LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Board Member Address

Salutations, Michigan Fraud Fighters!

Our Fall 2017 Fraud Conference in October was a great success! Our speaker, Tom Golden, provided us with in-depth detail of the skills needed to conduct an admission-seeking interview. Tom's vast experience permitted us to not only hear how those interviews are accomplished, but gave us relative case examples that demonstrated the interviewing skills. Tom spoke of a few State of Michigan cases he has worked as well as overseas cases. The cases he worked in Michigan resulted in FBI referrals and several criminal charges being filed. From the comments received, everyone in attendance went away with ideas and new knowledge that could be immediately placed into practice.

I am also happy to announce that our Winter 2018 Fraud Conference is scheduled for February 22 in Grand Rapids! Our speaker will be Daniel Porter. Daniel has over 20 years of experience in investigations both in the private and public sectors. He is an investigator for the Tennessee Comptroller's Office and has experience at Tennessee Department of Transportation as well as being a licensed private investigator. His presentation is *Fraud Investigations from A to Z.* This will be another exciting and informative conference! See page 3 for the presentation description and watch your email for the registration form. We hope to see you there!

Melanie Marks

LACFE Chapter Secretary

IN THIS ISSUE

Board Member Address

Fraud Talk Podcast – The Stories Numbers Tell

Upcoming Events & Conference Description

In The News

The Dangers of Open Wi-Fi

Fraud Talk Podcast

The Stories Numbers Tell: **How One Woman Stole $53 Million Over 20 Years**

Andi McNeal, CFE, CPA, interviews Dr. Kelly Richmond Pope, CPA, filmmaker, & Assoc Prof of Accounting at DePaul University. They discuss Pope's latest documentary. "All the Queen's Horses," a film examining bookkeeper Rita Crundwell and the largest municipal fraud in U.S. history. This podcast is a product of the ACFE and may be downloaded at http://www.acfe.com/podcasts/The-Stories-Numbers-Tell.mp3

UPCOMING EVENTS

LOCAL:

Lansing Chapter of the ACFE – Winter Fraud Conference
February 22, 2018
Grand Rapids, MI – The Bluff Banquet & Conference Center
Speaker – Daniel Porter
Topic – "Fraud Investigations from A to Z"
See page 3 for presentation description

AGA Webinar – Auditing Challenges and Best Practices
December 6, 2017
Lansing, MI – Constitution Hall Arthur Iverson Conference Room
Learn More at http://www.lansing-aga.org/EventCalendar/EventDetails.aspx?ItemID=90&mid=24&pageid=22

Southeast Michigan Chapter of the ACFE
24th Annual Fraud Conference
April 26, 2018
VisTaTech at Schoolcraft College
Learn More at http://semcacfe.org/Annual_Fraud_Conference

NATIONAL:

Auditing for Internal Fraud
December 12-13, 2017
Las Vegas, NV
Learn More at http://www.acfe.com/events.aspx?id=4294997463

Investigating Conflicts of Interest
February 5, 2018
Atlanta, GA
Learn More at http://www.acfe.com/events.aspx?id=4294999879

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

used with permission from mooselakecartoons.com

Winter 2018 Fraud Conference – Feb. 22, 2018
Fraud Investigations from A to Z

Presented by Daniel Porter, CFE

Each fraud investigation is like a box of chocolates, you never know what you're going to get. Despite these differences, a series of logical steps must be followed, and specific techniques must be used to reach an accurate conclusion. From handling the initial tip, planning and executing your investigation, maintaining chain of custody over evidence, analyzing data, interviewing witnesses and subjects, documenting your work, and writing your report to communicating your results to management, law enforcement and prosecutors.

Whether you conduct fraud investigations full time or on an as needed basis, this seminar "Fraud Investigations from A to Z" will provide you with multiple takeaways you can immediately implement in your fraud investigation practice. Daniel will guide you through the entire process and provide relevant case studies of actual fraud investigations to reinforce the training and in some cases provide entertainment.

Daniel has over 20 years of investigative experience in both the private and in the public sector ranging from employees stealing gas for personal vehicles to $20 million frauds of Federal grant funds. His experience in loss prevention, as a licensed private investigator, as an investigator in the Tennessee Comptroller's Office, and as an investigations manager with the Tennessee Department of Transportation provides him insight to the different challenges faced by internal and external auditors, accounting/finance professionals, and fraud examiners.

NOTE:
Research is being conducted for topics and speakers for Spring 2018 and Fall 2018 Fraud Conferences. We could use your help! What topics do you have interest? Is there a specific topic or speaker you would like to hear?

Your input is very important since these events are your CPE opportunities. Please contact Melanie Marks at lacfemrmarks@gmail.com with your ideas and suggestions.

