FUTURE OF

FINANCIAL FRAUD INVESTIGATIONS:

AI FOR AI

Nationwide Fraud Losses Topped $10 billion in 2023. It's Time We Step Up!

TABLE OF CONTENT

FOREWORD

Federal Trade Commission reports that consumers lost more than $10 billion to financial frauds in 2023, reaching a never-touched-before benchmark. Most money was lost to investment scams, followed by imposter scams. [1]

Much of this unprecedented surge in financial fraud cases can be attributed to technologies like Generative AI.

As the U.S. Department of Treasury rightly warned, *"Generative AI can help existing threat actors ... giving them complex attack capabilities* ***previously available only to the most well-resourced actors.***" [2]

However, the good news amongst all these unpleasant facts is that government and investigative agencies are not falling behind in using AI to counterattack.

- In a significant win, the U.S. Department of Treasury announced a recovery of $375 million after implementing an AI-based process in 2023 to mitigate check fraud, which had increased by 385% since the pandemic. [3]

- The Internal Revenue Service also invested $400 million in creating the Return Review Program (RRP), which uses artificial intelligence to detect potential fraud in refund-seeking tax returns. The program assesses fraud risks and directs suspicious cases to investigators for a thorough examination. [4]

The Federal Trade Commission launched the Voice Cloning Challenge in November 2023 to "promote the development of ideas to protect consumers from the misuse of artificial intelligence-enabled voice cloning for fraud and other harms." [5]

CHAPTER 1

USE OF AI FOR NEFARIOUS PURPOSES

It has become easier than ever for threat actors to commit financial fraud. With the advent of AI and Gen AI, they can effortlessly generate highly personalized phishing messages and create deep fake content that can deceive even the most vigilant individuals.

To make it worse, this fake content looks so real that it has ushered in a new level of complexity in financial fraud, making detection increasingly difficult. Federal Trade Commission Chair Lina Khan confirmed, *"We are seeing risks that **AI could be used to turbocharge fraud and scams.**"*

1.1 Synthetic Identity Fraud

The FBI has identified Synthetic Identity Fraud as one of the fastest-growing crimes across the USA.[6] Moreover, Deduce reveals a startling 10% surge in Super Synthetic Identities within the final quarter of 2023 alone.[7]

These AI-enhanced Super Synthetic Identities blur the lines between fiction and reality. They merge real and fabricated Personal Identifiable Information (PII) with algorithmically generated, human-like online behaviors that convincingly suggest a physical presence. They include realistic-looking documents, biometric details, fake activities, and histories, presenting a new challenge for fraud prevention systems.

1.2 Spear Phishing

A November 2023 SlashNext report unveils a shocking 1265% spike in phishing emails and a 967% increase in credential phishing within just one year.[8] Additionally, Quishing–QR code-based phishing, is another phishing scam proliferating in the USA.[9]

This surge is unsurprising as criminals have transitioned from a spray-and-pray approach to highly sophisticated, targeted attacks.

At the core of this transformation are advanced LLMs (large language models) like FraudGPT, designed explicitly to facilitate financial fraud. FraudGPT was introduced as an unrestricted counterpart to ChatGPT, and it's available for a few hundred dollars on the dark web.

Generative AI technologies, particularly with tools like FraudGPT, have significantly blurred the line between real and fake. Where unusual fonts and grammatical errors once signaled scams, generative AI has largely removed these red flags. This technology enables scammers to create highly personalized and error-free messages, contributing to a surge in scams.

And the scams have gone far beyond the phishing emails. Scammers can now accurately impersonate individuals, utilizing their voices for fake phone calls or their images for deceptive video calls.

1.3 Ponzi Schemes and Investment Scams

In 2023, consumers experienced substantial financial losses to investment scams, with more than $4.6 billion lost, making it the most costly category of fraud reported. [10]

Recent federal agency crackdowns on many organizations perpetrating such scams include a lawsuit against investment advice company WealthPress. The company was asked to refund more than $1.2 million to consumers who were deceived and pay a $500,000 civil penalty for outlandish and false scams. [11]

Unfortunately, AI is only exacerbating these scams by assisting criminals in crafting convincing phishing emails, texts, and calls for all the stages of the Investment Scams Life Cycle:

1. **Lurking** – gathering information about potential victims
2. **Alluring** – providing short-term profits to gain victims' trust
3. **Catching** – convincing the victim to join the fake investment opportunity
4. **Executing** – deceiving a victim into investing through an unfamiliar software
5. **Vanishing** – closing the interaction when the victim wants to withdraw their funds

