LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Board Member Address

Hello Fraud Fighters of Michigan!

Spring Conference is May 10! There is still time to register and the LACFE Board is please to announce our new Group Pricing. Register 4 or more and we will give you a nice discount. Contact the LACFE Board President or Vice President for details.

Now, back to our Conference. Our topic is Using Data Analytics to Detect Fraud presented by Bethmara Kessler. We can all utilize better and more effective ways to detect anomalies during our work. This course will be helpful on demonstrating techniques to assist us in detecting a variety of fraud schemes through data analytics testing. See page 3 of the newsletter for more details on the topic and the speaker.

So, sign up now while there is still time! And bring some friends!

Also, watch for our flyer describing the Fall Conference topic of Fraud Risk Management. Our tentative date is October 25 in Grand Rapids. We will be sending out a summary of this topic in late May.

Hope to see you soon!

LACFE Chapter Board

IN THIS ISSUE

Fraud Talk Podcast

The Domino Effect of Identity Theft

Alana Benson, researcher, writer and fraud consultant, breaks down the ways identity theft leads to other crimes and how fraud examiners can prepare for the future.

This podcast is a product of the ACFE and may be downloaded at

http://www.acfe.com/podcasts/The-Domino-Effect-of-Identity-Theft.mp3

UPCOMING EVENTS

LOCAL:

AGA Webinar: Fraud/Data Analytics
May 16, 2018
Lansing, MI – VanWagoner Building
Learn More at http://www.lansing-aga.org/EventCalendar/EventDetails.aspx?ItemID=94&mid=24&pageid=22

MICPA
May 10, 2018
Frankenmuth or Troy, MI
Learn More at https://store.micpa.org/product/71141?_ga=2.121962379.1056684312.1525030408-192701530.1525030408 OR
https://store.micpa.org/product/76524?_ga=2.93174941.1056684312.1525030408-192701530.1525030408

Michigan Chamber of Commerce Webinar: Keeping Your Data Safe
May 10, 2018
10:00 a.m. to 11:00 a.m.
Learn More at https://www.michamber.com/webinars/privacy-and-cyber-security-webinar-series

Lansing Chapter of the ACFE – Spring Fraud Conference
May 10, 2018
Lansing, MI – Lansing Automakers Federal Credit Union
Topic: Using Data Analytics to Detect Fraud
Speaker: Bethmara Kessler, CFE, CISA

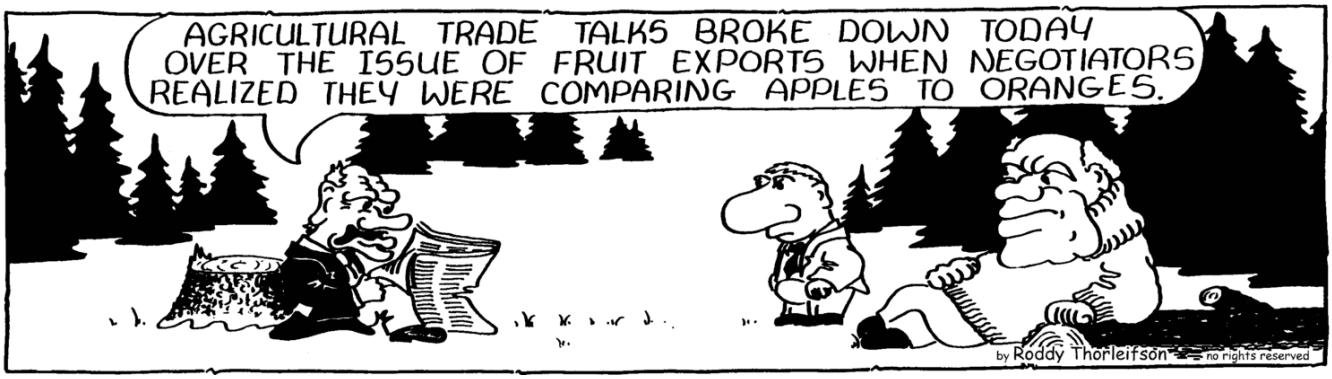
Lansing Chapter of the ACFE – Fall Fraud Conference
October 25, 2018
Grand Rapids, MI
Topic: Fraud Risk Management
Speaker: Bethmara Kessler, CFE, CISA

NATIONAL:

Conducting Internal Investigations
May 3-4, 2018
Austin, TX
Learn More at http://www.acfe.com/events.aspx?id=4294999993

Developing an Integrated Anti-Fraud, Compliance and Ethics Program
May 10-11, 2018
Boston, MA
Learn More at http://www.acfe.com/events.aspx?id=4294999525

If you have an event that you would like posted in our newsletter or if you wish to share an article, please contact Melanie Marks at lacfemrmarks@gmail.com



Register Today

Spring Fraud Conference – May 10, 2018

Using Data Analytics to Detect Fraud

Presented by Bethmara Kessler, CFE, CISA

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 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.

