LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Artificial Intelligence is being discussed everywhere recently. The idea that machines could think is thought to be first proposed by Alan Turing in 1950. The first versions of AI were in use in the 1980s and most will have heard of IBM's inventions that beat both chess and Jeopardy champions. But where are we now?

Many of our daily activities use AI: internet searches, entertainment algorithms, digital personal assistants, perhaps your car, or even your job uses a form of AI. Some believe AI will further reduce the need for human employees while increasing speed and accuracy. Perhaps AI can provide a multitude of benefits and improvements to human life we only dream of?

Of course, with any technology there is the possibility of misuse. Stories abound of scammers using AI to defraud. National security may be targeted by criminals using AI to disrupt and damage infrastructure and/or computer networks. There are numerous appeals for regulation and a pause in development.

Collectively, we are charging into the AI space without knowing all the possibilities and downfalls. I don't believe anyone has all the answers. Perhaps, if we fully understood the potential harm we wouldn't go forward, but then, we'd lose the opportunity to be in awe of the benefits.

In This Issue

Fraud Talk Podcast

Law Enforcement vs. Private Practice Investigations - Tony McClements - Fraud Talk - Episode 129

In Episode 129 of Fraud Talk, Tony McClements, the Head of Investigations at Martin Kenney & Co., discusses his career trajectory through three decades in law enforcement to the private practice cases he oversees today. Joining ACFE Communications Manager John Duffley, Tony outlines the challenges between both types of investigations, the benefits to building a team of young, up-and-coming investigators, and emerging technologies and data reports that can be utilized for complex cases.

https://acfe.podbean.com/e/law-enforcement-vs-private-practice-investigations-tony-mcclements-fraud-talk-episode-129/

UPCOMING EVENTS

LOCAL:

Southeast Area Michigan Chapter of the ACFE
29th Annual Fraud Conference
VisTaTech Center at Schoolcraft College, Livonia, MI
April 25, 2023
7:30 am – 5:00 pm
Learn more: https://semcacfe.org/meetinginfo.php?id=84&ts=1677517825

ACFE South Florida Chapter #11 presents 2nd Annual Golf & Fraud Training
Webinar/In-Person
May 4, 2023
Learn more: https://acfesouthflorida.org/event-4876828

Southwest Ohio Chapter of the ACFE presents Explaining Fraud and Other Financial Crimes: Can Criminological Theories Help?
Webinar/In-Person
Friday, May 12, 2023
12:00 PM - 1:00 PM
Learn more: https://swohacfe.org/event-4928685

MICPA - Winning the Fraud Battle in the Digital Age: Prevention and Detection
MICPA Learning Center Troy, MI
Thursday, May 18, 2023
8:00 am - 4:00 pm
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=142339

NATIONAL:

ACFE AML Concerns and Issues for 2023
Webinar – *Free for ACFE Members*
April 4, 2023
12:00 p.m. EST
Learn more: Event Details (acfe.com)

ACFE Implementing an Effective KYC Customer Journey: From Journey Mapping to Deployment
Webinar – *Free for ACFE Members*
April 18, 2023
11:00 a.m. EST
Learn more: Event Details (acfe.com)

2023 ACFE Global Fraud Conference
Seattle, WA and Online
June 11 - 16, 2023
Learn more: 34th 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, please contact Jennifer Ostwald at jenny1661@hotmail.com

AI Fraud: The Hidden Dangers of Machine Learning-Based Scams

January 06, 2023
Laura Harris, CFE
https://acfeinsights.squarespace.com/acfe-insights/2023/1/6/ai-and-fraud

Artificial intelligence (AI) itself is not inherently fraudulent. AI is a field of computer science that focuses on the development of computer systems that can perform tasks that typically require human-like intelligence, such as learning, problem solving and decision making. AI technologies are used in a wide range of applications, including speech recognition, language translation and image recognition.

However, like any technology, AI can be used for both legitimate and illegitimate purposes. There is the potential for AI to be used to facilitate fraudulent activities, such as generating fake or misleading information, or automating scams or other fraudulent schemes. AI can also be used to detect and prevent fraud by analyzing data and identifying patterns that may indicate fraudulent activity.

Machine learning is a subfield of AI that focuses on the development of algorithms and models that can learn from data and improve its performance over time. Machine learning has already made a significant impact in a variety of fields, including computer science, finance, healthcare and transportation, and it is expected to continue to play a major role in the future of AI and other emerging technologies with the development of new algorithms and approaches that can enable machine learning systems to perform more complex and sophisticated tasks.