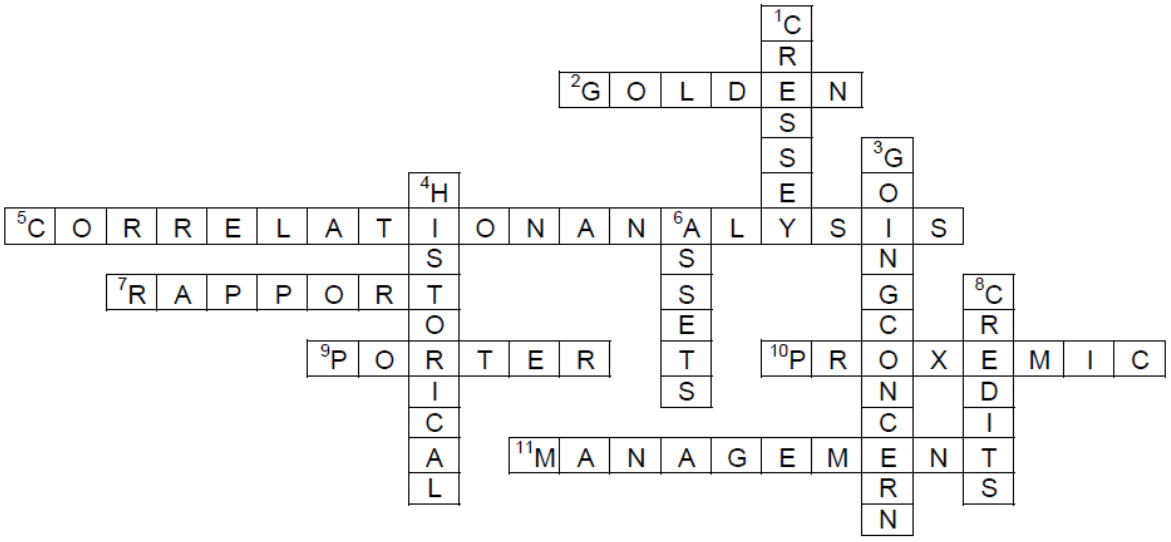
IN THE NEWS

Ski resort owner reaches tentative deal in $200M fraud case
https://www.cnbc.com/2017/11/22/the-associated-press-ski-resort-owner-reaches-tentative-deal-in-200m-fraud-case.html

Former IRS employee sentenced on health care fraud charge
https://www.justice.gov/usao-wdva/pr/former-irs-employee-sentenced-health-care-fraud-charge

Owner of two Miami home health agencies sentenced to more than six years in prison for role in $74 million medicare fraud conspiracy
https://www.justice.gov/usao-sdfl/pr/owner-two-miami-home-health-agencies-sentenced-more-six-years-prison-role-74-million

November Crossword Answers



DOWN

1. Fraud Triangle criminologist creator
3. The assumption an entity will continue long enough to fulfill its financial/legal obligations
4. The type of cost that is the proper basis for recording most assets
6. The first part of the accounting equation
8. Increases liabilities

ACROSS

2. Fall 2017 LACFE Conference Speaker
5. Data analysis function used to determine the relationship between two variables in raw data
7. Relation marked by harmony, conformity, accord, or affinity
9. Winter 2018 LACFE Conference Speaker
10. Type of interview communication that uses interpersonal space to convey meaning
11. Party ultimately responsible for prevention and detection of fraud within an organization

W	M	B	H	E	O	J	G	J	K	Y	U	K	E	Z
Q	N	A	C	W	H	T	Z	N	R	G	I	W	L	H
T	B	J	R	Y	M	D	Q	E	I	C	D	K	Z	B
T	F	A	I	U	C	A	B	N	K	F	C	G	Z	N
J	Q	K	M	X	P	I	Y	B	Z	Y	R	O	E	Y
H	H	V	I	M	R	V	A	K	P	I	L	U	B	N
E	Q	E	N	B	Z	C	X	U	E	C	K	Z	M	N
I	X	F	A	J	K	H	L	U	Z	Q	B	G	E	S
B	F	T	L	H	W	L	S	C	T	I	X	J	W	F
P	N	R	O	F	A	L	S	I	F	I	E	D	M	C
A	O	Z	L	R	X	X	U	B	F	S	K	D	F	G
Q	F	N	V	V	T	F	R	A	U	D	M	B	K	B
H	M	C	Z	Q	A	I	A	L	Z	L	L	D	K	B
E	N	T	O	I	H	Y	O	A	C	A	Y	J	I	P
G	N	I	M	M	I	K	S	N	O	Y	R	U	P	D

BRIBERY **CRIMINAL**

EMBEZZLE **EXTORTION**

FALSIFIED **FRAUD**

KICKBACK **PONZI**

SKIMMING **SMURFING**

The Dangers of Open Wi-Fi

By James I. Marasco, CPA, CIA, CFE
James is a partner at Stonebridge Business Partners.
stonebridgebp.com

When you're away from home or work, it becomes difficult to get through the day without having access to the Internet. Whether you're checking your email, social media, paying bills or trying to stay connected to the office, access to the Internet has become critical. Most people don't realize the dangers that can arise from connecting to an open Wi-Fi source.

