LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

LACFE Board Position Opening

Long-term Treasurer and Board Member, Chris Arsenault, has resigned from the board. Thank you Chris for your dedication to the LACFE and our mission!

Please contact President Mark Lee if you or someone you know is interested in serving on the LACFE Board: president@lansingacfe.org

LACFE Conferences

If you missed it, LACFE President Mark Lee summarized the Winter Conference training, see page 2.

The LACFE Spring Conference will be on May 21, 2024, initial details are on pages 3 and 4.

In This Issue

Fraud Talk Podcast: Inside the ACFE's Top 5 Most Scandalous Frauds of the Year
_____

Message from LACFE President, Mark Lee
_____

Upcoming Events
_____

Top 5 Fraud Trends of 2024
_____

Insights from the 2024 Anti-Fraud Technology Benchmarking Report
_____

Recent News Headlines
_____

Fraud Talk Podcast

Inside the ACFE's Top 5 Most Scandalous Frauds of the Year - John Warren - Fraud Talk - Episode 140

In this special edition of Fraud Talk, we focus on the ACFE's annual round-up featured in Fraud Magazine, a highlight anticipated by many in the industry. This year, we offer you an exclusive behind-the-scenes glimpse into the process of selecting the top five most scandalous frauds of 2023. Join John Warren, CEO of the ACFE, and Jennifer Liebman, Assistant Editor of Fraud Magazine, as they meticulously unravel each case, providing an in-depth analysis and insight into the complexities and implications of these notable frauds.

https://acfe.podbean.com/e/inside-the-acfe-s-top-five-most-scandalous-frauds-of-the-year-john-warren-fraud-talk-episode-139/

Message from the LACFE President:

I want to thank everyone who attended the LACFE Winter Conference on February 15th! We had a really good turnout and, for those who couldn't make it, here is a quick rundown. Hosted by Maner Costerisan in Lansing, attendees filled the conference room to learn about forensic linguistics from presenter Joe Koenig and about government embezzlement from Rick Roybal. Although the weather caused some unexpected delays for attendees and presenters alike, the conference was full of interesting and useful information.

Joe's presentation on forensic linguistics went into detail about how an interviewee's choice of words and the manner in which they communicate, as well as what they leave out, can offer glimpses into the portions of their story where they may be trying to hide something, or where they may have an emotional connection with the events being depicted. An interesting point Joe made was that memories have a physical aspect to them that fabricated tales just do not have. Because we experience events through all of our senses, powerful events can leave an imprint of those senses into our memory, such as associating a smell or sound with certain events. By adding the types of skills that Joe presented on to your fraud examiner toolbox, you should be better able to identify weak points in a subject's story, perhaps even helping to distinguish fact from fiction. They can definitely provide ques on where your follow up questions and efforts should be focused.

Rick gave a dynamic and engaging presentation on government embezzlement. Although centered on the Oregon Health Administration, the lessons are applicable to nearly any organization. One of the things Rick pointed out was the unique nature of this particular fraud. Most embezzlement schemes start slow and grow slowly over a long period of time, where this one occurred over a relatively short span of time and really focused on maximizing the amount stolen. The audience was engaged, and the group interaction led to some really good discussion.

I really hope to see you all at our Spring Conference on May 21st for what promises to be another interesting and unique presentation. Frank Perri, author of "Red Collar White Collar Crime," will talk about when typical white collar crimes turn violent and what they have in common. I am really looking forward to it! (See the announcement in this month's newsletter for more information!)

~Mark

UPCOMING EVENTS

LOCAL:

SEMCACFE 30th Annual Fraud Conference
April 16, 2024 (early registration ends March 31st)
7:30 AM - 5:00 PM
VisTaTech Center at Schoolcraft College
18600 Haggerty Road
Livonia, MI 48152
Learn more: SEMCACFE - Upcoming Events

LACFE Spring Fraud Conference - *Red-Collar, White-Collar Crime*
Presented by Frank S. Perri, JD, CPA, CFE
May 21, 2024
More Details Soon! See a primer on the conference below.