The use of AI in fraud depends on how it is implemented and used. Individuals and organizations should be aware of the potential risks and take appropriate measures to protect themselves from fraudulent activity, whether it involves AI or other technologies.

There are a few reasons why someone might use AI for fraudulent purposes:
Speed and efficiency: AI can process large amounts of data and perform tasks quickly, which makes it a potentially useful tool for automating fraudulent activities.

- Anonymity: AI can be used to carry out fraudulent activities without leaving a traceable human trail.
- Evasion of detection: AI can be used to generate fake or misleading information that is difficult for humans to detect as fraudulent.
- Personal gain: Fraud is often motivated by a desire to obtain financial or other benefits through deceptive or dishonest means. AI can be used as a tool to facilitate this type of activity.
- Generating fake or misleading information: AI could be used to create fake websites, social media accounts, or other online content that is designed to deceive or mislead people. This could include generating fake reviews or manipulating online ratings to mislead consumers.
- Automating scams: AI could be used to automate scams or fraudulent schemes, such as by sending out mass emails or text messages that are designed to trick people into

revealing sensitive information or sending money.
- Spoofing phone numbers or email addresses: AI could be used to create fake phone numbers or email addresses that are designed to deceive people into thinking they are communicating with a legitimate entity.
- Generating fake documents: AI could be used to create fake documents, such as contracts or invoices, that are designed to mislead or deceive people.
- Automation of scams: AI could be used to automate scams or fraudulent schemes, such as by sending out mass emails or text messages that are designed to trick people into revealing sensitive information or sending money.
- Evasion of detection: AI could be used to evade detection by generating fake or misleading information that is difficult for humans to identify as fraudulent. This could make it more difficult for authorities to identify and track down cybercriminals.
- Increased sophistication of attacks: AI could be used to increase the sophistication of cyber-attacks, such as by generating more convincing phishing emails or by adapting to the defenses of targeted organizations.

Impersonation

AI systems can be used to impersonate a real person in a number of ways, depending on the specific context and the capabilities of the AI system in question. Here are a few examples of how AI could be used to impersonate a real person:

- AI systems can be trained to generate text or speech that is designed to mimic the style, tone, and language patterns of a particular person. This could include generating social media posts, emails, or other forms of written communication that are designed to sound like they were written by a verified source.
- AI systems can be used to generate images or videos that are designed to look like a particular person.
- AI systems can be used to manipulate online profiles or accounts to make them appear more like the person being impersonated, including changing profile information or generating fake activitiy on social media or other online platforms.

The use of AI to impersonate a real person can be a highly sophisticated and effective form of deception, and it is important for individuals and organizations to be aware of the potential for this type of activity and to take steps to protect themselves from it.

There are a few ways you can tell the difference between writing produced by a person and writing produced by AI. Here are a few things to consider:

- Style and tone: AI-generated writing may lack the subtle nuances and variations in style and tone that are characteristic of human writing. It may also contain repetitive or formulaic language.
- Grammar and syntax: AI-generated writing may contain errors in grammar and syntax that are less common in human writing.
- Cohesion and organization: AI-generated writing may be less cohesive and less well-organized than writing produced by a person. It may lack transitions or logical connections between ideas.
- Context and content: AI-generated writing may be less contextually relevant or may contain content that is unrelated to the topic at hand.

It is important to note that the capabilities of AI in generating human-like writing have improved significantly in recent years, and it is becoming increasingly difficult to distinguish between writing produced by AI and writing produced by a person. In some cases, it may be necessary to use multiple methods or to consult with experts in order to determine the source of a given piece of writing.

There are a number of steps that individuals and organizations can take to prevent AI-assisted fraud. Some recommendations include:

- Implement strong security measures, such as using unique passwords for all accounts, enabling two-factor authentication, and keeping all software and security protocols up to date.
- Be cautious about sharing personal information. Be selective about the personal information you share online and be cautious about responding to requests for personal information from unknown sources.
- Verify the authenticity of information and communications. Be skeptical of information and communications that seem suspicious or too good to be true and take steps to verify their authenticity before acting on them.
- Educate yourself about the common signs of fraudulent activity, such as unsolicited requests for personal information or offers that seem too good to be true.
- Report suspicious activity. If you suspect that you are the target of fraudulent activity, or if you come across suspicious information or communications, report it to the appropriate authorities or organizations.

