Association of Certified Fraud Examiners

Austin Chapter – Spring 2024 Seminar

PROGRAM

Detailed Descriptions and Biographies of Speakers

Texas Financial Crimes Intelligence Center (FCIC): Investigating Organized Financial Crime **by Capt. Jeff Roberts, Texas FCIC, Tyler, Texas**

Organized crime is usually the driving force behind the majority of financial crimes, including gas pump, ATM, & POS skimming; check forgery, fuel theft, and many more. Texas FCIC is the statewide agency authorized by the legislature in 2021 to bring together local, state, and federal law enforcement agencies along with financial, fuel, and retail industries to protect consumers and the Texas economy. FCIC also is a source for training of law enforcement and industry partners in methods to prevent, identify, and investigate financial crimes.

Learning Objectives – After attending this session, participants will be able to:

- Explain the authority and types of investigations done by FCIC
- Describe some of the methods utilized by this relatively new state agency to leverage the combined knowledge and skills from multiple law enforcement sectors to combat organized financial crime
- Identify the types of specialized training provided to law enforcement and industry partners

Speaker's Bio: Jeff Roberts began his law enforcement career with the Tyler Police Department in 2007. As a detective in the Special Investigations Division, he served as a Task Force Officer with the U.S. Secret Service North Texas Financial Crimes Taskforce (NTFCT) focused on fighting organized financial crimes with an expertise in skimming investigations. Jeff co-created Texas Commission on Law Enforcement (TCOLE)-approved training for Texas law enforcement seeking standardization for skimmer specific investigation techniques. In 2019 he worked on legislative changes assisting law enforcement as they adapt to ever-changing fraud trends. In October 2021, Jeff transitioned to his current role as Captain of Internal Operations at the Texas Financial Crimes Intelligence Center (TX FCIC).

Ransomware, Cyber-warfare, AI Viruses, & More
by Zach Kelley, Faculty member, Information Systems & Analytics

With so much to discuss regarding cybersecurity and artificial intelligence, it is difficult to know where to begin! First, this session will focus on increases in ransomware and payments made (such as $22M by Change Healthcare and the subsequent implosion of their Blackcat attackers. A second topic will be cyber-warfare crossfire hitting unintended targets (such as small-town water utilities) and focused assaults on the U.S. from China and Russia. Then, there will be a discussion of the first viruses being forwarded through AI and black box issues with GPT models. Prior to the session, consider reviewing the following:

- Muleshoe Water Supply, 2024: www.texastribune.org/2024/04/19/texas-cyberattacks-russia/
- Map of ransomware attacks 2018-2024: www.comparitech.com/ransomware-attack-map/
- Krebs on Security: https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/

Learning Objectives – After attending this session, participants will be able to:

- Describe the increase in ransomware attacks, corporate responses and consequences
- Explain how municipal water supply systems inadvertently became victims of cyberwarfare
- Describe the real targeted cyber attacks against the U.S. by China and Russia
- Analyze the potential impact of AI viruses and black box issues with GPT

Speaker's Bio: Zach Kelley, BBA (CIS) & MS (Accounting Information Technology) is a faculty member in Information Systems & Analytics, teaching courses that have included: Information Security, Accounting Information Systems, Business Intelligence, Programming, Agile, Statistical Analysis, & ERP. He has more than 10 years professional experience in senior IT leadership positions (up to & including CEO) and more than 20 years' experience in logistics & SCM, and far more years than he is willing to admit in IT in general. Experience was in firms with annual revenues from $5 to $700 million. Also experienced in the deployment, maintenance & modification of ERP systems built for industry-specific applications (SAP, Innovative IES, Infor XA, and one in-house logistics system).

"Changing Privacy Protection Laws in Texas"
by [speaker TBD]

This session will include a discussion of state laws enacted during the 2021 and 2023 legislative sessions and plans for additional legislation for the 2024 session, all of which have been designed to protect the privacy of our citizens.

Case Study: Follow the Money - A Forty Million Dollar Medicaid Heist
by Donna Knapp, CPA, CFF, CFE, Forensic Accounting Investigator

This is the largest Medicaid fraud case ever investigated by the TX HHSC Office of the Inspector General (OIG). It began when the OIG Data Analytics team identified the provider as an outlier. The case was handed to the Major Case Unit (MCU) of the OIG to investigate, and a comprehensive forensic accounting analysis was conducted that uncovered fraudulent billing and money flowing to key suspects through shell companies. MCU worked jointly with federal authorities to identify the scope of the fraud. A pattern of excessive billing with little to no services provided and the use of unskilled staff to operate the facility were identified by the investigators. Over a four-year period, this facility generated enough billings to make them the largest mental health provider in Texas even though they accommodated less than 60 patients.

Learning Objectives - after attending this session, participants will be able to:

- Identify the fraud schemes utilized to overbill Medicaid
- Describe methods, including forensic accounting, OSINT, data analytics, asset forfeiture, and interviewing, used by state and federal authorities to investigate this case
- Analyze how the fraud could have been prevented

Speaker's Bio: Donna Knapp, CPA, CFF, CFE, is a Forensic Accounting Investigator with the Major Case Unit (MCU) of the TX HHSC Office of the Inspector General (OIG).
She has more than 20 years of experience in fraud examination and forensic accounting. She has been a member of the ACFE for 14 years.

Financial Fraud in Sports
by Jesse Silvertown, CA, CPA, CFF

Some aspects of professional sports organizations and the athletes themselves (both pro & amateur) make them targets for many kinds of fraud and corruption ranging from investment schemes to embezzlement to bribery. One of the latest to make news headlines was the $22 million fraud against the Jacksonville Jaguars committed by one perpetrator over a period of only four years. That fraud, along with several others, will be discussed to demonstrate how they were committed and factors that make the sports industry particularly vulnerable.

Learning Objectives – After this session, participants will be able to:

- Identify types of fraud committed against professional athletes and sports organizations
- Explain factors that cause the athletes and sports organizations to be vulnerable
- Analyze ways in which such frauds might be prevented
- Demonstrate how forensic accountants operate within the sports industry

Speaker's Bio: Mr. Silvertown earned his degree from Ivey Business School in Western Ontario and became a Chartered Accountant & Chartered Professional Accountant in Canada; he then obtained his CFF from the AICPA in the U.S., all while working at EY, first as an auditor and then in forensic accounting. He is a 15-year finance & accounting veteran in media, sports, tech, and entertainment. His consulting firm, The Ledge Company, provides services in the area of CFO advisory, forensic accounting, M&A, and disputes. In his career, Silvertown has worked on hundreds of matters and authored many articles on the topic, including one on the Jacksonville Jaguars fraud in December 2023 issue of *Forbes*: www.forbes.com/sites/jessesilvertown/2023/12/15/the-jaguars-employee-charged-with-22-million-of-fraud-is-a-wakeup-to-the-sports-industry/?sh=5aaa6ef56153