AI also aids in other vital processes, such as developing fraudulent investment software that disappears without any trace. [12]

1.4 Voice Spoofing

In a study conducted by McAfee in May 2023, 25% of respondents said they had experienced an AI voice cloning scam or knew someone who had. 70% of them said they could not differentiate between a clone and a real voice.[13]

The case of Jennifer DeStefano in April 2023 exemplifies the terrifying potential of voice cloning. She received a distressing call from what she believed was her kidnapped daughter, pleading for help and a $50,000 ransom for her release. This call, however, was not from her daughter, who was safe on a ski trip, but from criminals who had expertly cloned her voice.[14]

This fraud technique preys on the innate panic and desperation that ensue when a person believes their loved one is in danger. The natural human instinct is to act swiftly, which criminals exploit, leveraging AI to create emotionally manipulative and convincing scenarios.

According to Chinese tech giant Baidu, it took merely 3.7 seconds of audio to clone a voice in 2019. With the speed at which technology is advancing, the time could have only decreased.[15]

1.5 Deepfake Videos

The November 2023 Identity Fraud Report by Sumsub delivered an alarming revelation: a tenfold increase in deepfakes globally from 2022 to 2023, with an exponential **1440% surge in North America alone.**[16]

At the core of this technology lies the seamless merging of images and videos facilitated by AI algorithms. What once required extensive data inputs has now been simplified to using few images, leading to the creation of compelling deepfake videos.

In one particular instance that made headlines recently, an employee at a Hong Kong-based multinational corporation fell victim to a deepfake scam that led to a $25 million loss. During a video conferencing call, the criminal used a deepfake video of the company's CFO to deceive the employee into authorizing the fraudulent transaction.[17]

The availability and accessibility of resources amplify this threat, with a simple online search directing to hundreds of tutorials on creating a deepfake video.

Criminals are exploiting AI to orchestrate financial fraud at a larger scale and much faster than ever. To stay ahead in the game, investigators must also adopt these advanced tools.

CHAPTER 2

USE OF AI FOR DETECTION AND PREVENTION

AI thrives on data. And the amount of data available in electronic records, emails, contacts, text messages, bank transfers, etc., makes AI and ML very well-suited for financial fraud detection. Here is how:

2.1 Asset Tracing, Recovery, Restitution and Management

Existing technology already presented challenges in asset tracing. By leveraging AI, criminals can easily forge more intricate synthetic identities and obscure their financial trails. If criminals are using AI to obscure the money trail, investigators cannot discover it manually.

Here is how AI algorithms can help investigators track and recover these illicit assets using:

- **Pattern Recognition:** Detection of suspicious patterns in transactional data to flag potential fraud.
- **Network Analysis:** Mapping complex financial networks to reveal hidden connections and trace illicit funds.
- **Predictive Analysis:** Forecasting future asset-hiding attempts based on historical data to aid in asset recovery.
- **Natural Language Processing (NLP):** Extracting vital information from unstructured data for financial investigations.
- **Deep Learning Modeling:** Recognizing intricate patterns across various data types, aiding in accurate predictions and image reconstruction.

Apart from tracking and recovery, AI can also take care of the restitution and management of these funds:

- **Validation and Liquidation:** Optimizing asset valuation and sale timing for maximum returns.
- **Transparent Decision-making:** Enhancing the transparency in asset retribution decisions, promoting accountability.
- **Efficiency in Restitution:** Accelerating asset-victim matching for swift compensation.
- **Regulatory Compliance:** Ensuring unbiased asset management and adapting practices with evolving legal standards.

2.2 Preventing Spear Phishing and Quishing

ML algorithms must be trained on a large dataset of real and phishing emails to understand malicious patterns. There are three main methods for this:

- **Social Graph Analysis:** Creating a map of normal communication patterns among employees helps identify unusual connections, like rare interactions between departments that could indicate suspicious activity.
- **Employee Communication Profiling:** Everyone has a unique writing style and habits. Natural Language Processing (NLP) can analyze these patterns, such as specific phrases, formatting choices, or sentence structures to identify who sent an email.
- **Email Structure Analysis:** ML can examine technical details of emails, like IP addresses and header information; it can flag emails with mismatched or suspicious data, such as emails claiming to be from one source but showing signs of being spoofed or modified.

