



AMERICAN  
BANKRUPTCY  
INSTITUTE

## Winter Leadership Conference

# **WORKSHOP: Fraud, Frenzy and the Future: Unmasking Deceit in Complex Bankruptcy Cases**

Hosted by the Commercial Fraud & Emerging Industries  
and Technology Committees

**Warren Darakananda**

The Brattle Group, Inc.; Los Angeles

**Rachel Jaffe Mauceri**

Robinson & Cole LLP; Philadelphia

**Kathy Bazoian Phelps**

Raines Feldman Littrell LLP; Los Angeles

**Fraud, Frenzy and the Future:  
Unmasking Deceit in Complex Bankruptcy Cases**

**Panelists**

Warren Darakananda  
The Brattle Group

Rahcel Jaffe Mauceri  
Robinson & Cole LLP

Kathy Bazoian Phelps  
Raines Feldman Littrell LLP

American Bankruptcy Institute  
Scottsdale, AZ  
December 1, 2023

## Commercial Fraud in Bankruptcy and the Role of Artificial Intelligence

By Kathy Bazoian Phelps

Commercial fraud isn't going away. Often times, if the fraud is significant enough, the company finds itself in bankruptcy – perhaps from a voluntarily filing, or creditors may throw it into an involuntary bankruptcy, or regulators may seek an asset freeze and the appointment of a receiver. Creditors, trustees, regulators, and other interested parties commonly look first to the reason for the company failure. Was it bad luck, poor management, an economic downturn, or might there be fraud involved?

The debtor-in-possession, chief restructuring officer, Chapter 11 trustee, or receiver will often assemble a team of professionals, including forensic accountants, financial advisors, lawyers, and other investigators to figure out what happened, determine whether fraud has occurred and what happened to all of the money.

Technology, and artificial intelligence (AI) in particular, can be a double edge sword in fraud cases. AI may be what first enabled the fraud to take place, but it also may be the very thing that unravels the fraud and bolsters recoveries.

This article will discuss different types of fraud that may have led up to an insolvency proceeding, red flag warning signs of fraud, and the role that AI can play in luring in investors and growing the fraudulent scheme. This article does not cover the very substantial assistance that AI can provide in the investigatory work done to try to unravel the fraud.

### I. Types of Fraud

#### A. Ponzi Schemes

One of the more common types of large-scale frauds that land in insolvency proceedings are Ponzi schemes. If a true Ponzi scheme, ongoing business operations are unlikely as the scheme will have to stop operating since new funds will not be coming in and promised returns will not be paid out.

A Ponzi scheme is a fraudulent enterprise run under the pretense of a legitimate profit-making business. Investments are solicited from new investors, and those funds are then used to pay earlier investors. That, of course, induces further investments. All the while, the Ponzi scheme operator siphons off a substantial part of the funds for personal use and makes transfers of the investor funds to earlier investors and third parties. The scheme is destined to fail, often landing in a bankruptcy or receivership proceeding.

The facts considered by courts to determine whether a Ponzi scheme exists range in scope. One court created a four-factor analysis that many other courts have relied upon:

(1) deposits were made by investors; (2) the Debtor conducted little or no legitimate business operations as represented to investors; (3) the purported business operations of the Debtor produced little or no profits or earnings; and (4) the source of payments to investors was from cash infused by new investors.<sup>1</sup>

## **B. Theft of Cash**

There are a number of fraudulent schemes that involve different elements of fraud but may not rise to the level of a full Ponzi scheme. These fraudulent activities can nevertheless bankrupt a company if the dollars are large enough and if the fraud has gone undetected for a long time.

### **1. Embezzlement**

Embezzlement is the fraudulent taking of personal property by someone to whom it was entrusted. This often occurs when an employee misappropriates funds from an employer. Methods of embezzlement differ. Some embezzlers “skim off the top” so that they continually acquire a small amount over a long time period, helping to reduce the likelihood of being caught. On the other hand, some embezzlers steal a very large amount of money or property in a single instance and then disappear.

### **2. Cash larceny**

Cash larceny is the theft of money that appears on an organization’s books. This could involve employees writing checks to themselves or for their benefit, reversing cash transactions, or the creation of a fictitious vendor so that checks to the vendor can be cashed by the employee. This type of fraud can be detected through cash reconciliations of the organization’s records.

