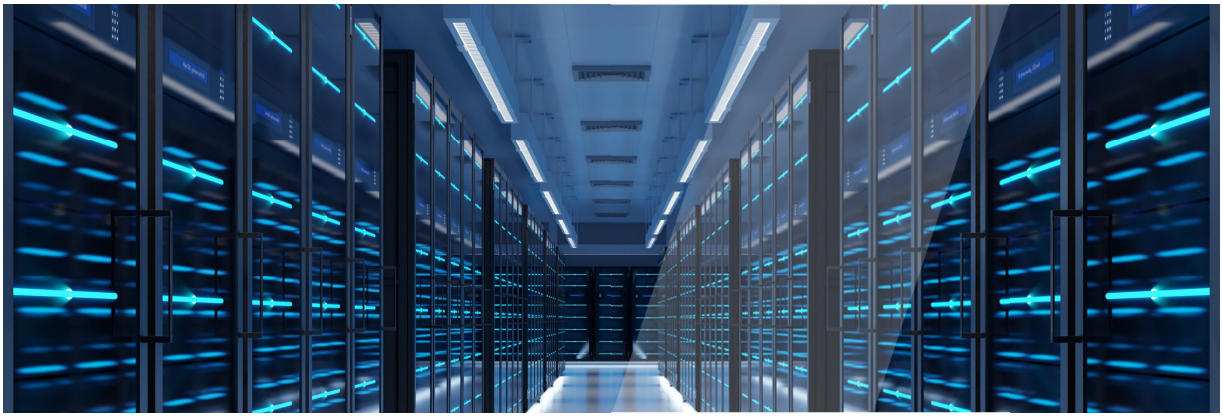


Artificial Intelligence: The Evolution of Fraud Investigations
2024 Fall Forensics Institute

November 7, 2024

forvis mazars

1

TO RECEIVE CPE CREDIT

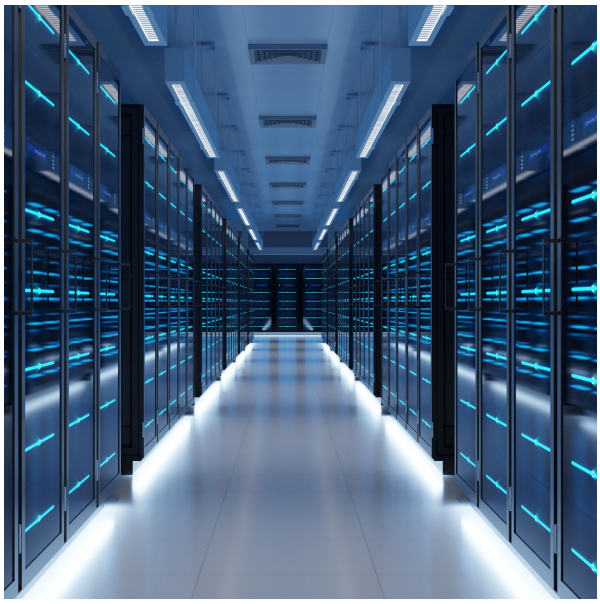
- Attendees must respond to at least 3 of the 4 polling questions per CPE hour
- Attendee must be logged in for a minimum of 50 minutes per every CPE hour in order to receive CPE credit

forvis mazars

2

Agenda

1. Introductions
2. Define Artificial Intelligence
3. AI & the Fraud Triangle
4. AI & Fraudulent Behavior
5. AI & Fraud Investigations
6. Preparation for AI Changes
7. Closing Questions



3

Meet the Presenters

Sean Leonard
Manager
sean.leonard@us.forvismazars.com

Ben Wallace
Consultant
ben.wallace@us.forvismazars.com

4

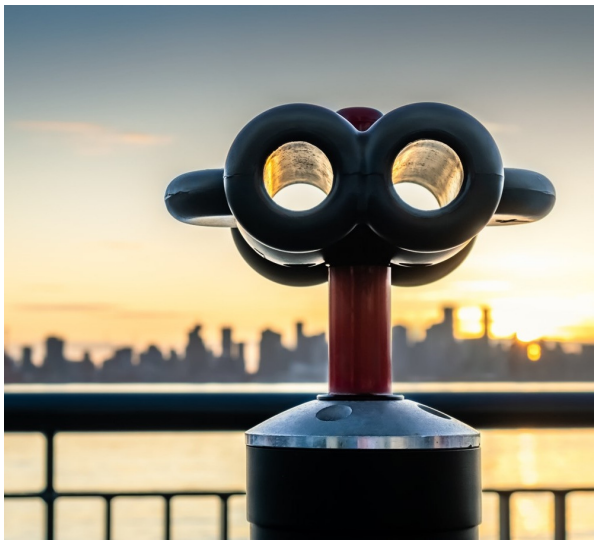
01

Define Artificial Intelligence

5

What Is Artificial Intelligence?