To prevent Quishing, AI algorithms can be utilized to discern if the URL in the QR code is safe, before redirecting the user to the destination website.[18]

2.3 Saving Public from Ponzi Schemes and Investment Scams

Turn the table on fraudsters. While scammers utilize psychological tactics to deceive their targets, AI can level the playing field by analyzing the emotional cues within scam communications.

ML algorithms can be trained to recognize specific patterns and features expected in fraud schemes. Algorithms can identify fluctuations in scammers' emotional patterns, sentiments, and feelings, aiding in early detection and flagging of Ponzi schemes and other investment scams, effectively thwarting their efforts.

2.4 Identifying Voice for Being Fake or Genuine

AI can differentiate between real and fake voices and analyze complex audio patterns that are indiscernible to the human ear. This is how it works step-by-step:

- **Feature Extraction:** The AI algorithms analyze the voice recording and extract features like tone, pitch, speed, and other unique characteristics of the sound waves.
- **Acoustic Modeling:** It captures the acoustic environment of the recording, like background noise, echo and reverberation, which helps indicate whether it is recorded in a natural setting or artificially manipulated.
- **Machine Learning Models:** The extracted features are fed into already trained ML models, which helps to tell the subtle differences between genuine human voices and those that are synthesized or altered.
- **Classification:** Once the above processes are completed, the AI classifies the voice as either real or fake based on the likelihoods calculated by the model.

While AI excels in detecting and protecting fraudulent activities through advanced algorithms and data analysis, its utilization in legal proceedings has sparked some debates. Let's explore the consequences in the next chapter. [19]

CHAPTER 3

USE OF AI IN LEGAL PROCEEDINGS

When ChatGPT was launched in November 2022, almost everyone tried it out. Many have sought comfort in utilizing these now omnipresent chatbots (the likes of ChatGPT) to assist with everyday tasks.

Even lawyers couldn't resist. There was an upsurge in the use of AI-based evidence and citations in the court. However, many were not admissible for legitimate reasons, as mentioned below:

- In June 2023, sanctions were imposed on two New York lawyers for submitting a legal brief containing six fictitious case citations generated by ChatGPT. [20]
- In another case of December 2023, it was found that Donald Trump's ex-lawyer mistakenly gave fake case citations generated by Google Bard to his attorney for an official court filing. [21]
- In a significant move, the 5th US Circuit Court of Appeals proposed a rule requiring lawyers to guarantee that they did not rely on artificial intelligence to draft court briefs.

However, in what is being considered as the most significant discussion on the influence of AI on law, the US Supreme Court Chief Justice John Roberts said in a year-end report that "any use of AI requires caution and humility." He talked about how "AI is based largely on existing information, which can inform but not make decisions" and that "machines cannot fully replace key actors in court." [22]

While much uncertainty persists around the use of AI in financial fraud investigation, the future seems bright as the technology advances and professionals learn its proper use. As rightly noted by The Association of Certified Fraud Examiners, "New tools might be developed, with sufficient safeguards in place, that end up in the fraud-fighting toolkit." [23]

CHAPTER 4

IMPACT OF AI ON THE ROLE OF FINANCIAL FRAUD INVESTIGATORS

AI is not here to replace financial fraud investigators. President Biden's Executive Order clarified that AI aims to improve efficiency and simplify the fraud investigation process, not job displacement. [24]

However, with the growing technology, as more and more crimes become AI-assisted, those who do not realize AI's full potential and use it to complement their expertise will be replaced.

Here's how AI can assist investigators to ditch the cumbersome tasks and focus on more meaningful aspects of financial fraud investigations:

4.1 Entity Link Analysis

AI significantly transforms the process of entity link analysis in financial investigations by enhancing speed, accuracy, and comprehensiveness.

AI can automatically integrate and analyze data from diverse sources such as bank records, transaction logs, and public databases. AI can detect subtle relationships and irregularities across accounts and transactions that are characteristic of money laundering or other types of financial fraud. Moreover, AI can be instrumental in presenting these relationships through compelling visualizations.