By following these recommendations, you can help protect yourself and your organization from AI-assisted fraud and other forms of cybercrime.

ACFE Training Director, Jason Zirke, CFE, used AI to write the following anti-fraud poem:

A deceitful act, a moral waste

Lies and tricks for personal gain

Leaving others in financial pain

From identity theft to Ponzi schemes

Fraud takes on many different means

It preys on those who trust and believe

Leaving them hurt with no relief

It lurks in shadows, waiting to pounce

It preys on those who don't keep an ounce

Of skepticism, or trust too much

Falling victim to its wicked touch

But fear not, for justice will prevail

The guilty will be sent to jail

They'll pay for their crimes, that much is true

Fraudsters can't escape their due

So, report the fraud and don't be shy

Seek help, don't let the fraudster by

Stand up and fight, don't let them win

Together we can stop this sin

Video of the Month

How scammers can use 'deep voice' AI technology to trick you | About That - YouTube

CBC News: Scammers are using artificial intelligence to create audio recordings that imitate a real voice. Andrew explores how the technology works and investigates how scammers have already used it to steal millions of dollars.

How a 30-year-old fintech founder fooled JPMorgan Chase

January 16, 2023
https://finshots.in/archive/how-jp-morgan-got-scammed/

The Story
Step 1: Scream from the rooftops that the American college system is broken! That students graduate with $30,000 in student loans.

Step 2: Start a fintech business to fix this problem. Target Gen-Z college students and help them fill out arduous forms to get scholarships and financial aid.

Step 3: Get on the celebrated Forbes 30 Under 30 list for fighting for a worthwhile cause. People will notice you now.

Step 4: Attract the attention of a bank that'd love to get its hands on your user list. After all, your college-going user list is the perfect future customer for a bank. Catch 'em when they're young.

Step 5: Finally, and this is the most important step of them all—If you don't have the 4.25 million users to ask for a $175 million buyout, just fake the customer data!!! Yup, do whatever it takes to fool the bank into believing that the startup was a phenomenal success. And keep your fingers crossed.

Or as the tech bros say, "Fake it till you make it."

That's what Charlie Javice, the founder of fintech startup Frank, did. Or at least that's what JPMorgan Chase, the bank that paid $175 million to buy the startup is now alleging. It's saying that it got scammed by Javice.

Now you're probably wondering—how on earth did a massive bank like JPMC miss the red flags before coughing up all that money? Who did all the due diligence to check if Javice's claims were airtight?

Well, let's just say that Javice outplayed the banking giant. And made a mockery of its due diligence process.

Before we get into how she did that, we first need to see how JPMC finally realized that it may have been duped.

In January 2022, after the acquisition was done and dusted, the bank decided to spam Frank's users with a campaign. Probably to get them to buy some financial product that would make the bank some money. So it randomly picked 400,000 users from the list Frank provided it during the due diligence process and sent out emails.

But…the campaign went horribly wrong.

You see, only 28% of emails were delivered. And JPMC usually has a high a 99% delivery rate for its campaigns. And even worse—only 1.1% of the delivered emails were opened. Compared to 30% for a typical JPMC campaign.

That's when JPMC smelt something suspicious. It launched an investigation. It managed to get a hold of all of Charlie Javice's old emails. And voila, the sham emerged in all its glory.

See, Frank did not have the 4 million customers that it claimed. It only had a measly 300,000. But you don't get $175 million for that, right?

So what did Javice do?

Apparently, Javice first sent her Director of Engineering an email with a link to an article titled "Generating Tabular Synthetic Data Using GANs." The article notes that "[t]he goal is to generate synthetic data that is similar to the actual data in terms of statistics and demographics."

Basically, she wanted to artificially inflate the user base with fake data!

The Director wasn't impressed. He asked if it was even legal to do this. Now you can imagine that Javice's response would've been in the affirmative. She even said that it was standard practice during investments and that no one would end up in an 'orange jumpsuit' (meaning prison time) over this.

Okay.

But the Director was having none of this. He refused to play along (clap, clap) and sent a list of only the real users—just 293,000 of them.

Oh yeah, not even 10% of what Frank claimed to have.

But Javice couldn't send this to JPMC, no? She wanted the $175 million. So, she took external help.