Bethmara is the Senior Vice President of Integrated Global Services at Campbell Soup Company. She has extensive experience in leadership roles in audit, risk management, information systems, and corporate investigations with EMI Group, Plc.; Avon Products, Inc.; RJR Nabisco, Inc.; and Ernst & Young. Bethmara was also the CAE and Co-Chief Compliance Officer at Warner Music Group and was the Senior Vice President of Enterprise Business Risk Management at Limited Brands, Inc. She is a contributing author to the ACFE's *Fraud Examiners Manual* and *Fraud Casebook: Lessons from the Bad Side of Business*. Several specialty publications, such as *Internal Auditor Magazine* and *Journal of Accountancy*, have featured articles written by Bethmara.

IN THE NEWS

Tennessee Physician Agrees to Pay Nearly $200,000 to Government for Kickback Scheme
https://www.justice.gov/usao-ndwv/pr/tennessee-physician-agrees-pay-nearly-200000-government-kickback-scheme

China-backed buyout fund founder guilty of insider trading -U.S. court
https://www.cnbc.com/2018/04/24/reuters-america-china-backed-buyout-fund-founder-guilty-of-insider-trading-u-s-court.html

Athens County Home Health Care Agency Owner Sentenced for Committing $2M Fraud
https://www.justice.gov/usao-sdoh/pr/athens-county-home-health-care-agency-owner-sentenced-committing-2m-fraud

Waldorf Man Sentenced to 4 Years in Prison For Running Oxycodone Pill M
https://www.justice.gov/usao-md/pr/waldorf-man-sentenced-4-years-prison-running-oxycodone-pill-mill

Lance Armstrong Settles Federal Fraud Case For $5 Million
https://www.nytimes.com/2018/04/19/sports/cycling/lance-armstrong-postal-service.html

Former Congressman Stockman Convicted of Fraud In Texas
https://www.reuters.com/article/us-texas-crime-stockman/former-congressman-stockman-convicted-of-fraud-in-texas-idUSKBN1HJ3BX

Craziest Business Expenses of the Year

AccountingToday February 23, 2018

$ Charge for helicopter ride to work to make a client meeting in time - $6,500; not approved

$ Charge for massage in lieu of dinner - $50; not approved

$ Charge for hang glider “to avoid a divorce” - $2,000; approved

$ Charge for boarding a pet snake - $30; approved

$ Charge for vehicle remote start so supervisor didn’t get into cold truck - $450; not approved

$ Charge for hip waders since the “water level was high in service area” - $89; not approved

$ Charge for replacing leather pants ruined on work desk - $885; approved

$ Charge for 40 kilos of cheese for snacks in marketing booth - $134; approved

$ Charge for car wash because someone spit on car in company lot - $30; approved

Score One For The Good Guys!

Court Enters Permanent Injunction and Civil Penalty Against Utah Telemarketers
United States v. Feature Films for Families, Inc., et al.

Docket Number: 2:11-CV-0419 (D. Utah)

On March 23, 2018, the district court entered a stipulated order permanently enjoining three Utah-based telemarketing companies and their owner from engaging in deceptive and abusive telemarketing practices. The order also imposes a civil penalty of approximately $45.4 million, of which all but $487,735 is conditionally suspended based on the defendants' financial condition. This case was initiated in 2011, alleging that the defendants, Feature Films for Families, Inc., Corporations for Character, L.C., Family Films of Utah, Inc., and Forrest S. Baker III, committed widespread violations of the FTC Act and Telemarketing Sales Rule (TSR) in various telemarketing campaigns to sell DVDs and movie tickets, and in charitable solicitation call campaigns.

On May 25, 2016, following eight days of trial, a jury found the defendants committed more than 117 million knowing violations of the TSR, including 99 million calls to phone numbers on the Do Not Call Registry, and more than four million additional calls in which they made misleading statements to induce DVD sales. The verdict was the first ever in an action to enforce the Telemarketing Sales Rule and Do Not Call Registry rule.

New Jersey Man Pleads Guilty to Large-Scale International Mass-Mailing Fraud Scheme
United States v. Ryan Young

Docket Number: 2:18-CR-0046 (E.D.N.Y.)