### **3. Skimming**

Skimming is fraud that involves the theft of money that has not yet been recorded in the organization’s books. For example, an employee accepts cash for a sale but keeps that cash rather than ringing it up as a sale at the cash register.

### **4. Lapping**

Lapping is a form of skimming where money received in payment of a receivable is stolen. To fill the hole, the next payment that is received for a different receivable is applied to the first receivable and so on.

---

<sup>1</sup> *Rieser v. Hayslip (In re Canyon Sys. Corp.)*, 343 B.R. 615, 630 (Bankr. S.D. Ohio 2006) (citation omitted).

## 5. Billing fraud

Billing fraud is the theft of cash when, for example, an employee charges personal purchases and disguises them as a business expense. Phony supporting documentation is prepared and the company pays the bills and receives no benefit.

## 6. Fraudulent submission of expense reports

Theft occurs when an employee submits personal expenses or phony expenses through expense reports to be reimbursed by the company, charging for things like excess mileage, extravagant meals, and gifts.

## C. Financial Statement Fraud

This type of fraud occurs when a company attempts to make the financials appear better or more robust than they are and, based on fictitious documentation, borrows money or improperly solicits invest dollars. Some examples of financial statement fraud are:

- a. Overstating revenue by recording sales prematurely
- b. Reallocating revenues to future periods to present a better financial picture
- c. Understating expenses
- d. Hiding or misrepresenting related party transactions
- e. Creating off-balance sheet accounts
- f. Improperly valuating assets or hiding liabilities

## II. Due Diligence to Uncover Fraud

### A. Warning Signs of Ponzi Schemes

The SEC has published red flag warning signs which many Ponzi schemes share in common:

- **High investment returns with little or no risk.** Every investment carries some degree of risk, and investments yielding higher returns typically involve more risk. Be highly suspicious of any “guaranteed” investment opportunity.
- **Overly consistent returns.** Investment values tend to go up and down over time, especially those offering potentially high returns. Be suspect of an investment that continues to generate regular, positive returns regardless of overall market conditions.
- **Unregistered investments.** Ponzi schemes typically involve investments that have not been registered with the SEC or with state

regulators. Registration is important because it provides investors with access to key information about the company's management, products, services, and finances.

- **Unlicensed sellers.** Federal and state securities laws require investment professionals and their firms to be licensed or registered. Most Ponzi schemes involve unlicensed individuals or unregistered firms.
- **Secretive and/or complex strategies.** Avoiding investments you do not understand, or for which you cannot get complete information, is a good rule of thumb.
- **Issues with paperwork.** Do not accept excuses regarding why you cannot review information about an investment in writing. Also, account statement errors and inconsistencies may be signs that funds are not being invested as promised.
- **Difficulty receiving payments.** Be suspicious if you do not receive a payment or have difficulty cashing out your investment. Keep in mind that Ponzi scheme promoters routinely encourage participants to “roll over” investments and sometimes promise returns offering even higher returns on the amount rolled over.<sup>2</sup>

## B. Types of Due Diligence

A lack of reasonable due diligence, especially in the face of red flag warning signs, is the primary reason that investors are scammed by Ponzi scheme perpetrators. Separately, once a company is in bankruptcy, similar due diligence analysis can assist in detecting and ultimately in unraveling a fraud. Fraud can be uncovered in a variety of ways – by a tip, by management review, by an internal audit, or sometimes accident. Additionally, some fraudsters in operating companies are discovered by police or other agencies. Lastly, we have seen the fraudster confess, usually admitting that they misappropriated less than they actually did, as the pressure becomes too much. Once in bankruptcy, a team of professionals can not only discover fraud, but can begin the process of unwinding the fraud to seek recovery for victims and creditors.

Some areas of due diligence designed to detect fraud are summarized as follows:

### 1. Bank Records

- Corraling all bank statements, cancelled checks, deposit detail and wire transfers

---

<sup>2</sup> SEC, *Ponzi Schemes — What are some Ponzi scheme “red flags”?*, <http://www.sec.gov/fast-answers/answersponzhtmi.html>.