Lansing AGA - Webinar - Robotic Process Automation/AI
Webinar
March 6, 2024
2:00 – 4:00 PM
Learn more: Webinar - Robotic Process Automation/AI - (lansing-aga.org)

NATIONAL:

ACFE Utilizing Artificial Intelligence Tools in Anti-Fraud Programs
Virtual Seminar
April 18, 2024 (early registration ends March 19th)
Learn more: Event Details (acfe.com)

ACFE Detecting Fraud Through Vendor Audits
Virtual Seminar
April 19, 2024 (early registration ends March 20th)
Learn more: Event Details (acfe.com)

ACFE Tracing and Recovering Fraud Losses
Virtual Seminar
April 23 - 25, 2024 (early registration ends March 25th)
Learn more: Event Details (acfe.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

LACFE Spring Fraud Conference - *Red-Collar, White-Collar Crime* Presented by Frank S. Perri, JD, CPA, CFE

Frank S. Perri, JD, CPA, CFE

With over 25 years' experience as a criminal trial attorney, Frank also coined the term "red-collar crime". He has lectured at the graduate level in forensic accounting at DePaul University. In 2016, Frank was the ACFE Hubbard Award Recipient for best co-authored article in the *Fraud Magazine* coupled with authoring the books: Red-Collar, White-Collar Crime: Corporate, Predatory and Violent Fraud Offenders and Fraud Examination and White-Collar Crime: An Accounting, Behavioral, and Criminological Approach.

Red Collar Crime

In this presentation we debunk the myth surrounding the fraud offender profile as non-violent and how misperceptions about their profile increases the probability of erroneous risk assessments especially as to their potential for lethality. Topics include:
- The Origin of Red Collar Crime
- Fraud Detection and Homicidal Motive
- Criminal Thinking Patterns: What are they?
- Family, Fraud, and Violence
- Murder-for-Hire Considerations
- International Red Collar Considerations
- Fraud Detection and Workplace Violence
- Gender Distinctions and Red Collar Methodologies
- Red Collar Interview Case Study: What Went Wrong?
- Fraud Examination and Litigation Considerations
- Behavioral Risk Factors Facilitating Fraud Detection Violence

Predatory Fraud Offenders: The Formula Behind Their Success

In this presentation, we unpack the predatory fraud offender profile by examining risk factors that contribute to victims enhancing their trust and diminishing their skepticism of these predators to ultimately being exploited with ease. Topics include:
- Fraud and the Exploitable Concept of Trust
- Affinity Characteristics Facilitating Predation,
- Predatory Fraud Offender Skill Base
- The Role of Projection Bias Facilitating Predation
- The Role of Social Influence Facilitating Predation
- Organizational Fraud Predators: Target Preferences
- Challenges Overcoming Predator Victimization

- Regulatory Failures: Bernard Madoff and the SEC
- Mitigation of Predatory Financial Exploitation

Why Corporate Fraud Flourishes: A Multidisciplinary Approach

In this presentation, a multidisciplinary approach creating a template to understand why corporate fraud flourishes is provided. We learn how to spot corrupt leadership red-flags especially for the benefit of antifraud professionals. Topics include but are not limited to:

- Corrupt Leadership Displaying Criminal Thinking Traits
- Destructive Behavioral Leadership Traits
- Corrupt Leadership Interpersonal Strategies
- The Normalization of Corporate Fraud
- Challenges in Overcoming Corporate Fraud
- Followership Facilitating Corporate Fraud
- The Role of Ethical Fading and Ethical Blindness
- Corporate Governance Failure Risk Factors
- Whistleblowers: Public Heroes and Organizational Villains
- Mitigation of Organizational Misconduct

Terror Financing

In this presentation, attendees become acquainted with how terror organizations fund their operations. Topics covered include:

- Terrorism and Organized Crime Nexus
- Terror Financing Schemes
- The Movement of Terrorist Funds
- Al Qaeda's Reliance on Terror Financing
- New Trends: The Use of Cryptocurrency
- Mitigation Considerations

Top 5 Fraud Trends of 2024

February 20, 2024
Mason Wilder, CFE
https://www.acfeinsights.com/acfe-insights/top-5-fraud-trends-of-2024

Detecting and preventing fraud is a daunting task that requires anti-fraud professionals to regularly adapt to a continuously evolving risk landscape. There are consistent factors in fraud, like social engineering tactics that exploit human behavioral tendencies or external financial pressures that lead fraudsters to commit their crimes, but there are also trends and themes that emerge and affect the anti-fraud profession on a more limited timeframe.

Forecasting is inherently a risky exercise, but based on recent fraud-related news and discussions with subject matter experts over the course of regular ACFE operations, here are five trends that are expected to have a significant impact on the anti-fraud profession in 2024.

Scams Enhanced by Generative AI

Generative artificial intelligence (AI) technology, or deep learning AI models used for high-quality image, video, audio or text generation, became much more mainstream with the introduction of ChatGPT in late 2022. The proliferation of easy-to-use generative AI software, such as programs or apps that generate deepfakes, has already been utilized by fraudsters to generate more convincing images, video, audio and text in their scams, but the scale of its weaponization will grow tremendously in 2024, and affect both individuals and organizations. One major fraud involving deepfakes of multiple people on a single video call already caused a multinational company in Hong Kong to lose more than $25 million this year, and numerous other examples of scams ranging from virtual kidnappings utilizing voice cloning technology to romance frauds leveraging text generation similar to ChatGPT capabilities have been reported and will only increase.

