LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

LACFE Board Position Filled

Rebecca Brinkley has agreed to fill our open board seat. Rebecca is a CFE and is an internal Audit Manager with the Office of Internal Audit Services for the State of Michigan.

Thanks, Rebecca! Let's welcome her to the Lansing ACFE Chapter's Board of Directors!

LACFE Winter Conference

The Winter Conference is on February 15th and registration is open now. Don't delay, seating is limited and the registration deadline is February 9th. There are more details on page 2 and the flyer is on page 3.

Job Opening: Wayne State University Senior Information Technology Auditor

Highlights: 2 for 1 retirement matching, 100% tuition benefit, salary range: $65,000 – $86,000. See Career Site (csod.com)

In This Issue

Fraud Talk Podcast

Fraud in Your Backyard: Fraud in Homeowners and Condo Owners Associations - Belinda Kitos - Fraud Talk - Episode 139

Belinda Kitos, CFE, CICA and president of SCF Inc., was elected as treasurer of her homeowners association, but when she opened the books she discovered a $1.2 million fraud in her own backyard. In this month's episode of Fraud Talk, Kitos and Jason Zirkle, training director of the ACFE, explore their own experiences investigating HOA fraud and the red flags of these schemes.

Fraud in Your Backyard: Fraud in Homeowners and Condo Owners Associations - Belinda Kitos - Fraud Talk - Episode 139 | Fraud Talk (podbean.com)

UPCOMING EVENTS

LOCAL:

ACFE SW Ohio Chapter - Accounting Integrity Builds Trust (Ethics)
Virtual
February 09, 2024
12:00 – 2:00 pm
Learn more: https://swohacfe.org/events

LACFE Winter Fraud Conference - Get Rich Quick: How to Embezzle from the Government *and* Forensic Linguistics: An Introduction
Maner Costerisan, Lansing MI
February 15, 2024
8:15 – 4:30 pm
Registration: https://www.lansingacfe.com/?page_id=90 *See poster below!*

MICPA Forensic Accounting: When The Office Is A Crime Scene
Webinar
March 5, 2024
11:00 – 3:00 pm
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=146099

NATIONAL:

Identity Theft Awareness Week 2024
Identity Theft Awareness Week starts January 29!
Visit ftc.gov/IDTheftWeek for details on free events and resources.

FEDERAL TRADE COMMISSION
IdentityTheft.gov
Identity theft happens in every community
Learn to reduce your risk
ftc.gov/IDTheftWeek
#IDTheftWeek
January 29 – February 2, 2024

ACFE Developing an Integrated Anti-Fraud, Compliance and Ethics Program
Virtual Seminar
March 26 - 28, 2024 (early registration ends February 26th)
Learn more: Event Details (acfe.com)

ACFE 2024 Women's Summit
In-Person (Washington D.C.) or Virtual
March 8, 2024 (early registration ends February 7th)
Learn more: 2024 ACFE Womens Summit (fraudconference.com)

ACFE 35th Annual ACFE Global Fraud Conference
In-Person (Las Vegas, NV) or Virtual
June 23 - 28, 2024 (early registration ends March 19th)
Learn more: 35th Annual ACFE Global Fraud Conference

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article or job opening, please contact Jennifer Ostwald at jenny1661@hotmail.com

