LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Board:

Congratulations go to the re-elected officers as follows: President Mark Lee, Vice President Bethany Verble, Secretary Melanie Marks, Treasurer Chris Arsenault, and Training Director Molly Jeltema. Thank you for continuing to serve!

We are still looking for one more person to fill a vacated board seat. Contact LACFE President Mark Lee if you would like information on the position (president@lansingacfe.com).

Annual Meeting and Training:

Thank you for joining us at the Annual Meeting and Free Training event!

LACFE Fall Conference:

Stay tuned for upcoming information about the Fall Conference that will likely be held in November. We're looking at some in-depth training that will be fascinating.

In This Issue

Fraud Talk Podcast

Chopping Down Black Axe - Tom Cronkright - Fraud Talk - Episode 135

Tom Cronkright, the lead witness in the FBI's inditement of Black Axe, an international cybercrime syndicate based out of Nigeria, speaks with ACFE President John Gill, CFE, in this month's episode of Fraud Talk. As the co-founder of CertifID and CEO of a title agency, Tom has been at the forefront of helping the real estate industry address payments fraud and discusses his experience as a victim of fraud and the operations of the international fraud group he helped indict.

Chopping Down Black Axe - Tom Cronkright - Fraud Talk - Episode 135 | Fraud Talk (podbean.com)

UPCOMING EVENTS

LOCAL:

SEMCACFE Southwest Michigan Area Chapter
Monthly Meeting October 5th is Student Night
St. John's Banquet & Conference Center, Southfield MI
Learn more: https://semcacfe.org/meetinginfo.php?id=89&ts=1695385411

ACFE Southwest Ohio Chapter - Detecting Human Trafficking Enterprises in Southwest Ohio
In-Person/Virtual
Friday October 13, 2023
12:00 – 1:00pm
Learn more: https://swohacfe.org/event-5352970

MICPA Critical Issues That CPAs in Industry Will Need to Face This Year
MICPA Learning Center Troy, MI
October 23, 2023
8:00 am - 11:30 am
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=148429

Twin Cities ACFE and Central Ohio Chapter Present: Wirecard Scandal
Virtual
November 8, 2023
LACFE Members in good standing are eligible for the 'membership rate'.
Learn more: https://twincitiescfe.org/meetinginfo.php

ACFE Southwest Ohio Chapter
5th Annual Dayton Fraud, Cyber & Ethics Conference
In-Person/Virtual
November 15 - 16, 2023 (early registration ends October 31st)
Learn more: https://swohacfe.org/event-5351176 and see poster below!

NATIONAL:

ACFE Understanding the Mindset of a Fraudster
Virtual Seminar
November 28-29, 2023 (early registration ends September 15th)
Learn more: Event Details (acfe.com)

ACFE Contract and Procurement Fraud
Virtual Seminar
December 5-7, 2023 (early registration ends November 6th)
Learn more: Event Details (acfe.com)

****For Chapter Leaders** ACFE Chapter Leaders Summit**
Omni Austin Hotel Downtown, Austin Texas
December 14–15, 2023
Learn more: Event Details (acfe.com)

2023 CHAPTER OF THE YEAR

ACFE Association of Certified Fraud Examiners

Southwest Ohio Chapter

SOUTHWEST OHIO CHAPTER

5th Annual DAYTON FRAUD, CYBER & ETHICS CONFERENCE

NOVEMBER 15 & 16, 2023

12:00PM-4:30PM EASTERN

VIRTUAL CONFERENCE *(HELD ON ZOOM)*

8 total hours of CPE* *(4 each day)*

(including 2 hours of Approved ACFE Ethics/Ohio PSR Ethics credit)

Co-sponsors: AXIOM® CONSULTING

University of Dayton Center for Cybersecurity & Data Intelligence

Pricing: EARLY BIRD *(By October 31, 2023)*

$75 one day | $100 both days

Regular Price: $100 one day | $125 both days

REGISTER AT: **https://swohacfe.org**

*CPE credits are based on a 50-minute hour. CPE is offered through the ACFE as well as the Accountancy Board of Ohio (sponsor number CPE.00467).