As the technology gets better, so do the scams using it. Fraud examiners can help protect themselves, their employers or clients, and their communities by raising awareness about these scams, and encouraging everyone to exercise a high level of skepticism with any digital communications, but especially those that involve a request for money.

A Resurgence of Cryptocurrency and Digital Asset Fraud

Bitcoin was at its highest price since late 2021. Frauds and scams related to cryptocurrencies, coins, tokens and all the other confusing things under the digital assets umbrella have historically ebbed and flowed along with the prices of popular cryptocurrencies, particularly bitcoins. With increased enthusiasm around digital assets and more mainstream adoption, fraudsters will follow. Expect an increase in SIM swaps, digital wallet account takeovers, ransomware, investment scams, hacks or exploitation of decentralized finance (DeFi) companies, and any other fraud schemes either targeting or involving digital assets.

The irreversibility and pseudonymity of digital asset transactions makes them inherently riskier, even when they are not extra attractive to fraudsters due to crypto prices, so consumers should stay diligent about not reusing their passwords for digital wallets, considering

multifactor authentication protocols that do not rely on SMS, and being wary of any cannot-miss investment opportunities framing themselves as related to recently approved Bitcoin Exchange Traded Funds (ETFs). Sending fiat currency instead of cryptocurrency for a transaction will likely have more recourse available in the event of a fraud.

Meanwhile, fraud examiners at organizations that deal in digital assets or possess them should assess existing anti-fraud controls and look for opportunities to improve them.

Fraud Involving AI Service Providers

When a technology hype cycle kicks off, there is never a shortage of companies looking to cash in on the craze or investors looking to identify the next "unicorn" or spread investments across the sector to hedge their bets. This can create a lot of pressure for emerging technology-focused companies to perform, or at least maintain the appearance of performance to reassure existing investors and attract new ones, such as Theranos, Wirecard, Nikola and FTX.

With more than $150 billion underlined_reportedly invested in AI startups since the beginning of 2021, the same kinds of financial pressures that led leaders of the previously mentioned companies to fabricate results or employ creative (fraudulent) accounting practices are in place for the AI sector. This might play out as a singular, major fraud scandal affecting a major player in the sector, with the direct impact mostly limited to the company's investors and creditors.

Alternatively, it could play out in the failure of multiple start-ups on a smaller scale. Either outcome would likely shake public faith in the sector and in turn affect the trajectory of the technology's adoption and the viability of AI companies doing things by the book.

Fraud examiners tasked with due diligence or auditing engagements concerning AI service providers should keep these factors in mind and perhaps apply a little more scrutiny to make sure that they do not overlook any red flags.

Increased Obligations and/or Liabilities for Preventing and Detecting Fraud

The passage, or royal assent, of the United Kingdom Economic Crime and Corporate Transparency Bill in late 2023 establishes a new failure to prevent offence [sic] for organizations that profit from fraud committed by their employees, even if they were unaware of the fraud while it was occurring. Since new laws and/or regulations that emerge from Europe often end up producing copycat responses from other regions, anti-fraud programs could be tasked with preventing yet another fraud-related liability.

Meanwhile, the International Auditing and Assurance Standards Board (IAASB) recently proposed a change to its standards for auditors that would increase the responsibilities to detect fraud in a client's financial statements. This came months after the Public Company Accounting Oversight Board (PCAOB) made a similar proposal to update its standards related to auditors' responsibilities to detect fraud. Although neither proposal has yet been adopted and reflected in updates to the standards, it could happen in 2024 and would have a significant impact on auditors and ultimately strengthen the anti-fraud profession, assuming auditors embrace the upgraded fraud detection responsibilities.

Continued COVID Fraud Enforcement in the U.S.

In 2022, the United States passed legislation that extended the statute of limitations for fraud related to several federal benefit programs from five years to 10, meaning that federal law enforcement in the U.S. will not have to be as selective with investigation, enforcement and prosecution of these fraud cases.

Many fraudsters who carried out COVID benefit fraud have yet to face any consequences from their schemes, simply because the resources required to work through the caseload have exceeded what the federal government has been able to allocate. As these fraudsters have been out there living their best lives, it is reasonable to suspect they have been looking for other fraud schemes to carry out, since most fraudsters do not decide to quit committing fraud when they believe they have gotten away with it.

However, there are a great many federal law enforcement agents working dutifully to investigate these cases, so many fraudsters will be getting very unwelcome knocks on their doors in 2024 that could ultimately provide investigative leads for other frauds they have committed. These investigations and prosecutions will also likely provide incredibly valuable blueprints for future fraud investigations as law enforcement agents develop and hone new techniques to uncover and prove fraud, trace assets and recover funds.