The Lansing Chapter of the Association of Certified Fraud Examiners

Winter Fraud Conference

Get Rich Quick: How to Embezzle from the Government

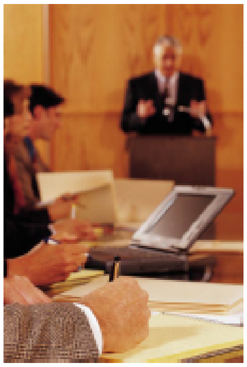
and

Forensic Linguistics: An Introduction

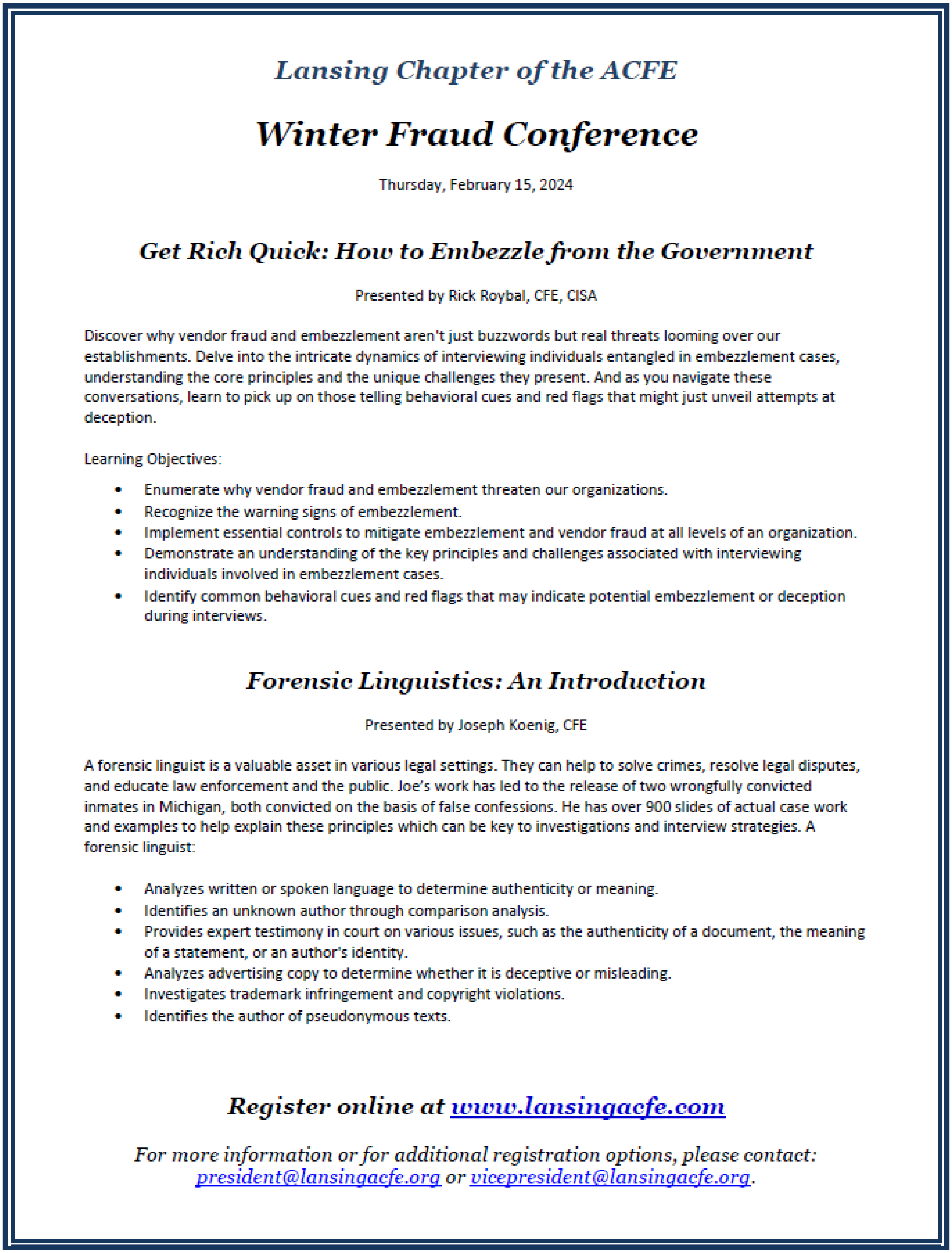
February 15, 2024

- Space Limited! –

Hosted by: Maner Costerisan
2425 E. Grand River Avenue, Lansing, Michigan 48912



CONFERENCE DETAILS	
Sign In:	8:00 am – 8:15 am
Conference:	8:15 am – 4:30 pm
Conference Fee:	$160 members, $195 non-members
Lunch Included:	12:00 pm – 12:30 pm
Registration:	Through Friday, February 9, 2024
CPE Credit:	8 Hours
Dress:	Business Casual