Her colleague and Chief Growth Officer Olivier Amar jumped in. He reached out to a company called ASL Marketing, Inc. A firm that claimed to have "the most comprehensive, accurate and responsive data of high school students, college students and young adults available anywhere." It could give Frank exactly what it needed!

So Amar paid ASL $105,000. And bought a list of 4.5 million students.

He then tapped another company called Enformion for the email addresses of students who were part of ASL's list. And paid them $70,000 for their troubles.

Meanwhile, Javice was cooking up something too. She'd found a "Data Science Professor." A teacher at a college in New York City. And wanted his help to create fake lists.

And that's when it becomes really scandalous!

So, Javice asked the Professor to generate addresses for the fake students. And the Data Science Professor emailed Javice asking, “I can’t seem to find addresses in my raw files . . . Should I attempt to fabricate them?”

Javice responded saying, “I just wouldn’t want the street to not exist in the state.” Basically, the addresses could be fake. But she didn’t want a non-existent XYZ street name to pop up. It had to be real.

But the Professor replied that “‘real addresses’ may not be doable.”

So Javice had a brainwave. She figured out that, “[I]f we can’t do real addresses whats the best we can do for that? Worse comes to wors[t] we can try a unique ID.”

Basically, she fooled JPMorgan by convincing them that the Unique ID in the list was to protect the confidentiality of the student users. That the Unique ID was tied to real addresses in the back end. And the bank believed her.

Then came the email IDs. And this is even juicier.

Here’s an excerpt from JPMC’s complaint.

In an email at 12:56 p.m., the Data Science Professor, referring to the template Javice sent an hour earlier, asked Javice: “You have the student email marked as ‘provided as unique ID’ but didn’t we agree to make fake ones a la ‘asdugnsdf@gmail.com’? Or do you want unique ID after all?”

In a response sent six minutes later at 1:02 p.m., Javice asked, “will the fake emails look real with an eye check or better to use unique ID?”

At 1:37 p.m., the Data Science Professor confirmed “[t]hey will look fake. So let’s use unique ID.”

So yeah, the Unique IDs emerged again. All under the veil of ‘privacy.’

It all seemed so genuine. So when JPMC did the due diligence, it passed with flying colours.

And finally, there’s the scam invoicing bit after the deed was done.

When the Professor sent Javice a bill of $13,300 for the work done, he was quite elaborate. He described that he’d performed “college major generation” that included creating “first names, last names, emails, phone numbers”.

Quite an honest man!

But Javice freaked out. A sharp auditor would definitely ask questions about this.

So she asked him to remove it all. And simply send a one-line invoice saying “for data analysis.” She even sent him a bonus of $4,700. Probably to keep his mouth shut.

And the Professor's response was: "Wow. Thank you. Here is the new invoice." Yeah, the fraud didn't really matter anymore.

But Javice sweetened the deal further. She even offered the Professor a full-time position at JPMC after the buyout. Now hiring the man into the same bank he helped defraud is quite the killer move!

It all sounds crazy to be true.

But that folks is how a Forbes 30 Under 30 winner fooled one of America's largest banks.

To sum it up—Frank paid a total of $193,000 to ASL, Enformion, and the Professor for a list of 'fake' email addresses. And then sold that list to JPMorgan for a whopping $175 million.

Definitely a contender for the scam of the year, don't you think?

Until then…

PS: Charlie Javice has filed a suit against JPMorgan Chase too alleging that she hasn't been paid her due and that the bank's plan to monetise the student data by bombarding them with emails about credit cards and loans was a poor business plan. So make of this what you will.

Earth Day Word Search Challenge

AIR
ANIMALS
APRIL
AWARENESS
CHANGE
CLEAN
CLIMATE
COMPASSION
CONSERVATION
CONTINENT
DEFORESTATION
DESERT
EARTH DAY
ECOLOGY
ENDANGERED
ENERGY
ENVIRONMENT
EROSION
EXTINCT
FACTORY
FUTURE
GARBAGE
GLOBAL WARMING
GROWTH
HARMONY
HEMISPHERE
INDUSTRY
LAKE
LITTER
MOUNTAIN
NATURAL RESOURCES
NUCLEAR
OCEAN
OZONE
PEACE
PLANET
PLANTS
POLAR REGION
POLLUTION
POND
POWER PLANT
PRESERVE
PROTECT
RAINBOW
RAINFOREST
RECYCLE
REDUCE
REFORESTATION
RENEWABLE
REUSE
RIVER
SAFE
SKY
SOIL
SUSTAINABLE
TREES
VALLEY
WASTE
WATER
WEATHER
WETLANDS
WILDERNESS
WILDLIFE
WORLD