- Trace the flow of funds and identify improper payments, payments to insiders, vendors and lenders
  - Build a preference and fraudulent transfer data base
- 2. Financial Statements**
    - Review audited financial statements
    - Review tax returns
    - Check for accuracy and completeness
    - Call the auditor
  - 3. Company Records Review**
    - Books and records of the business
    - Vendor files
    - Emails
    - Tracing of the cash through the bank accounts
    - Evaluation of proofs of claim
    - Interviews
    - Employee files
    - Company credit card usage
    - Disbursements
  - 4. Public Information About the Company**
    - Investigate negative news coverage
    - Conduct nationwide litigation search
    - Conduct criminal background check
    - Explore social networking sites
  - 5. The Business Model**
    - Investigate the need for investor funds
    - Is there a plausible, sustainable investment strategy?
    - Is there independently verifiable performance?
    - Are there unusual legal provisions?
  - 6. Complicated Corporate Structure**
    - Who are the principals?
    - Are there multiple levels of corporate ownership?
    - Are there affiliated companies in the same business?
    - Are there intercompany purchases and sales?
  - 7. Operational Issues**
    - Investigate accounting and reporting systems
    - Investigate reports made to customers
    - Are operations consistent with reports?
    - Is there micro-management by owner?

- Is there turnover at significant financial positions?

**8. Investigate Company's Auditor**

- Is the auditor for the investment truly independent?
- Is the size of the audit shop proportionate to the size of the investment?

**9. Red Flags from Financial Transactions**

- Customers who provide insufficient or suspicious information
- Customers who are reluctant to comply with reporting or record-keeping requirements
- Funds transferred to or from a financial secrecy haven
- Unusual transfers of funds between related entities
- Sudden inconsistencies in currency transaction patterns and shell company activities
- Significant increases in the number or amount of transactions
- Transactions that are not consistent with the customer's business or income level
- Transactions designed to lose the paper trail
- Circumvention of internal control procedures
- Lavish lifestyle of customers, which should not be supported by present income
- Customers with multiple accounts
- Diversion of funds to personal accounts
- Increases in the number or amount of transactions
- Transactions not consistent with company's business or income level
- Transactions designed to lose the paper trail
- Circumvention of internal control procedures.
- Irregular documentation
- Suspicious Intra-Company Transfers

**III. How AI is Used to Perpetuate a Fraudulent Scheme**

In addition to the more standard red flag warning signs of fraud, AI adds another layer of complexity. AI can be used to create AI algorithms to create more convincing and targeted schemes, or it may be used to analyze market trends and predict investor behavior that is then exploited to make fraudulent schemes seem more legitimate. AI may be used along with personal information obtained online to personalize scam texts and emails, making the fraud hard to detect. Fraudsters do not hesitate to take advantage of news and buzz around AI to entice investors into fraudulent schemes, AI is often offered up as the very reason why a scheme is able to generate greater profits. Using voice cloning and other AI impersonation through email or social media, fraudsters can obtain confidential information.



Below are some specific examples of how fraudsters can use AI to promote fraudulent schemes.

### 1. Social Engineering and Phishing Attacks

AI can analyze large volumes of data and create personalized phishing emails or messages that are believable and convincing due to their personalized nature. The messages contain individuals' online behavior and preferences as AI crafts messages that are designed to deceive the target.

### 2. Deepfake Technology

AI can generate deepfake videos or audio recordings that impersonate others. Fraudsters often impersonate people with authority in an organization as part of a scheme to manipulate individuals into divulging sensitive information or authorizing fraudulent transactions.

### 3. Algorithmic Trading Manipulation

AI can create algorithms to manipulate financial markets. For example, AI can create sophisticated trading bots that artificially inflate the value of a stock before selling it off in a pump and dump scheme.

### 4. Identity Theft

AI can be used to gather and analyze vast amounts of personal data from various sources which can then be used to create fake identities for fraudulent purposes such as opening bank accounts or applying for credit cards.

### 5. Fraudulent Account Creation

AI can automate the creation of fake accounts on online platforms, making it harder for security systems to detect patterns of suspicious behavior. These accounts can be used for various fraudulent activities, including fake reviews, scams, or spreading misinformation.

### 6. Credential Stuffing Attacks

AI can test large sets of username and password combinations obtained from data breaches on various online platforms. This method, known as credential stuffing, can gain unauthorized access to user accounts.

### 7. Adversarial Attacks on AI Systems

Fraudsters can manipulate AI systems themselves. Through adversarial attacks, they may subtly modify input data to deceive AI algorithms, leading to misclassifications or incorrect decisions. This can be particularly concerning in AI-powered fraud detection systems.

8. Chatbot Scams

AI-driven chatbots can be programmed to engage with users and extract sensitive information. These chatbots can mimic legitimate customer service interactions, leading individuals to unknowingly share personal details or login credentials.