4.2 Forensic Accounting

Forensic Accountants use AI to detect complex patterns of financial fraud and anomaly detection much faster than traditional methods. Its three compelling use cases are:

- **Structuring and Smurfing:** Criminals break down large transaction amounts into smaller amounts to avoid suspicion. This makes them much more difficult to flag and trace as they do not get automatically triggered. AI can be deployed to analyze unusual activities based on data points like transaction values and initiation locations.
- **Layering:** To make tracing challenging, money is shifted between banks, different bank accounts, and countries. AI models can be trained to detect such layering attempts and recognize money laundering patterns.
- **Integration:** Investigators can use AI to detect integration attempts to combine illicit funds with legitimate assets to conceal their origin through transaction monitoring, screening, and risk scoring.

AI is just a broader component of the investigative toolkit, not a panacea or solution in itself. It does not replace the need for human intuition, reasoning, and contextual understanding. However, investigators need to upskill themselves to use AI correctly.

CHAPTER 5

THE AI SKILL GAP WHY INVESTIGATORS NEED TO STEP UP

In order to make the most of AI's capabilities, investigators need to learn data analysis and interpretation skills. Here is why:

- **Understanding AI Outputs:** The outputs generated by AI models can be complex. Hence, investigators must interpret the output accurately to discern between the genuine fraudulent activity and the false positives.

- **Critically Evaluating AI Models:** Investigators must constantly evaluate the validity of the AI models' assumptions, the data's relevance, and the algorithms' appropriateness. This ensures that the AI's findings are reliable and applicable to real-world scenarios.

- **Data Preparation:** Data must be cleaned, organized, and transformed before AI is employed. Investigators must make critical decisions about which data to retain or remove and how to present it effectively for analysis. Grasping the subtle details of the data ensures that AI models are trained on relevant and high-quality datasets, which fosters more precise results.

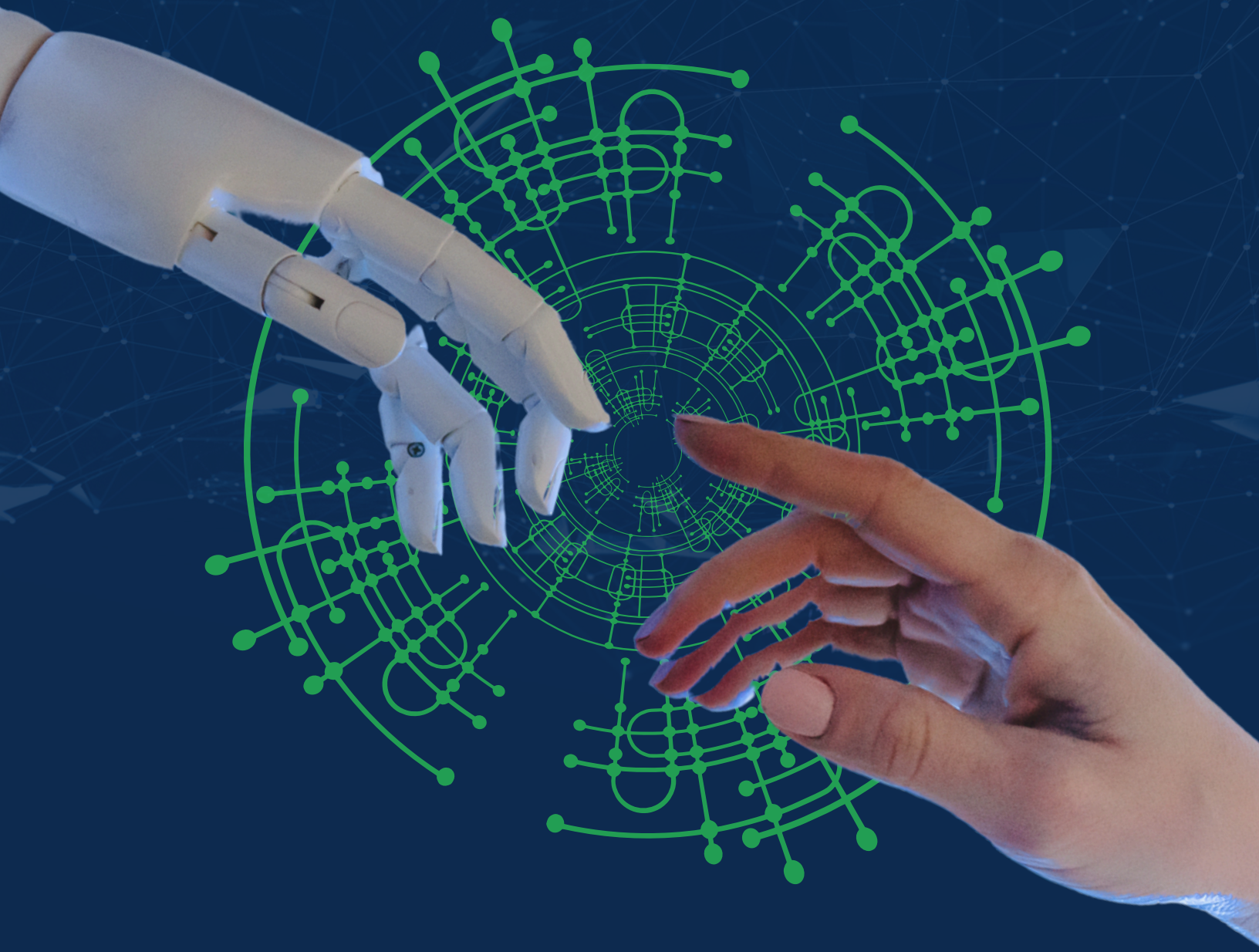
- **Ethical Considerations:** Conducting data analysis requires adherence to ethical and legal standards, particularly in privacy and data protection areas. Investigators need to be aware of the ethical limits within which AI can be used to scrutinize financial data. AI algorithms might inherently introduce biases, leading to inaccurate profiling and unfair targeting. Investigators must understand the boundaries within which AI can ethically analyze financial data. These biases include:

  - **Sampling Bias:** Unequal representation of data samples leading to skewed conclusions
  - **Selection Bias:** Cherry-picking data or cases, distorting the accuracy of findings
  - **Labeling Bias:** Subjective or prejudiced collection of data, affecting analysis outcome
  - **Cultural Bias:** Incorporating cultural stereotypes or preferences into AI systems, impacting decisions
  - **Data Collection Bias:** Systematic errors during data gathering, compromising the integrity of results
  - **Algorithmic Bias:** Discriminatory outcomes due to flawed algorithms or biased training data
  - **Temporal Bias:** Inaccurate conclusions due to outdated or insufficiently recent data

While there are various ways to develop the required skills, the next chapter provides some actionable advice on the subject.

CHAPTER 6

ACTIONABLE WAYS TO STAY UPDATED ON AI



Change is the only constant in this world. Those who adapt to the changes do far better than those who don't.

With that in mind, below is a list of training programs, podcasts, influencers, and custom GPTs to follow so you can stay updated on how AI is transforming the financial fraud investigation landscape.

6.1 Training Programs to Attend in 2024

AI significantly transforms the process of entity link analysis in financial investigations by enhancing speed, accuracy, and comprehensiveness.

1 Conference on Artificial Intelligence and Financial Stability

Organized by the Financial Stability Oversight Council (FSOC) and the Brookings Institution, the two-day conference is an opportunity for the public and private sectors to convene and explore the innovation and risks of AI in financial services. [25]

Date: **June 6-7, 2024**
Venue: **The U.S. Department of The Treasury and the Brookings Institution, Washington DC**

2 35th Annual ACFE Global Fraud Conference

The 35th edition of the Global Fraud Conference, organized by the Association of Certified Fraud Examiners, will feature industry experts from various fields as speakers for more than 90 education sessions on the latest anti-fraud techniques, tools, and discoveries. [26]

Date: **June 23-28, 2024**
Venue: **Las Vegas + Virtual**

3 2024 ACFE Anti-Fraud Leadership Summit

An exclusive one-day event on preparing for emerging anti-fraud trends and technologies, using analytics tools in anti-fraud initiatives. The best practices for anti-fraud and anti-corruption programs, and much more. [27]

Date: **September 23, 2024**
Venue: **New York**

4 **2024 ACFE Government Anti-Fraud Summit**
Hosted by the ACFE Law Enforcement and Government Alliance, the event will deliver the latest insights, techniques, and tools to address anti-fraud challenges specific to law enforcement and government agencies. [28]

Date: **November 14, 2024**
Venue: **Washington DC + Virtual**

5 **5th ACM International Conference on AI in Finance**
A scholarly peer-reviewed conference, it aims to bring together researchers from academia and industry to discuss challenges, advances and insights on the impact of AI and ML on finance. [29]

Date: **November, 14-16, 2024**
Venue: **New York University's Tandon School of Engineering**

6.2 Podcasts to Follow

1 **Fraudology**
Hosted by Karisse Hendrick, an award-winning cyber fraud expert and an ecommerce fraud prevention consultant, Fraudology deals with the "science and study of fraud." The guests range from former cybercriminals to law enforcement employees, discussing different types of financial scams from the perspective of a fraud fighter. [30]