- Artificial Intelligence
  - "Technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy."[1]
- Examples of AI:
  - Netflix (Machine Learning Algorithms)
  - Google Generative AI (Appears in Search Browser)
  - Copilot (Windows Artificial Intelligence Assistant)
  - Chatbots (Algorithms Utilizing User Responses)



1: https://www.ibm.com/topics/artificial-intelligence

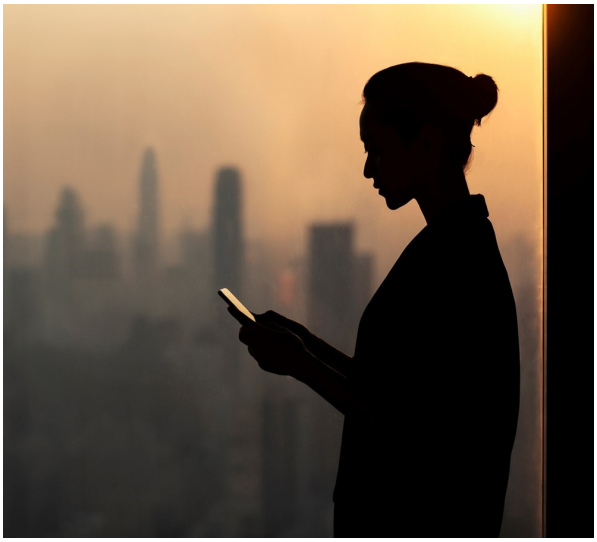
6

forvis mazars

6

History of Artificial Intelligence

- **1935** – Alan Turing began development of a computing machine with limitless memory
- **1945** – AI began its application in chess
- **1951** – Christopher Strachey developed the first AI program at the University of Oxford
- **1972** – MYCIN, a system developed to treat blood infections, began development at Stanford University
- **1980s** – Nouvelle AI began development in MIT AI Laboratory [1]



1: https://www.britannica.com/science/history-of-artificial-intelligence/Connectionism

7

forvis mazars

7

How Does AI Relate to Fraud?

- As noted in our definition, AI is designed to mimic human comprehension, critical thinking, behavior, & problem solving.
- Fraudsters utilizing AI can replicate human behavior on a level never seen before its development.

8

forvis mazars

8

CPE Question 1

What is an example of AI?

