LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Please don't forget to renew your LACFE membership by January 31st! Membership | (lansingacfe.com)

In This Issue

Fraud Talk Podcast

Scam's Calling: Unraveling the Robocall Racket - Alex Quilici - Fraud Talk - Episode 136

"We've been trying to reach you about your car's extended warranty" is an all-too-common robocall scam aiming to bilk victims out of their money. Alex Quilici, CEO of YouMail, discusses the intricacies of robocalls, what differentiates beneficial robocalls from scams and the regulations that both aid and obstruct the fight against these schemes with Jennifer Lieberman, assistant editor of Fraud Magazine, in the latest episode of Fraud Talk.

Scam's Calling: Unraveling the Robocall Racket - Alex Quilici - Fraud Talk - Episode 136 | Fraud Talk (podbean.com)

UPCOMING EVENTS

LOCAL:

AGA Webinar - Uniform Guidance and Grant Accounting
Webinar
January 17, 2024
2:00 – 4:00 pm
Learn more: https://lansing-aga.org/EventCalendar/EventDetails.aspx?ItemID=151&mid=24&pageid=22

ACFE South Florida Chapter - Medley of Fraud
Webinar
January 18, 2024
Learn more: https://acfesouthflorida.org/page-18098

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

NATIONAL:

ACFE Fraud Risk Management
Virtual Seminar
February 20-22, 2024 (early registration ends January 22nd)
Learn more: Event Details (acfe.com)

ACFE Compliance Challenges with FinCEN's Beneficial Ownership Database
Virtual Seminar - ** FREE FOR ACFE MEMBERS**
January 31, 2024
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)

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

Fraud, Waste and Abuse Schemes in the Addiction Treatment Industry

December 05, 2023
Isaac Asamoah
https://www.acfeinsights.com/acfe-insights/addiction-treatment-industry-fraud

Substance use disorder (SUD), commonly referred to as just addiction, is a treatable mental disorder that affects a person's brain and behavior, leading to their inability to control their use of substances like legal or illegal drugs, alcohol or medications. With addiction being the most severe form of SUD, symptoms can range from moderate to severe. In 2021, drug abuse was added to the list of high-risk situations by the Government Accountability Office (GAO). GAO high-risk list are areas susceptible to increased fraud, waste and abuse.

Treatment for substance use disorders was an out-of-pocket expense that only the wealthy could afford until the Mental Health Parity and Addiction Equity Act was passed in 2008. More people now have access to SUD treatment because of the passage of legislation like the Patient Protection and Affordable Care Act. The Department of Health and Human Services (HHS) estimates that the financial cost of substance addiction is $193 billion for illegal drug usage and $249 billion for alcohol consumption.

Causes Of the Opioid Crisis in the United States

The Congressional Budget Office pinpoints 3 factors that led to the Opioid epidemic in 2018. These factors are increase in prescription by physicians, increase in demand for self-medication, increase in consumption of opioid medications due to the illicit access of the market and illegal trafficking of opioids into the market.

What is so peculiar with fraud and abuse in substance use abuse and addiction treatment?

Fraud occurs in a variety of healthcare settings, such as laboratories, dentist offices, home health agencies, pharmacies and transportation. What, therefore, distinguishes fraud, waste and abuse in drug use disorders? According to (SAMSHA 2014), the SUD treatment sector is expected to continue growing, reaching a value of $34 billion by 2020. Only 2.7 million (6.5%) of the 41.1 million persons who need treatment for substance use disorders (SUD) during the course of the previous year received it at a specialty treatment center, according to the 2020 National Survey on Drug Use and Health (National Survey on drug abuse and health, 2020). Help is needed for vulnerable individuals to treat their substance dependence, yet many of them receive little to no assistance because of fraud, waste and abuse schemes. Zachary A. Cunha, the defendants' attorney, stated, "What makes the fraud scheme that we have charged today particularly pernicious is that it was not only, as we allege, designed to defraud by enriching these defendants with federal and private healthcare dollars they did not earn," but it also defrauded a vulnerable population of recovery patients of the full, genuine support and treatment that they need to have.