Staying on high alert of fraud and implementing extra safeguards to independently verify emails and investment programs is paramount to stemming the tide of AI-induced fraud. While AI can be powerful tool to advance society, it is also being used as a force of evil to defraud unsuspecting and innocent people.

## Kathy Bazoian Phelps

Kathy Bazoian Phelps  
Raines Feldman Littrell LLP  
1900 Avenue of the Stars, 19<sup>th</sup> Floor  
Los Angeles CA 90067  
310-424-4080 (office)  
310-488-4883 (cell)  
[kphelps@raineslaw.com](mailto:kphelps@raineslaw.com)

Kathy Bazoian Phelps is a partner at Raines Feldman Littrell LLP in the Los Angeles office and has been a lawyer since 1991. She practices in the areas of bankruptcy law and fraud litigation, and frequently represents bankruptcy trustees and state and federal receivers, as well as serving as a Chapter 11 trustee herself. She represents litigants and parties in interest in bankruptcy and receivership cases and other insolvency proceedings. She is particularly knowledgeable about the administration of Ponzi scheme cases and has extensive litigation experience in claims arising in these types of cases and in tracing and recovering assets.

Kathy has lectured widely and written on bankruptcy and receivership matters, with a focus on Ponzi schemes. Her book entitled *The Ponzi Book: A Legal Resource for Unraveling Ponzi Schemes*, co-authored with Hon. Steven Rhodes, has garnered national and international attention as the authoritative work on Ponzi scheme law.

In addition to her roles as lawyer, speaker and author, Kathy also serves as a mediator and is currently on the mediation and arbitration rosters for the Financial Industry Regulatory Authority, as well as the Bankruptcy Mediation Panel for the Central District of California and the Bankruptcy Mediation Panel for the District of Arizona.

### Publications

- *The Ponzi Book: A Legal Resource for Unraveling Ponzi Schemes*. co-authored with Hon. Steven Rhodes (Ret.) (LexisNexis® 2012)
- *Fraud and Forensics: Piercing Through the Deception in a Commercial Fraud Case*, co-author (American Bankruptcy Institute 2015)
- *Ponzi-Proof Your Investments: An Investor's Guide to Avoiding Ponzi Schemes and Other Fraudulent Scams* (IRR Publishing 2013)
- *The Depths Of Deepening Insolvency: Damage Exposure For Officers, Directors and Others*, co-authored with Prof. Jack F. Williams (American Bankruptcy Institute 2013)
- Author of *The Ponzi Scheme Blog* at [www.theponziscHEMEblog.com](http://www.theponziscHEMEblog.com)

# ACFE INSIGHTS

NEWS AND ANALYSIS ON THE GLOBAL FIGHT AGAINST FRAUD

[ACFE INSIGHTS](#) [ACFE.COM](#) [FRAUD MAGAZINE](#) [BECOME A CFE](#) [EVENTS](#) [PRODUCTS](#)

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

January 06, 2023

ACFE Research  
Specialist

Laura Harris, CFE



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.

REGISTER TO ATTEND THE 35TH  
ANNUAL ACFE GLOBAL FRAUD  
CONFERENCE!

SEARCH ACFE INSIGHTS

SUBMIT A BLOG

Interested in contributing to *ACFE Insights*? Find out how you can become a featured guest blogger.

[LEARN MORE](#)

ARCHIVES BY CATEGORY

[Nonprofit Fraud](#)

[Internal Audit](#)

[Member Profile](#)

[ACFE News](#)

[ACFE Advisory Council](#)

[Insider Trading](#)

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

[Tax Fraud](#)  
[Accounting and Auditing](#)  
[Fraud Talk](#)  
[Computer Fraud](#)  
[Forensic Accounting](#)  
[ACFE History](#)  
[ACFE Chapters](#)  
[Healthcare Fraud](#)  
[Identity Fraud](#)  
[Audit](#)  
[Ponzi Scheme](#)  
[ACFE In the News](#)  
[AML](#)  
[Digital Forensics](#)  
[Consumer Fraud](#)  
[Corporate Governance](#)  
[Fraud Events](#)  
[Whistleblowing](#)  
[Data Analysis](#)  
[Bribery & Corruption](#)  
[Cyber Crime](#)  
[Compliance & Ethics](#)  
[Fraud News](#)  
[General Fraud](#)  
[ACFE Global Fraud Conference](#)  
[Career](#)  
[ACFE Events](#)  
[Fraud Investigation](#)  
[CFE Credential](#)  
[Fraud Resources](#)