Lansing Chapter of the ACFE

Winter Fraud Conference

Thursday, February 15, 2024

Get Rich Quick: How to Embezzle from the Government

Presented by Rick Roybal, CFE, CISA

Discover why vendor fraud and embezzlement aren't just buzzwords but real threats looming over our establishments. Delve into the intricate dynamics of interviewing individuals entangled in embezzlement cases, understanding the core principles and the unique challenges they present. And as you navigate these conversations, learn to pick up on those telling behavioral cues and red flags that might just unveil attempts at deception.

Learning Objectives:

- Enumerate why vendor fraud and embezzlement threaten our organizations.
- Recognize the warning signs of embezzlement.
- Implement essential controls to mitigate embezzlement and vendor fraud at all levels of an organization.
- Demonstrate an understanding of the key principles and challenges associated with interviewing individuals involved in embezzlement cases.
- Identify common behavioral cues and red flags that may indicate potential embezzlement or deception during interviews.

Forensic Linguistics: An Introduction

Presented by Joseph Koenig, CFE

A forensic linguist is a valuable asset in various legal settings. They can help to solve crimes, resolve legal disputes, and educate law enforcement and the public. Joe's work has led to the release of two wrongfully convicted inmates in Michigan, both convicted on the basis of false confessions. He has over 900 slides of actual case work and examples to help explain these principles which can be key to investigations and interview strategies. A forensic linguist:

- Analyzes written or spoken language to determine authenticity or meaning.
- Identifies an unknown author through comparison analysis.
- Provides expert testimony in court on various issues, such as the authenticity of a document, the meaning of a statement, or an author's identity.
- Analyzes advertising copy to determine whether it is deceptive or misleading.
- Investigates trademark infringement and copyright violations.
- Identifies the author of pseudonymous texts.

Register online at www.lansingacfe.com

For more information or for additional registration options, please contact: president@lansingacfe.org or vicepresident@lansingacfe.org.

Rick Roybal, CFE, CISA

Vendor-Risk Management “activist”, auditor, author, and speaker, Rick Roybal has worked in the oil and gas industry for almost two decades. Today, Rick works for Matador Resources, where he ensures vendor compliance with the company’s accounting and policies and procedures, as well as the accuracy and validity of its billing process. He has earned an MBA in Finance & Accounting, an MA in Linguistics, and a BA in Russian. His published work includes articles in COPAS’s *ACCOUNTS*, ACFE’s *FRAUD*, and IIA’s *Internal Auditor*.

Joseph Koenig, CFE

Joe retired from the Michigan State Police after 26 years and has 45 years of investigative experience in both the public and private sectors. He was lead investigator on the James R. Hoffa case, and has investigated homicides, organized crime, financial crimes, narcotics, and public corruption. He is Past President of the Michigan FBI National Academy Associates. He is a Certified Fraud Examiner (CFE), holds a BS in Accounting from Wayne State University, and a MA in Public Administration from Eastern Michigan University where he was a member of the Phi Kappa Phi Honor Society. He now owns and operates KMI Investigations in Western Michigan specializing in financial fraud investigations.

He authored the award-winning book “Getting the Truth” and is a much sought-after speaker on how to discover the real message, distinguishing truth from deception, and how to “sculpt” questions to get the truth. “Getting the Truth” won the 2016 Montaigne Medal Finalist and 2016 Indie General Non-Fiction Finalist Awards.