As per an investigation by STAT and the Boston Globe, individuals struggling with drug addiction are being used as pawns in a large-scale nationwide insurance fraud operation. Taking advantage of the growth in opioid addiction, these profit-seekers have accepted patients from all around the country. For Peter SanAngelo, who had been using heroin for ten years and was homeless, the promise of free insurance and lavish rehab in a faraway state turned out to be a lifeline. Using a fictitious address, a patient broker registered the Massachusetts man in a Pennsylvania Blue Cross plan and bought him an airline ticket to Florida. They even made a money-saving offer to purchase him cigarettes. Three months after the 33-year-old drug overdosed, he passed away.

Agencies Collaborating to Tackle Substance Use Disorder Treatment Fraud

The Federal Bureau of Investigations (FBI) is the primary agent charged with tackling healthcare fraud in the United States. However the FBI works with federal and state agencies such as the Center for Medicaid and Medicare Services (CMS), Department of Health and Human Services – Office of Inspector General (HHS – OIG), the Substance Abuse and Mental Health Services Administration (SAMSHA), Food and Drugs Authority (FDA), Center for Disease Control (CDC), Health Resources Services and Administration (HRSA), Drug Enforcement Administration (DEA), US Department of Justice – Office of Inspector General (USDOJ – OIG), Heroin and Opioid Awareness, Department of Homeland security (DHS) and the office of National and Drug Control Policy (ONDCP) etc. Apart from these federal agencies, the FBI works with state and private public agencies such as the Medicaid Fraud Control Unit (MFCU), Healthcare Fraud Prevention Partnership (HFPP), National Healthcare Anti-Fraud Association (NHCAA) and the National Insurance Crime Bureau (NICB).

Example of Fraud Scheme in Sober Homes

The announcement of the sober living homes cases on its one-year anniversary in 2020 marked the celebration of the first-ever national sober homes initiative, which included charges against more than a dozen criminal defendants in connection with over $845 million in allegedly false and fraudulent claims for tests and treatments for vulnerable patients seeking treatment for drug and/or alcohol addiction. The over $133 million in false and fraudulent claims that are additionally alleged in cases announced today reflect the ongoing efforts of the National Rapid Response Strike Force and the Health Care Fraud Unit Strike Force to prosecute individuals involved in illegal kickback and bribery schemes involving the referral of patients to substance abuse treatment facilities—where those patients may be subjected to medically unnecessary drug testing.

Example of Fraud Schemes in Addiction Treatment

One of the earliest healthcare fraud tactics is upcoding. In the addiction treatment sector, upcoding refers to doctors charging for higher level visits than actually completed (typically in an effort to receive higher reimbursements). For example, a doctor has up coded the service if they charge an addiction patient the maximum evaluation and management CPT 99215 (40+ minutes) for a visit that only took 25 minutes. CPT 99214 is the right code that the doctor ought to have used. A news release about an addiction treatment center accused of healthcare fraud was issued by the USDOJ in 2023. According to the documents included in the press release, Brier, Bruining and RCCA operated a chain of addiction treatment centers but failed to provide

patients with the required therapy and counselling sessions. In addition, they commonly submitted claims for 45-minute counselling sessions to Medicare, Medicaid and other health care payers, even though the sessions typically lasted 10 minutes or less. There have been times when the available therapist could not have finished the total quantity of treatment sessions in a 24-hour period due to the volume of sessions being billed at this rate.

Patient brokerage FWA schemes in the addiction industry includes patients shopping for prescriptions from physician to physician. Patients occasionally receive more prescriptions for medications than they need. This results in patients selling or giving their medications to family and friends. These medications are usually paid for through federal and state insurance programs like Medicare and Medicaid. Obtaining patients from patient recruiters is another aspect of patient brokerage for doctors. In exchange for patients, this typically entails the doctor paying the recruiter gifts and incentives, or "kickbacks." A South Florida clinic convicted in a $112 million addiction treatment fraud scheme was highlighted by the USDOJ in 2022. According to the Boston Globe and STAT investigation, patient brokers are paid for putting insured people in touch with treatment facilities; the treatment facilities then pocket thousands of dollars' worth of claims for each patient. Because Blue Cross Blue Shield plans have generous benefits and few restrictions on using out-of-network treatment programs for medical care, they often target specific plans.