[🔔 ACFE Insights RSS](#)



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 activity 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

**Have you enjoyed this article written by AI,  
but arranged by a human? Sound off in our  
[members-only Community](#).**

[Read More](#)



Together, Reducing Fraud Worldwide

[About the ACFE \(/about-the-acfe\)](#)
[\(/shopping-cart\)](#)
[Sign In \(/login\)](#)

[◀ Fraud Examiner Archives \(/fraud-resources/fraud-examiner-archives\)](#)

## ARTICLE

# Generative AI and the Fraud Examiner

By Samuel May | May 09, 2023

Share: [f \(/#facebook\)](#) [t \(/#twitter\)](#) [in \(/#linkedin\)](#) [e \(/#email\)](#)

This article will focus on the current capabilities of chatbots such as ChatGPT, Deepmind and Google's Bard. These chatbots represent a significant step forward for artificial intelligence (AI) and their applicability for common, day-to-day use.

Chatbots are large language model (LLM) AIs, neural networks that are trained (either self-supervised or with guidance and controls in place) on large quantities of text-based information. Currently, users communicate with the chatbot through text, though input will soon come from images, videos and other mediums as the capabilities of these AI increase.

## COOKIE SETTINGS

With any new advancement, it can be nearly impossible to accurately predict how prevalent, successful or long-lasting the use of a technology will ultimately be. Proponents of the current field of AI chatbots suggest that they will significantly increase

**Authors:****Samuel May, CFE**

Research Specialist,  
Association of Certified Fraud  
Examiners

productivity across virtually all job functions and provide an immensely powerful new tool to humanity. Opponents to the availability and use of these AI are more focused on the potential dangers of its expansion; even they believe the technology could be implemented across a remarkably diverse range of fields.

If you haven't had the chance to play with one of these chatbots yet, it is likely that you have seen video or articles discussing their use. In fact, the ACFE's Fraud Magazine has an article discussing the use of ChatGPT by cybercriminals in the May/June 2023 (<https://www.fraud-magazine.com/article.aspx?id=4295020976>) edition with some interesting inputs and AI responses.

Generally, after users sign up and are given access to the AI, they are provided with a short list of examples, capabilities and limitations before being directed to a blinking cursor in an empty text box. Text input is only limited by the imagination of the user. Depending on which chatbot you use, the responses can be limited by the creators of the AI. ChatGPT, for instance, will refuse to engage in "offensive behavior or language towards individuals or groups" if prompted to write something vulgar or derogatory. Increasingly, these guardrails are only minor impediments to getting what you want from the AI; workarounds (or "jailbreaks") are promulgated across the internet, from asking the AI to assume a persona to phrasing the output as a movie script or hypothetical.

## A warning at the beginning

Remember that anything typed into the text box of one of these AI tools is no longer private. Fraud examiners should be extremely careful with questions they ask and any information they feed into their prompts.

# How can fraud examiners make use of these chatbots?

Fraud examiners will need to pay attention to the capabilities and advancements of these AI technologies not just for their own use, but because they are already being leveraged by fraudsters (see [Is ChatGPT the newest gateway to fraud?](https://www.fraud-magazine.com/article.aspx?id=4295020976) (<https://www.fraud-magazine.com/article.aspx?id=4295020976>)).

The current slate of generative AI chatbots are essentially new tools that fraud examiners (and perpetrators) can and should learn to use.

Perhaps the easiest on-ramp for fraud examiners looking to learn to use these AIs is asking about fraud investigation fundamentals. Moving into a new field or investigating a new type of business? Ask the AI chatbot what you should look out for, what kind of frauds have occurred, how these specific kinds of businesses operate. At the very least, the chatbot can provide some useful search terms or definitions that can help establish a foundation for future learning. Ask Google Bard to explain how a kickback scheme works in a healthcare setting; its answer provides a basic definition of kickbacks and several common fraud schemes. These quick and easy answers should be used as a suggestive framework, not the gospel truth. Any information provided by a chatbot could be wholly false or grossly misleading. Verify any information it provides and conduct your own searches (and vet your own sources) for anything you will ultimately rely upon.