Connectivity

Our phones and tablets have become remote work stations and almost critical in our daily activities. As a result, simply using your phone or tablet's mobile connection could become expensive. Therefore, most people try to access a broadband connection where possible to alleviate using all of their cellular data allowance. Hotels, airports, restaurants and retailers all boast "free Wi-Fi" which tempts most individuals to simply connect onto their network. Before you connect again, consider the risks.

What's the Harm?

A June 2016 study by cyber security firm Symantec found that 87% of U.S. consumers have readily used public internet. More than 60% of consumers think their information is safe when using this connection according to the study. They mistakenly believe that the Wi-Fi provider or websites they are visiting will keep them safe. Some networks even offer passwords. Don't be fooled – these passwords are shared with others.

Cyber criminals have become exceptionally stealth at creating "false hot spots." When someone starts roaming for a free Internet connection at their local retailer/airport, etc., thieves have set up their own network routers broadcasting a similar name. As consumers are fooled into connecting to the fake networks, criminals can now track all of their activity. While this could be rather harmless if all someone does is read the news headlines. However, once they start accessing bank account, credit cards, social media accounts, etc., they are exposing this information to data thieves, along with their usernames and passwords.

Assuming the free Wi-Fi spots are legitimate, there are still substantial risks. Keep in mind that all of the information you're transferring between your device (phone, tablet, laptop) and the computer that you are connecting to is available to everybody on the network. This information can be intercepted by data thieves who "sniff" through the data running through network. Items like usernames, passwords and credit card information are exceptionally valuable to them for obvious reasons. What's even more alarming is that "Wi-Fi sniffing" may not be illegal, if the banners you receive upon initial login don't specifically prohibit it. The software needed for this is easy to use and inexpensive to obtain.

If usernames and passwords are stolen, attackers can access your device and install malware without your knowledge. They can obtain your photos, activate your camera or even turn your laptop into a listening device once they have access.

Open or free Wi-Fi can also pose other vulnerabilities. Sometimes hotspot providers offer free Wi-Fi to consumers in exchange for information. By clicking, "I accept" (to pages of small fine print) and providing a phone number or email in exchange for the site password, consumers may be allowing the provider to inject cookies into their browser to track their history and sell this information to advertisers. They could also track your physical location based on the Wi-Fi strength if moving through a mall or airport.

Protect yourself

The most obvious safeguard is not to connect to public Wi-Fi. Some newer cell phone models allow themselves to be used as a secure Wi-Fi hotspot so other devices (tablet, laptop, etc.) can connect through it. Unfortunately, this option will eat into your cellular data allowance. Another option involves purchasing/leasing a battery operated Mi-Fi device which creates a secure mobile Wi-Fi network wherever you travel.

If it's necessary to connect to an open network, make sure to choose the initial setting as "public network." The other choices that will pop up when you initially connect are "home" or "public network." This will trigger a preset list of settings. By choosing the public network option, it offers the most security involving network discovery, file sharing, media streaming, etc. Once online, limit your browsing to public sites. Refrain from logging into any email or social media accounts. Personal

banking or credit card sites should definitely be avoided, along with downloading any software. Keep in mind that there is a good possibility that others can see the information that is transferred or what you are doing.

Another option that is available is to connect through a Virtual Public Network or VPN similar to what most companies use for employees to connect remotely. A VPN creates a network within a network solution. Consumers can use the same technology which thwarts Wi-Fi sniffing and safeguards your data. There are many VPN services or options available that can be used with apps for cell phones and laptops. However, if going this route, don't be fooled by the cheapest provider. Do your research – some of them have been known to sell user information such as sites visited, applications downloaded, etc. Read their privacy policy and check their background and history.

Be aware

Next time you are out and about, don't be tempted by the quick and easy free Wi-Fi. Be aware of the vulnerabilities and take the necessary precautions to protect yourself from data hackers and cyber thieves.

First published in *The Daily Record* February 2017 taken from https://stonebridgebp.com/library/uncategorized/dangers-open-wi-fi/

QUOTE OF THE MONTH

"Rather fail with honor than succeed by fraud."

Sophocles