Data breaches and ID theft are still hitting records. Here's how to protect yourself

January 25, 2024
Betty Lin-Fisher
https://www.usatoday.com/story/money/2024/01/25/data-breach-id-theft-protection/72352690007/

2023 was a record-breaking year for data compromises – and that's not a good thing.

In its latest yearly report, the San Diego-based Identity Theft Resource Center said there were 3,205 data compromises in 2023, a 78% increase from 2022 and a new record, topping the previous all-time high of 1,860 set in 2021.

In 2023, there were also more than 353 million victims of ID theft, according to the center, a nonprofit organization that assists consumers when they have become victims and advocates for better protections for consumers and businesses. That's a decrease of 16% from 2022, which is consistent with a general trend of the number of victims dropping slightly each year "due to organized identity criminals focusing on specific information and identity-related fraud and scams rather than mass attacks," the organization said.

Notifications of data breaches without information on the rise

The number of data breach notices without specific information such as what happened, what the company has done to correct it, or what steps have been taken to make sure the breach doesn't happen again has nearly doubled year over year, said James. E. Lee, Identity Theft Resource Center's Chief Operating Officer. In 2023, more than 1,400 public breach notices did not contain such information.

"That's a problem and that creates risk for other businesses who could be attacked in a similar fashion and consumers who need to know how to protect themselves," Lee said.

There is no federal law that requires companies that have had a data breach to notify their customers or consumers more broadly, Lee said. There is instead a patchwork of state laws and federal regulations, with different requirements, he said. For instance, there is a federal regulation that any publicly traded company that has a data breach must notify consumers, but only 11% of data breaches last year would have qualified, Lee said.

"Every state has a different definition of what is a breach. Every state has a different trigger for when you have to send a notice. Every state has a different requirement for what information you include and who has to be notified," he said. It took until 2018 to have all 50 states pass a data-breach law and they're all over the board, Lee said.

Many laws don't have penalties for the company that had its information lost or breached and allow that organization to determine its risk and if it needs to notify consumers, Lee said.

Generally speaking, where the company is located is where the state law controls the notification, regardless of where affected consumers live, he said.

"But that's one of those things that we need to update because data breaches, just like data criminals, don't recognize those little imaginary (state) lines," he said.

Supply chain data attacks are on the rise
A growing target of data breach attacks by criminals is within a supply chain of a company and its sometimes smaller suppliers, Lee said.

"The criminals will attack a smaller organization that works for big companies," said Lee. Usually, those companies don't have as tight of security measures, but it still gets the criminals the bigger data they want, he said.

"For an identity criminal, that's Nirvana. I can pick one company and get the company that has hundreds if not thousands of companies (access to information)," Lee said.

Criminals are also ramping up what's called "zero-day attacks," which is an unknown flaw in a company's software to get in, Lee said. Even the guys who wrote the software don't know the flaw is there "and the bad guys find it," said Lee.

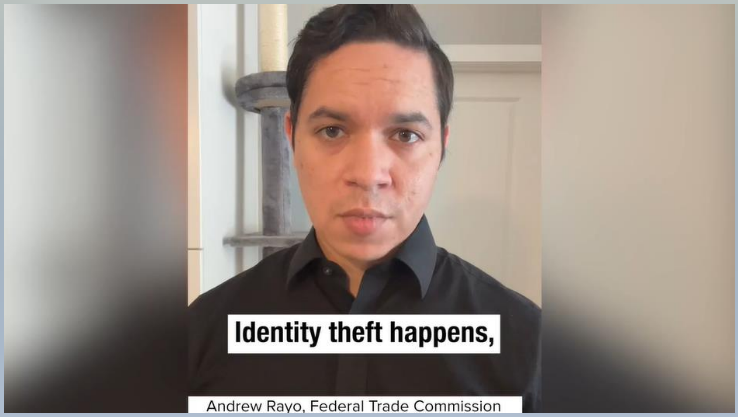
How do you protect yourself from data breaches or ID theft?
While there isn't a lot a consumer can do to prevent a company from becoming a data breach victim and therefore the consumer from becoming a target as well, Lee said there are ways consumers can protect themselves – especially before a data breach.