The simplest demonstration of the dangers of relying on an AI chatbot's research is to ask it about yourself. Start up a fresh chat with Bard and ask it to tell you about you. Based on a limited and not particularly random sample, the information Bard returned on different known individuals had numerous errors and inconsistencies. While fraud examiners might be tempted to shortcut conducting their own open-source intelligence (OSINT), these chatbots are not (currently) the best tool for the job.

# What does the AI think?

This article would be incomplete without what is now the standard approach when discussing generative AI: copying and pasting answers from a chatbot. While an AI was not asked to write portions of the article as some form of comparison, ChatGPT and Bard were both prompted with the question: “How can fraud examiners use generative AI?” The chatbots provided interesting responses:

Google Bard provides three uses and, interestingly, a few “use cases”:

*Generative AI can be used by fraud examiners in a variety of ways, including:*

- *Identifying fraudulent transactions: Generative AI can be used to identify fraudulent transactions by analyzing large amounts of data to identify patterns that are indicative of fraud. For example, generative AI can be used to identify credit card transactions that are likely to be fraudulent based on factors such as the amount of the transaction, the merchant and the customer's purchase history.*
- *Investigating fraud: Generative AI can be used to investigate fraud by helping fraud examiners to quickly and efficiently gather and analyze evidence. For example, generative AI can be used to identify potential witnesses, to locate relevant documents and to trace the flow of money.*
- *Preventing fraud: Generative AI can be used to prevent fraud by identifying and addressing the root causes of fraud. For example, generative AI can be used to identify vulnerabilities in payment systems, to develop training programs for employees on how to spot fraud and to create targeted prevention campaigns.*

COOKIES Here are some specific examples of how generative AI is being used by fraud examiners today:

## 2023 WINTER LEADERSHIP CONFERENCE

- *Bank of America: Bank of America is using generative AI to identify fraudulent credit card transactions. The bank's AI system analyzes billions of transactions every day to identify patterns that are indicative of fraud. For example, the system can identify transactions that are made from unusual locations or that are for unusually large amounts of money.*
- *PayPal: PayPal is using generative AI to investigate fraud. The company's AI system can quickly and efficiently gather and analyze evidence, such as emails, phone calls and social media posts. This helps PayPal to identify and prosecute fraudsters more quickly.*
- *Visa: Visa is using generative AI to prevent fraud. The company's AI system is constantly scanning the global payments network for signs of fraud. If the system identifies a potential fraud, it can automatically block the transaction.*

*Generative AI is a powerful tool that can be used to combat fraud. As the technology continues to develop, it is likely that fraud examiners will find even more ways to use it to protect their organizations from fraud.*

Fraud examiners would do well to take any “specific examples” provided by chatbots with copious amounts of salt. On a previous day, asking the same question, Bard provided a different list of three “real life” examples, one of which was the ACFE itself. Bard stated that the ACFE was actively using generative AI in reviewing data. This was a wholly incorrect statement.

ChatGPT provides:

*Fraud examiners can use generative AI in several ways, including:*

COOKIE SETTINGS

- *Fraud detection: Generative AI can analyze large amounts of data and identify patterns and anomalies that may indicate fraudulent behavior. For example, generative AI can be*

*trained to recognize fraudulent financial transactions or detect the use of false identities.*

- *Synthetic data generation: Fraud examiners can use generative AI to create synthetic data sets that mimic real-world scenarios. These synthetic data sets can be used to test fraud detection systems, train machine learning models, and conduct simulations of potential fraud scenarios.*
- *Fraud prediction: Generative AI can analyze historical data to predict future fraudulent activities. By analyzing patterns in data and identifying potential risk factors, generative AI can help fraud examiners anticipate and prevent fraudulent behavior.*
- *Fraud investigation: Generative AI can assist fraud examiners in investigating fraudulent activities by generating possible scenarios and identifying possible suspects. For example, generative AI can analyze email communications or social media activity to identify potential fraudsters or uncover hidden connections between suspects.*

*It's worth noting that while generative AI can be a powerful tool for fraud examiners, it's important to use it ethically and responsibly. Generative AI should be used in conjunction with human expertise and judgment to ensure that the results are accurate and unbiased.*

While machine learning does, and generative AI will, play a large role in data analysis and the detection of fraud, examiners should refrain from feeding any of the currently available chatbots real data for fraud detection. New tools might be developed, with sufficient safeguards in place, that end up in the fraud fighting toolkit, but the current slate of chatbots is not a proper venue for fraud detection.

