- \$5 discount on Chapter Fraud Seminars
- \$50 discount on Chapter Annual Fraud Conference
- Free lunch at the June Chapter Training/Business Luncheon Meeting
- Free lunch (1 day only) at ACFE October training, when held

- As an Associate Member, the opportunity to apply for the Chapter CFE Incentive Program Award (up to \$500)

Board of Officer Benefits:

- Free registration for 3 Board Members for the Joint Chapter/ACFE October fraud training class (\$695/each), when held
- Up to \$500 for one member for attendance at the ACFE Annual Conference as our Chapter Representative
- Free registration for all Board Members at the Chapter's Annual Fraud Conference (\$100 each)

-Renew Membership and report CPE at the same time
-20 CPE required, 10 of which must be fraud related, and 2 of which must be ethics
-10 hours can be carried over every 12 months

CPE Compliance for Certified Fraud Examiners– Continued...

(Continued from page 3)
information in one convenient place. Browse the [My CPE](#) for information and updates on:

- How CPE Works
- CPE Changes from Year to Year

-Maintaining CPE Records / CPE Audit

You may access the [My CPE](#) from your [My Account](#) section or at ACFE.com/ [CPE](#).

It is understandable that you may have questions, so feel free to contact the ACFE's CPE Compliance Team or Member Services by calling (800) 245-3321 or +1 (512) 478-9000, or by e-mail at CPE@ACFE.com.

Links to

ACFE Chapters

Pacific NW Chapter
www.fraud-examiners.org

Oregon Chapter
www.oacfe.org

Spokane Chapter
www.spokanefraud.org

Boise Chapter
www.boiseacfe.org

Big Sky Chapter (Montana)
kathy.arata-ward@josepheve.com

Vancouver, B.C.
www.cfevancouver.com

Edmonton Chapter
www.acfe-edmonton.com

Calgary Chapter
www.acfe-calgary.com

International ACFE Headquarters

www.ACFE.com

*Do you have ideas for our
next newsletter?*

*Want to write the review for
the last fraud training you
attended?*

*We would love your
feedback!*

Contact Robert Goehring at
President@fraud-examiners.org



Other ACFE Fraud Training Opportunities

- 2017 ACFE Fraud Conference Asia Pacific, Hong Kong 9/17/2017 - 9/19/2017
- 10th Annual ACFE Africa Conference, Johannesburg, SA 9/17/2017 - 9/20/2017
- Professional Interviewing Skills, Charlotte, NC 9/18/2017 - 9/19/2017
- CFE Exam Review Course, Dubai, UAE 9/24/2017 - 9/27/2017
- CFE Exam Review Course, Washington, D.C. 9/25/2017 - 9/28/2017
- Fraud Prevention, Tampa, FL 10/2/2017
- Understanding the Mindset of a Fraudster, Dallas, TX 10/2/2017
- Contract and Procurement Fraud, Dallas, TX 10/3/2017 - 10/4/2017
- Bribery and Corruption, Tampa, FL 10/3/2017 - 10/4/2017
- CFE Exam Review Course, Canberra, Australia 10/10/2017 - 10/13/2017
- Developing and Integrated Anti-Fraud, Compliance and Ethics Program, Los Angeles, CA 10/12/2017 - 10/13/2017
- Using Data Analytics to Detect Fraud, Seattle, WA 10/16/2017 - 10/17/2017
- CFE Exam Review Course, New York, NY 10/23/2017 - 10/26/2017
- CFE Exam Review Course, Zurich, Switzerland 10/23/2017 - 10/26/2017
- 2017 ACFE Fraud Conference Canada, Toronto 10/29/2017 - 11/1/2017

The ACFE contact point for all course offerings is Caitlin Perdue, Event Marketing Specialist, by phone at 1-800-245-3321, or at the website www.ACFE.com. Contact her for more information and actual registration procedures.

Other ACFE Chapter Annual Fraud Conferences

- Annual Fraud Conference, Spokane, WA Chapter (October 25-26, 2017—Spokane, WA)
- Anti-Fraud Training, Vancouver Chapter/Justice Institute of BC (to be announced)
- Annual Fraud Conference, Pacific Northwest Chapter (May 7, 2018—Tacoma, WA)
- Annual Fraud Conference, Oregon Chapter (to be announced)

The Chapter Board of Officers & Training Director

President
Robert Goehring, CFE, CPA
(253) 856-5262
President@fraud-examiners.org

Vice-President
Julie Armbrust, CFE, CPA
VicePresident@fraud-examiners.org

Secretary-Treasurer
Roger Gulliver, CFE, CPA, CISA, CBA
(253) 735-2392
Treasurer@fraud-examiners.org

Board Member-At-Large
Liz Larson, CFE, ACAMS
BoardMALI@fraud-examiners.org

Board Member-At-Large
Pete Miller, CFE, CPA
BoardMAL2@fraud-examiners.org

Board Member-At-Large
Nancy Pasternack, CFE, CPA/CFF, CIA
BoardMAL3@fraud-examiners.org

Board Member-At-Large / Training
Director
John J. Tollefsen, JD, CFE, CCS
(206) 624 5300 extension 604
TrainingDirector@fraud-examiners.org

President Emeritus
Joe Dervaes, CFE, ACFE Fellow, CIA
(253) 884-9303
PresidentEmeritusI@fraud-examiners.org