Why Behavioral Biometrics Is the Next Big Weapon to Fight Fraud

February 10, 2023
Carthic Kameshwaran
https://www.acfeinsights.com/acfe-insights/2023/2/9/why-behavioral-biometrics-is-the-next-big-weapon-to-fight-fraudnbsp

Behavioral biometrics is a modern method of identifying individuals based on the way they interact with devices, such as computers and smartphones. It is used to verify the identity of an individual through the analysis of patterns of human behavior, such as mouse movements, typing speed and pressure on touchscreens. Unlike traditional biometric methods, such as fingerprint scanning or face recognition, behavioral biometrics does not require any physical input from the user, making it a more convenient and less intrusive form of identification.

Adoption in Fraud Prevention
Behavioral biometrics is a relatively new technology, but it has already been widely adopted by organizations and individuals for a range of purposes. One of the most common applications of behavioral biometrics is in the field of cybersecurity, where it is used to detect and prevent fraudulent activities. For example, it can be used to detect unauthorized access attempts by monitoring the way a user interacts with a device and comparing it to previous behavior patterns. If the behavior does not match what is expected, the system can flag the activity as suspicious and take appropriate measures to prevent it.

Another application is in the field of mobile banking, where it is used to enhance the security of online transactions. By monitoring the way a user interacts with their device, the bank can verify the identity of the user and ensure that they are indeed the person who is making the transaction. This reduces the risk of fraud and helps to protect the customer's sensitive information.

Adoption in Operational Efficiency
In addition to its applications in cybersecurity and mobile banking, behavioral biometrics is also being used in the workplace to increase productivity and efficiency. For example, it can be used to monitor the performance of employees and identify areas where they need improvement. By tracking the way an employee interacts with their device, the system can detect patterns of behavior that are associated with low productivity, such as taking frequent breaks or spending too much time on non-work-related activities. This information can then be used to provide targeted training and support, helping to improve overall productivity and efficiency.

Another benefit of behavioral biometrics is its ability to improve the user experience. By tracking the way an individual interacts with a device, the system can learn their behavior patterns and preferences, making it easier for the user to complete tasks and access information. This can help to reduce frustration and improve the overall user experience.

Challenges
Despite the many benefits of behavioral biometrics, there are also some potential risks and challenges that must be considered. One of the main concerns is privacy, as the technology involves collecting and analyzing sensitive information about an individual's behavior patterns. This information could potentially be used for malicious purposes, such as identity theft or profiling.

Another challenge is the accuracy of behavioral biometrics. While the technology has made significant advancements in recent years, there is still a risk of false negatives or false positives. For example, a change in behavior, such as an injury or illness, could result in a false negative, preventing the individual from accessing their device or account. On the other hand, a false positive could result in the system mistakenly identifying a malicious user as the legitimate one.

Finally, there is the issue of cost, as implementing a behavioral biometrics system can be expensive. This includes the cost of purchasing and deploying the necessary hardware and software, as well as the cost of training staff and providing support to users.

Final Notes
In conclusion, behavioral biometrics is a promising technology with many potential applications and benefits. However, it is important to consider the potential risks and challenges before adopting the technology, including privacy, accuracy and cost. By carefully balancing the benefits and risks, organizations and individuals can make informed decisions about the use of behavioral biometrics and ensure that they are using the technology in an appropriate manner.

Quote of the Month

"AI systems with human-competitive intelligence can pose profound risks to society and humanity, as shown by extensive research[1] and acknowledged by top AI labs.[2] As stated in the widely-endorsed Asilomar AI Principles, Advanced AI could represent a profound change in the history of life on Earth, and should be planned for and managed with commensurate care and resources. Unfortunately, this level of planning and management is not happening, even though recent months have seen AI labs locked in an out-of-control race to develop and deploy ever more powerful digital minds that no one – not even their creators – can understand, predict, or reliably control."

— Open Letter: Pause Giant AI Experiments: An Open Letter - Future of Life Institute
Signed by more than 50,000, including: Yoshua Bengio, Stuart Russell, Elon Musk, Steve Wozniak, Yuval Noah Harari, Eman Mostaque, Andrew Yang, and John J Hopfield.