The creation of synthetic data, hypothetical fraud scenarios and what could essentially be “practice problems” for fraud examiners is an interesting idea and one use that poses considerably less threat to the safety of private or proprietary data. Fraud examiners looking to sharpen their data analysis techniques could turn to generative AI for producing case

COOKIE SETTINGS



studies with known answers instead of relying on de-identified or test data that currently exists in limited supply through internal or external training sources.

## Helpful uses

Fraud examiners might turn to chatbots and generative AI to assist in producing written reports or documentation. The number of instances of ChatGPT being used for school essays, clickbait articles and an entire swath of legitimate and illegitimate writing increases every day. Fraud examiners should, again, refrain from prompting AI with sensitive information to create a report, but fraud examiners should also be wary of plagiarism or lazy copy and paste jobs. Fraud reports are often the culmination of a laborious, intensive, complicated fraud examination and, while writing everything down could be the least “fun” part of the job, it is also the memorialization of everything that was done. AI-generated writing still comes replete with errors and inhuman, out-of-place phrasing. The creators of ChatGPT have gone so far as to release a tool capable of distinguishing between human work and AI generated text.

Outside of the written word, fraud examiners can jumpstart their programming or data analysis capabilities. Excel formulas, for instance, can be incredibly useful time savers when dealing with large data sets or crunching numbers. For fraud examiners who don't use them routinely, there is often some trial and error when trying to get known formulas to spit out the necessary information. Chatbots can be prompted with common language directions to return complex formulas. For the more tech-savvy fraud fighters, generative AI have proven incredibly useful for software development, once again taking basic commands and translating them into the requested programming language. Do you need to write a quick script or automate a frequently used command? Not even sure what that means? Generative AI can help explain, create and implement basic programs.

## What's next?

While ChatGPT might be a passing trend, a diversion to throw questions at when you've exhausted your social media updates, perhaps, generative AI is ramping up and pushing itself into everyday life. Fraud examiners are likely already seeing or will shortly be made aware of the use of AI chatbots in the commission of fraud. Fraud examiners can look to current chatbots to expand their skillsets, possibly save some time and, eventually, help combat fraud at every level. AI might not be there yet, but chatbots have already seen an explosion in use and capability in their short time on the stage. The ACFE will keep an eye on what comes next and work to keep fraud fighters informed.



(/)

[About the ACFE \(/about-the-acfe\)](/about-the-acfe)

[Contact Us \(/contact-us\)](/contact-us)

[For Media \(/about-the-acfe/newsroom-for-media\)](/about-the-acfe/newsroom-for-media)

[For Advertisers \(/about-the-acfe/for-advertisers\)](/about-the-acfe/for-advertisers)

---

Copyright 2023 Association of  
Certified Fraud Examiners, Inc.

[Site Policies \(/legal-and-site-policies\)](/legal-and-site-policies) |

[Privacy Policy \(/privacy-policy\)](/privacy-policy) |

[Accessibility Policy \(/accessibility-policy\)](/accessibility-policy)

**COOKIE SETTINGS**

# Faculty

**Warren Darakananda, CFA, CPA, ABV** is an associate in the Bankruptcy and Restructuring Practice at The Brattle Group in San Francisco and Los Angeles. He specializes in providing financial advisory, forensic accounting, fraud examination and expert testimony services to companies and their investors. Mr. Darakananda specializes in valuation, due diligence, accounting, financial reporting, claims analysis, securities analysis and fraud investigation, particularly in the context of corporate transactions. His recent engagements include matters involving Washington Prime Group, Tuesday Morning, Inc. and Twitter. He also has analyzed cross-border transactions, particularly those between the U.S. and Latin America, Australia and Asia. Mr. Darakananda is a Certified Public Accountant licensed to practice public accountancy by the California Board of Accountancy, and he is a member of the Chartered Financial Analyst Institute, the Association of Certified Fraud Examiners, the American Institute of Certified Public Accountants and the National Asian Pacific American Bar Association. He is Accredited in Business Valuation by the AICPA. Mr. Darakananda received his B.A./B.S. in economics and mathematics from the University of California, Los Angeles and his M.B.A. in finance from The Wharton School, The University of Pennsylvania.