NOVEMBER 15TH

ADAM LAWSON

Supervisory Special Agent, FBI Cincinnati – Cyber Squad

1 CPE

FBI Overview of the Cyber Threat Landscape

Mr. Lawson's FBI cyber team covers the lower 48 counties of Ohio for cyber intrusion matters. Mr. Lawson will provide an overview of the cyber threat landscape to include a description of threat actors and their motivations, the most common methods of cyber attacks, what to expect from the FBI after reporting an attack, and lessons learned from the victim's perspective.

JENNIFER MACKOVJAK *CFE, PI*

ANDREW KEITH *PI*

Co-founders and Partners, 221B Partners

1 CPE

A Look Under the Hood: What You Don't See if You Stop with Databases

Databases and municipal, state, and federal information and records indices provide invaluable research leads but typically don't tell "the full story." This presentation will highlight the importance of obtaining information from primary sources and not just relying on database records, court and government portals, and secondary sources.

HARRY LIDSKY

Special Agent in Charge (retired), U.S. Department of Justice and Founder, 4th Dimension Investigative and Security Solutions (4DISS)

2 CPEs

Off-Beat: Fugees Founder Pras Michel's $100,000,000 Failed Attempt to Influence President Trump and the DOJ

Mr. Lidsky will present a case study focusing on the domestic arm of an international conspiracy. He will discuss how Fugees band member Prakazrel "Pras" Michel organized a small group of co-conspirators seeking to facilitate the dismissal of the 1MDB investigation and secure the extradition of a Chinese asylum-seeker at the request of Low Taek Jho, a.k.a. Jho Low, the alleged mastermind behind the 1MDB scheme, and subject of the bestseller book "Billion Dollar Whale." Michel's group aspired to influence the top echelons of the US government, including the President of the United States and the Attorney General of the United States.

NOVEMBER 16TH

MARY BRESLIN *CFE, CIA*

Founder & Managing Partner, Verracy

ACFE 2023 Baker Award Recipient

1 CPE

Unveiling the Thrilling World of ChatGPT and Fraud Detection

ChatGPT isn't just a buzz term; it's a gateway to a whole new level of intrigue and deception. In this session, Ms. Breslin will delve into the cutting-edge applications of ChatGPT and explore the innovative ways in which fraudsters are exploiting its power to commit fraud. But that's not all! Get ready to witness a captivating showdown as we reveal how ChatGPT and other awe-inspiring AI tools can become formidable allies in the fight against fraud. Don't miss this face-off between deception and defense, as we unlock the potential of ChatGPT to empower fraud-fighters worldwide.

PIERRE RIVOLTA *Ph.D., CFE*

Associate Professor, Department of Criminology and Criminal Justice - Mount St. Joseph University

1 CPE

Fraud Theory, Revisited: An Examination of the Fraud Triangle and Competing Explanations For Fraud and Other Financial Crimes

In this session, Dr. Rivolta will summarize academic research on fraud theory, with a particular emphasis on the "fraud triangle." Attendees will learn about the origins of the fraud triangle, examine its empirical assessments, review its geometric (and other types of) evolutions, ponder its limitations and criticisms, assess its relevance to practitioners, and contemplate other theories of fraud causation.

ANTHONY J. MENENDEZ *MSA, CPA, CFE*

George A. Dasaro Distinguished Clinical Assistant Professor of Accounting, Loyola Marymount University

ACFE 2016 Sentinel Award Recipient

2 Ethics CPEs

A Whistleblower's Tale

Mr. Menendez is the renowned "Accountant Who Beat Halliburton" and a corporate whistleblower under Sarbanes-Oxley whose work ultimately led to significant advancements in protections for corporate whistleblowers. In this presentation, Mr. Menendez will recount the key events that led him to blow the whistle on oil giant Halliburton, and he will detail the ensuing fight for his livelihood, his credibility, and his family during a decade-long legal battle.