On Feb. 13, 2018, Ryan Young pleaded guilty to one count of conspiracy to commit mail fraud for his role in a large-scale international mail fraud scheme that brought in $50 million from victims between 2011 and 2016. Young worked with a co-conspirator named Ercan Barka, who pleaded guilty to the same charge in January. Young and Barka sent fraudulent prize notification letters to victims in the United States and numerous other countries.

The letters falsely claimed recipients had won money or valuable prizes, such as luxury cars. Victims were instructed to send small processing fees – typically $20 or $25 – to claim the prizes. Many victims received nothing; others received only a cheap piece of jewelry or a report listing unrelated sweepstakes.

District Court Enjoins Florida Company from Distributing Adulterated and Misbranded Drugs
United States v. MyNicNaxs, LLC et al.

Docket Number: 6:18-CV-0389 (M.D. Fla.)

On March 27, 2018, the district court permanently enjoined dietary supplement distributor MyNicNaxs LLC, and two principals of the company, Chevonne Torres and Michael Banner, from selling and distributing unapproved and misbranded new drugs. In a complaint filed on March 14, the United States alleged that the Florida company sold sexual enhancement and weight loss products in violation of the Federal Food, Drug, and Cosmetic Act.

The complaint alleged that the defendants marketed such products as drugs to treat serious conditions without FDA approval and without proof of safety and efficacy. The complaint further alleged that FDA tests showed that some of the defendants' products contained undisclosed pharmaceutical ingredients such as sildenafil, the active ingredient in Viagra. The consent decree entered by the court requires the defendants to implement specific remedial measures to comply with the law and obtain written approval from the FDA before distributing such drugs in the future.

Court of Appeals Affirms Convictions and Sentences for Peanut Corporation of America Salmonella-Outbreak Defendants
United States v. Stewart Parnell, Michael Parnell, and Mary Wilkerson

Docket Number: 15-14400 (11th Cir.)

On Jan. 23, 2018, the 11th Circuit Court of Appeals affirmed the convictions and sentences of three defendants found guilty of fraud and other charges related to the distribution of contaminated peanuts and peanut products by Peanut Corporation of America. Evidence at trial showed PCA products sickened hundreds and likely thousands of people during an outbreak of salmonellosis in 2008-09. PCA president Stewart Parnell, sales manager Michael Parnell, and quality assurance director Mary Wilkerson all were convicted in September 2014 and sentenced to 336 months, 240 months, and 60 months of imprisonment, respectively.

On appeal, the 11th Circuit ruled that juror exposure to extrinsic evidence of deaths related to the outbreak did not influence or contribute to the verdict. The Court also found no reversible error related to the district court's loss calculations at sentencing and ruled against the defendants on various evidentiary claims and other arguments.

Employee of Chinese Chemical Supplier Pleads Guilty in Scheme to Sell Mislabeled Dietary Supplements
United States v. Gao

Docket Number: 3:17-CR-546 (N.D. Tex.)

On April 3, 2018, Meifang Gao (aka Amy Gao), a Chinese citizen, pleaded guilty to mail fraud and smuggling charges in connection with a scheme to sell mislabeled dietary supplements containing hidden synthetic stimulants. Gao worked for a Chinese firm that sold raw ingredients to American companies for use in dietary supplements. According to an indictment returned in October 2017, Gao and two co-defendants agreed with a confidential government informant to either mislabel synthetic stimulants such as 1,4-DMAA or otherwise help to hide the true nature of a proposed dietary supplement from retailers.

In pleading guilty, Gao admitted that she knew major American dietary supplement retailers would refuse to carry supplements known to contain certain stimulants, such as DMAA. The court set a sentencing hearing for October 1, 2018.

What are the most common occupational fraud schemes in the U.S.?

Corruption – 30%

How is occupational fraud initially detected in the U.S.?

Tip – 37%

*Per ACFE 2018 Report To The Nations - http://www.acfe.com/report-to-the-nations/2018/

Romance Scams: The Price Some Will Pay for Love

By Stephanie Wood, CPA, CFE, CIA
Stephanie is part of the Leadership Team at Stonebridge Business Partners.
stonebridgebp.com

Online dating continues to be a popular method used to meet potential partners. If you type "dating website" in Google, a myriad of links pop up, and Google gives you a listing of the Top 20 dating sites. With all of these options available, it becomes an easy target for scammers looking to take advantage of someone. What better way to get into someone's wallet than through their heart?