**Rachel Jaffe Mauceri** is a partner with Robinson & Cole LLP in Philadelphia in the firm's Bankruptcy + Reorganizations Group and has more than 20 years of experience counseling clients in complex corporate bankruptcy and restructuring matters. She participates in all aspects of in- and out-of-court restructurings in such industries as health care, retail, energy, automotive, oil and gas, mortgage-servicing, real estate and telecommunications. Ms. Mauceri regularly represents official committees in chapter 11 cases and has experience counseling companies in pre-negotiated and traditional bankruptcy proceedings as well as out-of-court workouts, advising stalking-horse and other bidders in distressed and bankruptcy-related transactions, representing borrowers and financial institutions in the negotiation and documentation of secured lending facilities, advising indenture trustees and second-lien lenders, representing pension and health plans in connection with collective bargaining issues and proceedings under §§ 1113 and 1114 of the Bankruptcy Code, and counseling vendors, contract parties and other significant creditors and parties in interest on a variety of bankruptcy-related litigation and other issues. She is listed in *Chambers USA: America's Leading Lawyers for Business, Pennsylvania & Surrounds*, and she was named to the *IFLR 1000 United States* as a Notable Practitioner in 2022 and as a Rising Star in 2021, 2020 and 2019 in the area of Restructuring. In addition, she was named a Rising Star, Restructuring (including Bankruptcy): Corporate in *The Legal 500 US* in 2019, and she represented Tribe 9 Foods in its 2021 purchase of Carla's Pasta, which won the Food & Beverage Restructuring of the Year at the 14th Annual Turnaround Atlas Awards. She also represented The Bank of New York Mellon as indenture trustee in connection with the sale of North Philadelphia Health System, a transaction that won the 17th Annual M&A Advisor Sector Deal of the Year, in the category of "Healthcare and Life Sciences (Under \$100MM)." Ms. Mauceri regularly speaks and writes on current issues and topics in bankruptcy. She currently serves as vice chair of the Chapter Presidents Counsel of the Turnaround Management Association and as a member of TMA Global's Executive Board and board of directors, and she is chair of TMA's Philadelphia/Wilmington chapter. She also is a member of ABI and IWIRC, is co-chair of ABI's 2023 VALCON conference, and is secretary of the Consumer Bankruptcy Assistance Project. Prior to joining Robinson & Cole, Ms. Mauceri worked for two global law firms in New York and Philadelphia, respectively, focusing

on bankruptcy and restructuring matters. While in law school, she interned for Hon. Prudence Beatty Abram (ret.) of the U.S. Bankruptcy Court for the Southern District of New York. Ms. Mauceri received her B.A. in journalism from Ithaca College in 1995 and her J.D. *cum laude* in 2001 from Benjamin N. Cardozo School of Law, where she was elected to the Order of the Coif and was supervising editor of its law review.

**Kathy Bazoian Phelps** is a partner at Raines Feldman Littrell LLP in Los Angeles and has more than 30 years of practice in the areas of insolvency law, fiduciary representation and fraud litigation. Her practice includes representing federal equity and state court receivers and bankruptcy trustees, as well as serving as a fiduciary herself. Ms. Phelps frequently serves as special litigation counsel for fiduciaries and interested parties in fraud-related litigation or cases arising out of receivership and bankruptcy cases. She is particularly knowledgeable about the administration of Ponzi scheme cases and has litigation experience in claims arising in these types of cases. Ms. Phelps has lectured widely and written on bankruptcy and receivership matters, with a focus on Ponzi schemes. Her book *The Ponzi Book: A Legal Resource for Unraveling Ponzi Schemes*, co-authored with retired Bankruptcy Judge Steven Rhodes, has garnered national and international attention as the authoritative work on Ponzi scheme law. She also is author of *Ponzi-Proof Your Investments: An Investor's Guide to Avoiding Ponzi Schemes and Other Fraudulent Scams* (IRR Publishing 2013), a co-author of *Fraud and Forensics: Piercing Through the Deception in a Commercial Fraud Case* (American Bankruptcy Institute 2015) and *The Depths of Deepening Insolvency: Damage Exposure For Officers, Directors and Others* (American Bankruptcy Institute 2013), and author of The Ponzi Scheme Blog at [www.theponziscHEMEblog.com](http://www.theponziscHEMEblog.com). In addition to her roles as lawyer, speaker and author, Ms. Phelps has served as a mediator. She received her B.A. in international relations from Pomona College and her J.D. from University of California, Los Angeles in 1991.