2 **The Brett Johnson Show**
In his podcast on YouTube, Brett Johnson, former US most-wanted cybercriminal, discusses cybercrime, scams, fraud, and security and advises people on how to protect themselves from the kind of person he used to be. [31]

3 **Fraud Talk**
The Association of Certified Fraud Examiners' monthly podcast details different case studies of financial fraud and features anti-fraud experts who offer tools and suggestions for fighting it. [32]

4 **Anatomy of a Scam**
Hosted by Deborah Knight and Trevor Long, Anatomy of a Scam features cyber security and law enforcement experts who discuss the "epidemic of scams" and the necessary steps to counter them in the new era of artificial intelligence. [33]

5 **What the Fraud?**
A biweekly podcast started by Sumsub, an identity verification service, explores critical fraud issues like deep fakes, identity theft, account takeovers, etc., with industry experts from the world of artificial intelligence. [34]

6.3 LinkedIn Influencers to Follow

1 Frank McKenna

With over 30 years of experience in the fraud industry, Frank McKenna has designed various analytical products and tools that help customers reduce fraud losses and has co-authored multiple patents on fraud detection systems and methods.

A thought leader and industry expert, his LinkedIn posts are widely read. He also publishes a blog called FrankonFraud.com, which addresses leading issues of fraud in the industry and best practices for combating fraudsters.[35]

2 Brian Krebs

Former reporter at The Washington Post Brian Krebs writes stories on internet security, computer security, and cybercrime on his website KrebsOnSecurity.com.

With a following of 150,000+ on LinkedIn, he posts regularly on issues of artificial intelligence-enabled financial crime, such as phishing emails, messages, deep fakes, etc.[36]

3 Tony Sales

As the Chief Product Officer at We Fight Fraud, a collaboration between financial crime and fraud prevention specialists, he provides insights to combat fraud and financial crime in areas such as ID, credit card, bank, internet, data theft, hacking, cyber security, and physical security.

A former fraudster himself, he is called "The Social Engineering Expert" and deeply understands the psychology, techniques, and tactics of social engineering.[37]

6.4 Twitter Influencers to Follow

1 Adam Levin

An expert in cyber security, privacy, identity theft, fraud, and personal finance, Adam Levin has distinguished himself as a fierce consumer advocate for the past 40 years. He aims to educate consumers, businesses, law enforcement officials, and lawmakers on identity management and protection, privacy, credit, and election security issues.

He has appeared on several renowned TV and radio shows, including The Today Show, Good Morning America, CBS Evening News, ABC News Radio, and Bloomberg Radio. [38]

2 Shira Rubinoff

A recognized cybersecurity executive, blockchain advisor, global keynote speaker, and influencer, Shira has built two cybersecurity product companies.

She is active on all social media channels, including Twitter, LinkedIn, and YouTube, and often discusses AI in cybersecurity.[39]

3 Mikko

With over three decades of cybersecurity experience, Mikko has built labs, products, and research functions and has worked on countless investigations.

He often speaks on well-known forums about AI, financial fraud, and cybersecurity and boasts a Twitter following of 230k+. [40]

6.5 Custom GPTs

1. **Forensic Ledger Investigator**
   An AI forensic accountant, it is adept at unraveling complex financial puzzles, fraud detection, and financial disputes.[41]

2. **Financial Ledger Sleuth GPT**
   Specializes in uncovering financial discrepancies, fraud detection, and data analysis.[42]

These resources will not only keep you updated about the latest developments in AI in financial fraud investigations but also assist you in carrying out your own investigations using AI.

While these resources just show the picture, the real action can be seen in AI-powered fraud investigation tools. One such powerful tool, ScanWriter, is ready to unleash its AI capabilities. For the past decade, it has been empowering government agencies with its actionable data insights to maximize their efficiency and deepen their investigative research.

CHAPTER 7

SCANWRITER – YOUR RELIABLE AI ASSISTANT IN FINANCIAL FRAUD INVESTIGATIONS

ScanWriter Standard AI Edition provides a comprehensive plan for leveraging AI technologies to revolutionize financial investigations within federal government agencies. The software aims to enhance the efficiency, accuracy, and effectiveness of financial investigations for improved outcomes, reduced resource requirements, and enhanced regulatory compliance.