In the addiction treatment sector, invoicing for services not provided and performing unnecessary procedures for addicted individuals is another FWA scheme. To assist addicts in regaining sobriety, sober living homes are registering residents, but in the absence of stringent policies such as federal and state oversight agencies keeping an eye on and requiring proof of recovery from sober living homes, these patients might remain in the sober living homes as long as they can continue to bill federal and state insurance programs for profits at the expense of providing patients with high-quality care. The public was alerted to fraud schemes targeting Native Americans in May 2023 by the Department of Health and Human Services' Office of Inspector General. HHS-OIG advisory: Scammers set up fictitious sober living homes that claim to provide addiction treatment and assistance, specifically targeting vulnerable Native Americans. However, people who are asking for help are seriously put at risk because these places are fronts for illegal activity. In addition, Native Americans are the target of schemes including healthcare fraud and human trafficking. By adopting the identity of medical experts, thieves use victims' personal information and medical identities to sell fraudulent medical services or treatments. Subsequently, they make fraudulent charges for services that were never provided. A STAT / Boston Globe investigation revealed that patients are being moved to treatment centers hundreds of miles away from their homes for expensive, but frequently poor, care that is covered by premium health insurance benefits obtained using false addresses. In exchange for providing those patients, labs routinely pay fictitious bribes to sober houses. In order to continue receiving kickbacks fraudsters schedule a lot of tests or make drug-addled residents produce samples for patients who do not exist.

Three people were found guilty on Monday, according to federal prosecutors, of conspiracy to submit fraudulent claims for drug and alcohol treatment for students in order to cheat California's Medi-Cal program out of over $20 million. According to the statement, the group that was found guilty allowed students to enroll in its program for four years, until 2013, even if they had only once used alcohol or drugs. The students then produced paperwork to support their claim that they were suffering from a "medically diagnosed substance use disorder." Furthermore, the organization submitted bills for payment to the state's Medi-Cal drug program after forging student signatures on documents that purported to show that they had attended counselling sessions.

Post-mortem billing is the practice of doctors invoicing insurance companies—federal, state and private—for services provided to patients who have passed away. One technique to identify post-mortem I is to compare the date of service provided by the doctors with the member's death data that they have billed for. It is considered healthcare fraud if the billing was completed after the patient passed away. Medical practitioners frequently treat a variety of medical issues in their patients with controlled medications on a regular basis. From time to time, a provider may be subject to scrutiny by the Drug Enforcement Administration (DEA), which is looking into charges of drug diversion. A number of DEA enforcement actions, including the suspension or cancellation of their registration for the controlled substance, the loss of their state medical license or even criminal prosecution, may follow allegations that doctors or pharmacies are unlawfully dispensing controlled substances.

Video of the Month

Generative AI and its Role in Fraud Examination (youtube.com)

Artificial intelligence (AI) is growing into a widely accepted tool across industries. One of the most significant developments of this emerging technology is generative AI, which can be used by fraudsters to create human-like results that appear real and enhance elaborate fraud schemes.

From deepfakes to voice cloning, it's important for fraud examiners and anti-fraud professionals to recognize red flags and even utilize AI tools in their work.

The Dichotomy of Modern Government Fraud Schemes and Government Oversight's Contrasting Approach

January 02, 2024
Erik Halvorson
https://www.acfeinsights.com/acfe-insights/dichotomy-modern-government-fraud

While reading a recent Bloomberg article about deepfake imposter scams and new fraud trends, I was struck immediately by their graphic. There appeared to be an overwhelmingly substantial number of "high loss" fraud schemes being perpetrated in 2022 (as reported by the Federal Trade Commission). This was shocking as it appeared to show more high loss cases than low loss cases. This would signal a marked departure from decades of historical statistics. Statistics we, in program oversight, rely upon to strategize our anti-fraud endeavors.