Medically Necessary

September 29, 2023
Larry Benson
https://fraudoftheday.com/medically-necessary/

Will Medicare cover it? Roughly 11,000 Americans age into Medicare each day in the United States and the majority of them are asking that very question. Not an unreasonable question since the complexities and limitations of Medicare enrollment and policy changes can be overwhelming for patients and providers alike. For instance, Medicare will pay for urine testing samples if they are medically necessary. But it won't cover court ordered samples, for purposes of determining compliance with drug court rules. Ronald Coburn is familiar with the limitations of Medicare benefit coverage. Because Coburn owned a urine testing laboratory called LabTox. And he wanted to ensure that all urine tests that his company processed got paid for by Medicare.

Coburn obtained most of the urine drug samples that his company tested from facilities that provided substance abuse recovery. The programs were typically faith-based or homeless shelters which used drug testing to ensure that participants were drug free. Coburn got the facilities to refer urine samples to LabTox by falsely saying the cost would be covered by Medicaid and Medicare under a blanket order signed by a medical provider. Not his one and only in this scheme. Coburn then paid a doctor, identified only as Dr. O.J, $1,000 a month for the use of his signature. Dr. O.J. didn't see the patients, didn't choose which tests would be performed and didn't review the results. Coburn took care of that, along with submitting fraudulent bills to Medicare.

Coburn received from his scheme at least $1.5 million each year between 2017 and 2021. Because he had concealed his ownership of LabTox , Coburn thought he could avoid tax returns. But not reporting fraudulently received funds is actually illegal. And the Internal Revenue Service did not disappoint. One September 14, 2023, Coburn was found guilty and agreed to pay restitution of almost $6 million to both Medicare and the IRS.

Shout out to the Internal Revenue Service in this case.

Today's Fraud of The Day is based on article "Lexington business owner admits health fraud over urine samples, evading income taxes" published by the Lexington Herald Leader on September 14, 2023

The owner of a Lexington laboratory has admitted defrauding taxpayer-funded insurance programs and hiding his business ownership to avoid more than $3.5 million in federal income taxes. Ronald Coburn pleaded guilty this week in federal court in Lexington to one charge of health care fraud and a charge of tax evasion, according to court records.

Coburn owned LabTox LLC, which among other services tested urine drug samples for drugs. Coburn took part in getting payments from Medicaid and Medicare for testing samples that that were not eligible for reimbursement, according to his plea agreement.

Too Good to be True? 4 Ways to Avoid Vacation Rental Scams

September 1, 2023
Abbie Staiger
https://www.acfeinsights.com/acfe-insights/4-ways-to-avoid-vacation-rental-scams

Booking a vacation rental online comes with the convenience of browsing listings from the comfort of home. But it also opens the door to scammers trying to take advantage of unsuspecting travelers. Vacation rental fraud often involves fake property listings, compromised accounts, bait-and-switch tactics, double bookings and other deceptive practices targeting short-term rental guests. Being aware of the common types of vacation rental scams and red flags can help you identify fraudulent behavior and even avoid becoming the victim.

Common Types of Vacation Rental Scams

Fake listings are among the most common vacation rental scams. Fraudsters create convincing listings for properties that either do not exist or are not actually available for rent. When an unsuspecting guest tries to book, the “host” collects payment and often ceases communication shortly after that.

Account takeover scams involve fraudsters hacking into real rental accounts on sites like Airbnb or VRBO. They then change the listing details and rent out the property as if they are the real owner. By the time the actual owner finds out, the guest has already sent payment to the scammer.

Bait-and-switch scams use fake photos of a luxury property to lure guests in. But when the guest arrives, the property is completely different, usually run down and nothing like what was advertised.

Double booking scams happen when a host books the same rental property to multiple guests for overlapping dates. The guest who arrives last gets left scrambling when the home is already occupied.