ScanWriter Standard AI Edition provides investigators with multiple benefits:

- **The AI-Enabled Data Analytics Platform** incorporates advanced ML algorithms to analyze large volumes of structured and unstructured financial data, such as transaction records, emails, and social media data.
- **Pattern Recognition and Anomaly Detection** enables automatic identification of suspicious transactions, unusual behavior, and potential fraud.
- **Predictive Analysis** leverages historical data to forecast potential financial crimes, anticipate emerging trends, and prioritize investigations.
- **Natural Language Processing** for Document Processing extracts relevant information faster, facilitating information retrieval, entity extraction, and relationship mapping.
- **Collaboration and Knowledge Sharing** facilitate real-time information exchange, case management, and collective intelligence.
- **Ethical and Transparent AI** ensures that the AI algorithms and models adhere to ethical guidelines and maintain transparency.

Ready to explore the possibilities with ScanWriter? Contact us at alicia@personable.com to learn more and start a 14-day free pilot program designed exclusively for investigators in the public sector.

REFERENCES

1. https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public
2. https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf
3. https://home.treasury.gov/news/press-releases/jy2134
4. https://www.brookings.edu/articles/using-ai-and-machine-learning-to-reduce-government-fraud/
5. https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-announces-exploratory-challenge-prevent-harms-ai-enabled-voice-cloning
6. https://www.acamstoday.org/
7. https://www.deduce.com/resource/supersynthetic-identity-index/
8. https://www.cnbc.com/2023/11/28/ai-like-chatgpt-is-creating-huge-increase-in-malicious-phishing-email.html
9. https://www.fbi.gov/contact-us/field-offices/elpaso/news/fbi-tech-tuesday-building-a-digital-defense-against-qr-code-scams
10. https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public
11. https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-suit-requires-investment-advice-company-wealthpress-pay-17-million-deceiving-consumers
12. https://www.tandfonline.com/doi/abs/10.1080/01639625.2023.2244115
13. https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/

14 https://www.theguardian.com/us-news/2023/jun/14/ai-kidnapping-scam-senate-hearing-jennifer-destefano

15 https://www.forbes.com/sites/bernardmarr/2019/05/06/artificial-intelligence-can-now-copy-your-voice-what-does-that-mean-for-humans/?sh=4a7eec9272a2

16 https://www.prnewswire.com/news-releases/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023-301998891.html

17 https://economictimes.indiatimes.com/industry/tech/hong-kong-mnc-suffers-25-6-million-loss-in-deepfake-scam/articleshow/107465111.cms

18 http://archive.bionaturalists.in/id/eprint/2332/1/ijis_2024032515522794.pdf

19 https://www.researchgate.net/publication/372771141_Pre-training_of_Multi-order_Acoustic_Simulation_for_Replay_Voice_Spoofing_Detection

20 https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/

21 https://www.reuters.com/legal/ex-trump-fixer-michael-cohen-says-ai-created-fake-cases-court-filing-2023-12-29/

22 https://www.supremecourt.gov/publicinfo/year-end/2023year-endreport.pdf

23 https://www.acfe.com/fraud-resources/fraud-examiner-archives/fraud-examiner-article?s=may-2023-generative-ai

24 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

25 https://home.treasury.gov/news/press-releases/jy2167

26 https://www.fraudconference.com/35th-home.aspx

27 https://www.fraudconference.com/leadershipsummit2024.aspx

28 https://www.fraudconference.com/governmentsummit2024.aspx

29 https://ai-finance.org/

30 https://open.spotify.com/show/6atqSzy0Gea4596ZBrtZfo

31 https://www.thebrettjohnsonshow.com/

32 https://open.spotify.com/show/0fRLg5ta18zBtfZF949WaX

33 https://open.spotify.com/show/4l4vG4PIcnaGUcaAVJsufr

34 https://sumsub.com/podcast/

35 https://www.linkedin.com/in/frankmckenna/

36 https://www.linkedin.com/in/bkrebs/

37 https://www.linkedin.com/in/tony-sales-8311932a/?originalSubdomain=uk

38 https://twitter.com/Adam_K_Levin

39 https://twitter.com/Shirastweet

40 https://twitter.com/mikko

41 https://chat.openai.com/g/g-7iV2RaWSb-forensic-ledger-investigator

42 https://chat.openai.com/g/g-bEBYOC5iE-forensic-ledger-sleuth-gpt