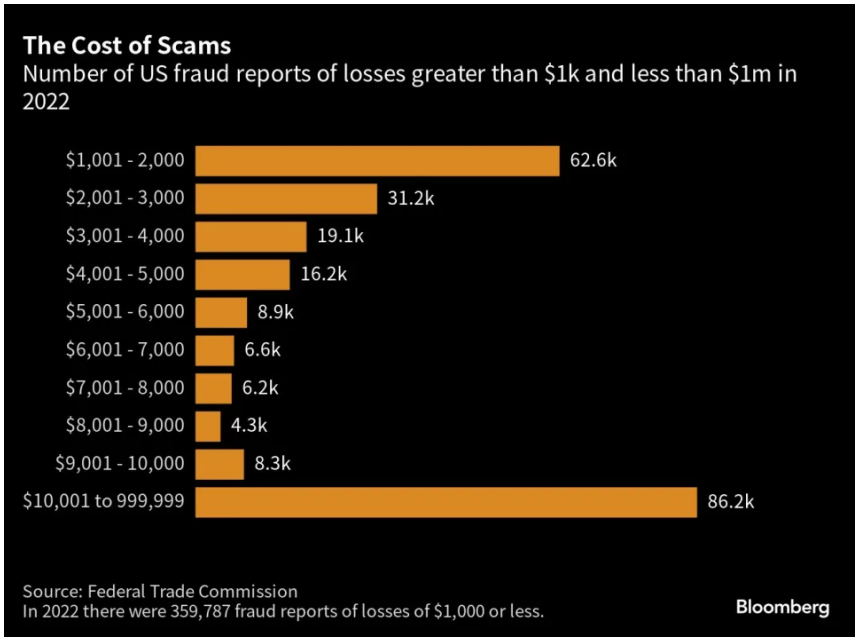

Figure one: The Federal Trade Commission's Cost of Scams 2022

Upon first glance, I felt a sense of righteous vindication as I have been shouting about the increased risk of sophisticated, high dollar loss schemes for years. Risk to the types of government programs that we see far too often splashed across the headlines of the news. The type of programs funded by massive budgets, guided by program managers who just review self-certifications; programs with funds spread out across multiple federal or state agencies, and overseen by contract or grant administrators trying to review hundreds of awards at a time. In fact, my fear over the last few years has changed. It is no longer the company that gets awarded a few grants or contracts and underperforms on them or fibs on an hourly timecard. My fear, and what keeps me up at night, has turned to stare down a massive tidal wave of domestic organized crime groups, international state sponsored groups, coordinated Fraud-as-a-Service (FaaS) groups, and creative hackers across the globe with technical prowess and seemingly unlimited energy.

All these groups share one common goal: the constant targeting of slow-moving and poorly defended government programs. These same government programs run by bureaucrats who fear if they slow the release of funds, even a little, to put controls in place they will be lambasted by their department or in the media.

Then I looked deeper into the chart and was offended as both a researcher and investigator. I realized first this is a terribly misleading graphic and second that even though I dislike the graphic the underlying premise of the article holds true. So, let us talk (briefly) about the graphic first, then explore the underlying message. You will notice a small footnote on the graphic that there were approximately 360,000 fraud reports of $1,000 or less. Combining the foot note with the strange Y-Axis groupings we see objectively there are significantly more small cases than large. Thus, bringing order back to our expectations of fraud case loss sizes and the volume of fraud we experience in government oversight.

Setting the graphic off to the side, let us talk about the underlying premise of the article. There is absolutely a new wave of fraud that is being perpetuated by new technology. Deepfakes are a part of those new fraud schemes, as the articles describe. Another fraud area on the rise is the use of generative AI Large Language Models (LLMs) and the use of “AI technology” to boost schemes by bad actors. AI Large Language Models are programs like ChatGPT. Technology boosts are technological enhancers like AI generated photos, voice simulators, phone number spoofers or AI coding systems that will write a malicious code for you. Both AI technology and technology boosts serve to bridge the gap for less technologically savvy bad actors who want to increase the complexity and sophistication of their fraud across their area of attack. One of the more interesting cases to emerge recently is dubbed FraudGPT. This program reportedly automates different phishing schemes and helps coach would-be fraudsters with suggestions on where to place malicious links. It also contains information on what the most frequently exploited online resources are and can even generate harmful code for its customers.

The rise of a Generative Pretrained Transformer (GPT) program without ethical constraints, used to support fraud, is fairly predictable. But, this GPT program has a surprising difference, the way this GPT service (purchasable through the dark web or via telegram’s messaging secure instant messaging groups) is marketed. FraudGPT has a monthly subscription fee. That is right, not even criminals can get away from the modern era of micro-billing services. Reportedly, the cost to use FraudGPT is $200 per month or $1,700 per year; which admittedly does provide a healthy 29% discount for annual membership. Despite being impressed by the discount, a subscription fee-based model is a business practice I did not think I would ever see in fraud. A practice that seems to demonstrate the organization and quasi-legitimacy of modern fraudsters. Because in the past can any of us see anyone linking their payment information to a service designed to break the law? That seems like one good cyber-based law enforcement operation away from unmasking a ton of bad actors.