Here are some tips from the ID Theft Resource Center:

- Freeze your credit with all credit bureaus, as a protective measure. Find out how to freeze your credit and other tips at www.idtheftcenter.org
- Change your password and switch to a 12-plus character passphrase.
- Enable two-factor authentication (with an app, if possible) on your accounts.
- If you are offered a passkey option from a website or your phone, which is beyond a password and can be fingerprint or facial ID options, take them.
- Keep an eye out for phishing attempts that claim to be from the breached organization.
- Follow the advice on the data breach notice offered by the impacted company.
- Change the passwords of other accounts with the same password as the breached account.

Video of the Month

[5 Ways to Protect Yourself from Identity Theft (FTC)]()



Generative AI is increasingly being used to commit identity fraud

January 24, 2024
Vivienne Nunis
https://www.marketplace.org/2024/01/24/generative-ai-identity-fraud/

Matt Vestge runs a graphic design and digital marketing firm; he also posts motivational videos on TikTok. At the end of 2020, Matt received a series of texts from an unknown number.

“They really were out of the blue,” Vestge said. “I didn’t believe much of anything he was saying until I received the pictures of my document.”

Vestge was shocked to find a text message containing photos of his personal ID documents. First, the fraudster demanded money. Then, when Vestge refused, he asked Vestge to join him on another scam.

Vestge turned down the offer and thought nothing more about it until last month, when he received an unwelcome letter from the Oregon Department of Revenue “stating that I had earned just over $6,000 worth of unemployment insurance, which I never did.”

Now, Vestge is struggling to prove it wasn’t him who claimed the benefits for which a tax bill must be paid.

“It can be really traumatic,” said Gavin Burton, who spent more than 25 years in London’s Metropolitan Police. Since then, he’s worked as a consultant and co-founded UFIKA, the U.K. Identity Fraud Advisory which supports victims and helps businesses deal with fraud.

“When I was in a place and we would go to counterfeiting factories,” he said, “these would traditionally be organized crime groups that were working in a kind of a two-bedroom maisonette above a kebab shop and they would be churning out false documents literally 24/7.”

During the COVID pandemic, there was a huge shift in the way companies began verifying our identities. Much of it moved online, and that played into the hands of fraudsters.

“There are websites out there on the internet, where you can just type in your name and what type of document you want, and for a very small amount of money, it can generate basically an AI-generated document with all of that data,” said Burton.

The improvements in generative AI mean it’s easy for criminals to commit fraud at scale. So who’s fighting against this growing army?

Richard Tomsett is with online verification company Onfido and is an expert in biometric fraud. “It’s very sophisticated and the tools are now very easy to come by and increasingly easy to use,” he said.

Fraud expert Gavin Burton said there's an arms race going on between companies like Onfido and the fraudsters they're trying to stop.

There are precautions we can take, however: "Try not to share pictures of you, your car and your registration number, or the house number of your property — yeah, those kinds of practical things," he said.

And if we do find our identity stolen?

"The one thing that you have to do is act quickly and not stick your head in the sand and think it's gonna go away. Don't ignore debt collectors letters and things like that," Burton said. "If you think, 'Well this is not for me. I've not applied for that mobile phone,' you do actually have to take quick, proactive action to try and resolve it."

I'VE CHANGED MY PASSWORD SO MANY TIMES I'LL HAVE TO FIND A HACKER TO TELL ME WHAT IT IS!
Englehart ©HARTFORD COURANT.
IDENTITY THEFT
caglecartoons.com courant.com/boblog on facebook and twitter

Quote of the Month

"If we don't act now to safeguard our privacy, we could all become victims of identity theft."

— Bill Nelson, current administrator of the National Aeronautics and Space Administration (NASA). Nelson previously served as a United States senator from Florida.