Time will tell how accurate or relevant these trends end up being this year, but hopefully these valuable insights can be extracted to aid in the prevention, detection or investigation of fraud in 2024 and beyond.

Video of the Month

My Wall Street Heist: The Story of Gary Foster – Trailer (youtube.com)

Gary Foster grew up in Jamaica before moving to New Jersey, where he landed his dream job on Wall Street. However, company loyalty turned to anger as he believed he was being deliberately underpaid. Leaning on trust from his coworkers and lack of controls, Foster ultimately stole $22 million from the company and avoided detection for several years.

Insights from the 2024 Anti-Fraud Technology Benchmarking Report

February 13, 2024
https://www.acfeinsights.com/acfe-insights/2024-anti-fraud-technology-benchmarking-report

The 2024 *Anti-Fraud Technology Benchmarking Report*, developed by the Association of Certified Fraud Examiners (ACFE) in partnership with SAS, highlights a significant trend in the fight against fraud. Drawing on survey data from nearly 1,200 ACFE members, this report underscores the growing interest and gradual adoption of generative artificial intelligence (AI) and machine learning (ML) in anti-fraud measures.

Generative AI: A New Frontier in Anti-Fraud Strategies

An overwhelming 83% of anti-fraud professionals anticipate integrating generative AI into their strategies within two years, marking a peak in interest since the survey's inception in 2019. This enthusiasm is mirrored by the data, showing a projected threefold increase in AI/ML utilization in anti-fraud programs over the next 24 months. Despite this keen interest, actual adoption has been slow, with only an 18% uptake among organizations—a mere 5% growth since 2019.

The Evolving Anti-Fraud Tech Landscape

The report not only sheds light on AI and ML, but it also reveals an uptick in the use of biometrics and robotics in fraud prevention efforts. Biometrics usage has increased by 14% since 2019, with 40% of respondents utilizing this technology. Robotics has seen a substantial rise from 9% in 2019 to 20% in recent years. This diversification of tools points to a broadening arsenal against fraud, even as the adoption of certain data analysis techniques has plateaued.

A Comprehensive Resource for Anti-Fraud Professionals

The report is complemented by SAS' online data dashboard, offering an in-depth analysis of anti-fraud tech trends across various industries and regions. This tool is invaluable for professionals seeking to tailor their anti-fraud strategies with the latest insights and data.

Navigating the Future of Fraud Prevention

The findings from the 2024 *Anti-Fraud Technology Benchmarking Report* signal a pivotal moment in the fight against fraud. As organizations navigate the complexities of implementing generative AI and other advanced technologies, the insights provided by the ACFE and SAS serve as a roadmap for strategic investment and ethical application. The potential of these technologies to revolutionize fraud prevention is immense, offering the promise of more accurate, efficient and comprehensive defenses against fraud, provided organizations first navigate the ethical and implementation challenges ahead.

Discover more about the evolving landscape of anti-fraud technology and how your organization can stay ahead in the fight against fraud by visiting the 2024 *Anti-Fraud Technology Benchmarking Report.*

Recent News Headlines

1/29/2024 [Manhattan DA pushes Venmo, Zelle, Cash App to crack down on fraud - ABC News (go.com)](#)

1/29/2024 [The IRS is launching a direct file pilot program for the 2024 tax season — here is how it will work (msn.com)](#)

1/23/2024 [Southern District of Texas | Football ticket scammer sent to prison | United States Department of Justice](#)

2/2/2024 [Alpena attorney arrested for various felonies, including embezzlement and fraud](#)

2/6/2024 [Biggest Deepfake Fraud? Fake Zoom Meeting, CFO Cloned, $25 Million Stolen](#)

2/7/2024 [Prominent NYC developer Nir Meir arrested in vast years-long $86M fraud scheme: prosecutors (msn.com)](#)

2/14/2024 [Michigan Woman Arrested For Role In Fraud Scheme Involving Theft Of Over $800,000 In Luxury And Designer Apparel And Accessories](#)

2/17/2024 [Michigan grocery store manager stole $750K from self-checkout kiosks over 16 months: state feds](#)

2/28/2024 [US Money Laundering Fight May Soon Turn Corner](#)

2/29/2024 [Detroit nonprofit director charged in scheme that stole houses from dozens of residents](#)

Quote of the Month

"Torture the data, and it will confess to everything"

— Ronald Coase, a British economist and author. Coase was educated at the London School of Economics, where he was a member of the faculty until 1951. He was the Clifton R. Musser Professor of Economics at the University of Chicago Law School, where he arrived in 1964 and remained for the rest of his life. He received the Nobel Memorial Prize in Economic Sciences in 1991.