The Online Dating World

According to statisticbrain.com, approximately 49.6 million people in the United States have tried online dating websites. As of January 1, 2018, popular dating websites, such as eHarmony.com and Match.com reported 17.5 million and 24.5 million members, respectively. The Better Business Bureau ("BBB") just recently conducted a study to learn more about the inner workings of online romance scams. Their report was published in February 2018, revealing some astonishing figures. According to their report, losses of nearly $1 billion in the United States and Canada were reported over the last three years. The report also noted that the FBI's Internet Fraud Complaint Center estimates that romance fraud causes the greatest dollar loss of any fraud scam affecting individuals, with the exception of investment frauds.

How is it done?

According to the BBB's report, it is estimated that at any one time there may be 25,000 fraudsters online with victims. A company that screens profiles for dating companies says that 500,000 of the 3.5 million profiles it scans every month are bogus.

Scammers looking for their next victim on dating websites create fake profiles to build online relationships, eventually convincing people to send them money. An article that was recently in

the news told the story of a North Carolina woman who met a man on the dating website “Plenty of Fish”. The man stated that he lived in Charlotte but was in Germany on business. After several months of building trust with the victim through text messages, phone calls, and pictures, the scammer eventually asked the woman for money, stating that his accounts were frozen. The woman sent him over $50,000. The man promised to pay her back, even asking her to pick him up from the airport, sending her actual flight information. After a long wait at the airport to pick him up, she realized what had happened. Other examples involve perpetrators impersonating soldiers, asking for money to purchase leave papers from the Army, pay medical expenses from combat wounds, or to get home from war. The scams are usually sophisticated and involve more than one person to corroborate the fake stories being told.

How to Protect Yourself

When it comes to finding love online, you must be aware of some of the dangers you could encounter. Using information published by the Federal Trade Commission, the following list highlights how to recognize a scam artist online:

- If a person wants to leave the dating website immediately and use personal email or instant messenger. Don’t immediately trust that someone online is who they say they are. Use the dating website to communicate with your potential sweetheart until you have met in person and feel comfortable with giving any personal information away.
- If a person claims love in a heartbeat. Despite the fact that many people believe in love at first sight, someone claiming love instantly upon connecting with you online is most likely a scam.
- Someone claims to live in the United States but is traveling or working overseas. Suggest meeting an online suitor in person. If they continue to use the excuse that they are working or traveling overseas, most likely it is a scam.
- If a person plans to visit but is prevented by a traumatic event or business deal gone sour. Be suspicious if they can’t visit due to a traumatic event or bad business deal. Especially if a request for money follows the incident.

- Never wire money to cover the following types of expenses:
    - Travel
    - Medical emergencies
    - Hotel bills
    - Hospital bills for a child or other relative
    - Visas or other official documents
    - Losses from temporary financial setback
- Be aware of someone asking for money after a mugging or robbery. Someone you meet online should not be asking you for money to get back home or get them out of trouble. Most likely this is a scam and will result in more requests and more money.

In addition to the tips above, the BBB's report shared some tools that could help individuals determine whether or not they are dealing with a scammer:

- Scamsurvivors.com has an online quiz that you can take to determine whether you are involved in a scam.
- Tineye.com is a search engine where users upload a photograph and the website finds if the image appears online anywhere else. Most profiles created by scammers will have a profile picture to make it look more legitimate. Users can go to Tineye to search to see if the photo appears anywhere else. Many times, scammers will use a stock photo, or something retrieved elsewhere on the Internet. Google chrome also allows users to right click on a photo and search for it.
- If the person claims to be working for a business overseas, call the U.S. Embassy in the appropriate country and they will verify if this business is real and provide some background on the company.

How to Report

If you or someone you know has been scammed, or suspect that someone is trying to scam you, you can report it to one or all of the following:

- The dating website
- The Federal Trade Commission
- The FBI's Internet Crime Complaint Center
- Your State Attorney General

Most reputable online dating websites have safeguards in place to identify questionable profiles and eliminate attempted fraudulent activity. However, if you come across a suspicious profile, it is important to report it immediately.

Remain Vigilant

Although the online dating world has allowed many individuals the opportunity to find love, there is still risk involved. Many people sign up with the intention of finding love and in doing so become vulnerable to those on the other side of the computer. Be aware of the red flags and know when to say no. Don't just follow your heart on this one.

Taken from: https://stonebridgebp.com/library/uncategorized/romance-scams-the-price-some-will-pay-for-love/

QUOTE OF THE MONTH

"Whoever is detected in a shameful fraud is ever after not believed even if they speak the truth."

Phaedrus