Red Flags of Vacation Rental Fraud

Listings with limited photos, details and reviews, or that seem “too good to be true” should raise red flags. Also, be suspicious of prices drastically lower than comparable rentals in the same area. Fraudsters often target the most vulnerable in their schemes. By offering well-below-average prices on fake rentals, people who do not have much money to spend in the first place become targets for this kind of tactic.

A host who pushes you to book or pay outside of the rental platform is another huge red flag. Legitimate hosts will have you book and pay through the platform, which offers protection. Contact info that differs between the listing and booking is also suspicious and should be verified through the platform primarily.

Avoiding vacation rental fraud starts by understanding red flags of potentially fraudulent behavior. Anyone booking vacation rentals should always:

- Verify the host through the rental platform.
- Search the listing address to confirm it is a rental property, not someone's residence.
- Always book and pay through the platform, not directly with a host. Use payment methods with fraud protections that are built in.
- Consider rental guarantee insurance that can reimburse you if fraud does occur. Before the trip, confirm all the details with the host again. This helps uncover any bait-and-switch schemes ahead of time.

What to Do if You Are a Victim

If you are the victim of a vacation rental scam, immediately contact the rental platform if you booked through one and dispute the charges with your bank or credit card company. You can also contact local law enforcement and file complaints with the Federal Trade Commission (FTC) if the scam took place in the U.S. Victims might also consider reporting identity theft if any personal information was compromised. Once personal situations are addressed, it's helpful to leave online reviews about the fraud to warn others of similar schemes on that particular property or even in the area.

Being vigilant can help travelers avoid falling prey to vacation rental scams. Do your due diligence on listings, hosts and payments to ensure your next vacation rental experience is smooth sailing.

Video of the Month

All About Experts and Rule 702 - YouTube

J.D. – A Lawyer Explains
Experts are critical figures in litigation. Learn more about them here.

FBI Warns of Rising Trend of Dual Ransomware Attacks Targeting U.S. Companies

September 30, 2023
https://thehackernews.com/2023/09/fbi-warns-of-rising-trend-of-dual.html

The U.S. Federal Bureau of Investigation (FBI) is warning of a new trend of dual ransomware attacks targeting the same victims, at least since July 2023.

"During these attacks, cyber threat actors deployed two different ransomware variants against victim companies from the following variants: AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal," the FBI said in an alert. "Variants were deployed in various combinations."

Not much is known about the scale of such attacks, although it's believed that they happen in close proximity to one another, ranging from anywhere between 48 hours to within 10 days.

Another notable change observed in ransomware attacks is the increased use of custom data theft, wiper tools, and malware to exert pressure on victims to pay up.

"This use of dual ransomware variants resulted in a combination of data encryption, exfiltration, and financial losses from ransom payments," the agency said. "Second ransomware attacks against an already compromised system could significantly harm victim entities."

It's worth noting that dual ransomware attacks are not an entirely novel phenomenon, with instances observed as early as May 2021.

Last year, Sophos revealed that an unnamed automotive supplier had been hit by a triple ransomware attack comprising Lockbit, Hive, and BlackCat over a span of two weeks between April and May 2022.

Then, earlier this month, Symantec detailed a 3AM ransomware attack targeting an unnamed victim following an unsuccessful attempt to deliver LockBit in the target network.

The shift in tactics boils down to several contributing factors, including the exploitation of zero-day vulnerabilities and the proliferation of initial access brokers and affiliates in the ransomware landscape, who can resell access to victim systems and deploy various strains in quick succession.

Organizations are advised to strengthen their defenses by maintaining offline backups, monitoring external remote connections and remote desktop protocol (RDP) use, enforcing phishing-resistant multi-factor authentication, auditing user accounts, and segmenting networks to prevent the spread of ransomware.

Bad Phishing Attack

Quote of the Month

“Training is everything. The peach was once a bitter almond; cauliflower is nothing but cabbage with a college education.”

— Mark Twain, from Pudd'nhead Wilson (1894)