Thinking about this situation objectively brings me back to sitting on a panel at Denver’s annual fraud retreat. During a panel I was asked how we should think about AI as it revolutionizes the world around us, and specifically in the area of fraud and anti-fraud mitigation. In my opinion, as oversight professionals, we need to expect to see two things. The first is that with AI boosting technological proficiencies we will see more fraud generally, both in increased sophistication and by volume of cases. The truth is technology has made fraud easier.

We need to do everything we can to prepare for this. The next is that while the area of technological fraud grows (and government slowly incorporates technological countermeasures and proactive analytics units) we will also see a rise in unsophisticated traditional fraud schemes. If you follow any of the financial crimes groups you will see that check fraud, for instance, almost doubled between 2021 and 2022 (up to ~680,000 instances in 2022) and will cost consumers a staggering $24B in 2023.

Technology has created a very strange dichotomy in our everyday world and fraud is a microcosm of that world. On the one hand, we have some of the most sophisticated technological fraud schemes ever now being attempted more often and by a broader swath of bad actors. On the other hand, as our focus, manpower and resources, move to combat technology enhanced schemes we leave a blind spot for unsophisticated schemes to thrive in. This idea about voluminous unsophisticated schemes thriving is supported by the footnote found on the initial chart we looked at. At a ratio of 2.2:1, schemes of $1,000 or less are outpacing all other fraud scheme loss amounts. If we look at scams which stole $10,000 or less on our initial chart, we see more than 523,000 cases (a ratio of more than 6:1 in favor of smaller schemes). While at the same time, year over year, we see a baffling continuous growth in larger, more sophisticated fraud schemes as well. Forcing us (in many cases) to either ignore one of the two types of fraud schemes or at best split our focus, funding and manpower. And in large government programs mired by years of “more with less” and “get the money out ASAP; we will chase the fraud later” this is a recipe for disaster.

Ultimately as fraud fighters trying to combat a rising tide of fraud of all levels of complexity, we need to be more flexible and dynamic. To do this we should leverage new technology and fraud analytics techniques by implementing tools being developed by private and commercial software companies. We should understand that social science research has progressed in areas of psychology, criminology, sociology and machine learning/AI that support our effort to identify fraud schemes earlier. This will give our controls a competitive advantage in identifying fraud and keeping losses low.

We also need to invest time and money into growing our people skills. As a special agent of 13 years, I have witnessed a steep decline in our ability to manage human assets, especially post-pandemic. We need to hone interview skills. We need to understand how to build (and maintain) long term strategic relationships with individuals outside our oversight field. And, even with the growth in technology we should remember our best assets are still our people. Especially supporting those that still possess their creative problem solving and optimism in the face of an increasingly difficult bureaucratic system to work and thrive in.

Fusing the human element with technological and research-based advancements might just give us the boost we need to combat these schemes. And while I cannot say for sure it will work, I can say for sure that if we fail to innovate and implement agile oversight we will fail. And failing means we continue to see headlines about losing billions of dollars in federal funds to fraud — headlines that will continue to erode public trust in our ability and the necessity of our work.

Christmas Carols Cryptogram
SOLUTION

1.0 COME ALL YE FAITHFUL

2.SILENT NIGHT, HOLY NIGHT

3.DECK THE HALLS WITH BOUGHS OF HOLLY

4.HARK! THE ANGELS SING

5.THE FIRST NOEL

6.WE WISH YOU A MERRY CHRISTMAS

7.IT CAME UPON THE MIDNIGHT CLEAR

8.I'M DREAMING OF A WHITE CHRISTMAS

9.AWAY IN THE MANGER

10.SANTA CLAUS IS COMING TO TOWN

11.SILVER BELLS

12.LITTLE DRUMMER BOY

13.GOD REST YE MERRY GENTLEMEN

14.RUDOLPH THE RED NOSED REINDEER

15.I SAW MOMMY KISSING SANTA CLAUS

16.JINGLE BELLS

17.HAVE YOURSELF A MERRY LITTLE CHRISTMAS

18.0 CHRISTMAS TREE

The Nutcracker Ballet

Word Search

SOLUTION