A Netflix Machine Learning Algorithms

B Digital Cameras

C Bluetooth

forvis mazars

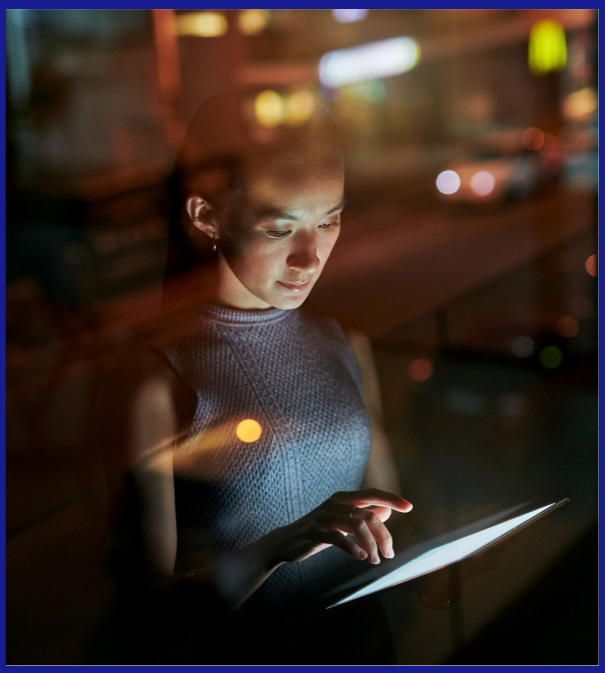
9

forvis mazars

10

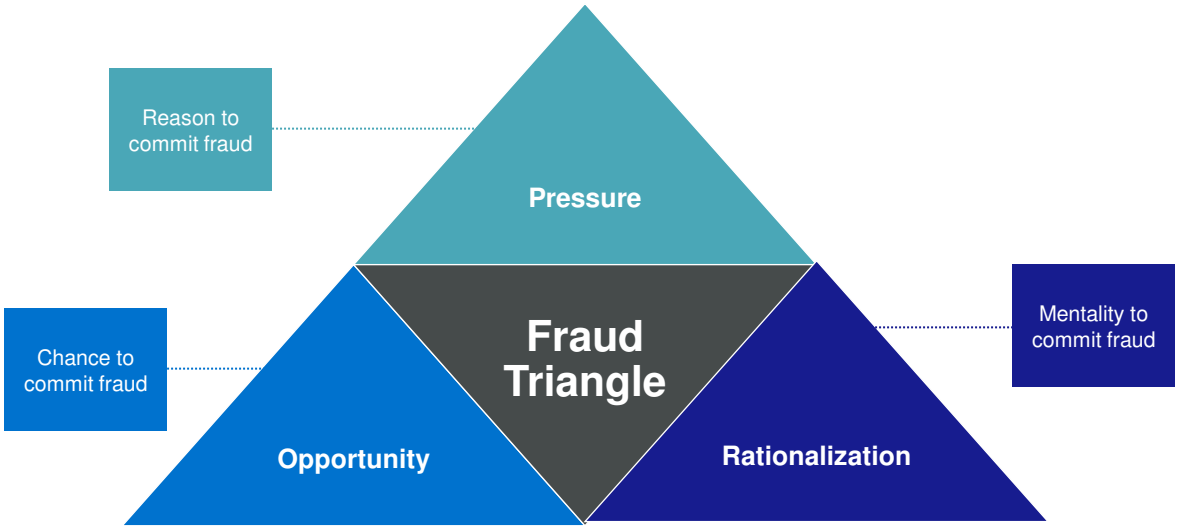
02

AI & the Fraud Triangle



11

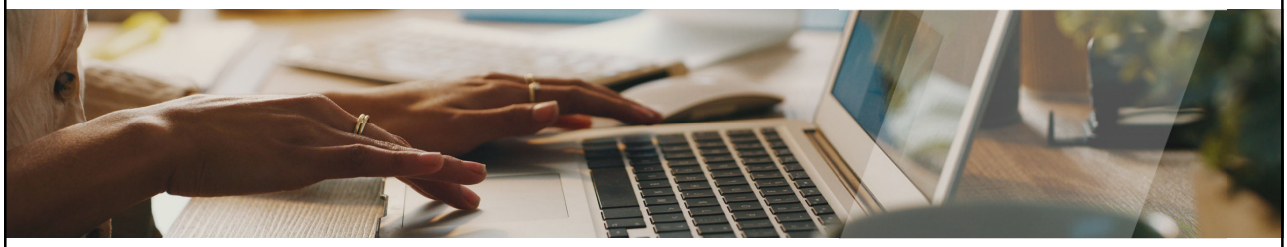
What Do People Need to Commit Fraud?



12

12

AI & the Fraud Triangle



AI & How It Changes Opportunity & Rationalization

- AI provides fraudsters with a unique set of tools that allows them to implement tactics that replicate human action, verbiage, & conversations without needing to be physically present or engaged in an act of fraud. This increases the opportunity portion of the Fraud Triangle.
- AI also puts a degree of separation between the fraudster & victim. By conducting fraud online or through machine learning programs, fraudsters do not have to face their victims during their acts of deceit. This impacts the rationalization portion of the Fraud Triangle.

forvis mazars

13

03

AI & Fraudulent Behavior

14

Fraud Risk to Businesses

$12 Billion
2023 Fraud Loss to GenAI

$40 Billion
2027 Fraud Loss to GenAI

230%
Increase

1: https://www2.deloitte.com/us/en/blog/accounting-finance-blog/2024/ai-fraud-risk-management.html

forvis mazars

15

How Is AI Increasing the Risk of Fraud?

Generative AI

- Programs like ChatGPT, founded by OpenAI, & many other generative AI models allow users to create complex & articulate passages, emails, photos, & videos that replicate the language & behavior of humans.

Generated by OpenAI's ChatGPT Image Generator Function "Man on Beach"

"Generative AI refers to deep learning models that can generate high-quality text, images, and other content based on the data they were trained on."[1]

1: https://research.ibm.com/blog/what-is-generative-AI

forvis mazars

16

Real or AI?

17

18

Real or AI?

19

20

Real or AI?

21

21

22

Real or AI?

23

23

24

Generative AI & Fraud

Phishing Scams “Spoofing”

Spoofing is a kind of phishing attack. The bad actor who sends the message is posing as a trusted person known to the message recipient. That's the difference between a more general phishing attack & a spoofing attack.[1]

Deep Fakes

A deep fake refers to a specific kind of synthetic media where a person in an image or video is swapped with another person's likeness.[2]

1: https://www.aicpa-cima.com/news/article/q-and-a-2-cyberattacks-cpa-firms-should-fear

2: https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

25

forvis mazars

25

Generative AI & Spoofing

Pre-Generative AI Spoofing/Phishing Email

Reminder [Email Invoice] : Receipt for Your Payment to DeLL Electronic Center.,LTD
Reference #PP-272-001-181-1919

S service@intl.paypal.com <DearCostumers@notification.account.support-suspicious-email-access-acc

Reply

Yesterday, 8:37 AM
You

Invoice Transaction.pdf
593 KB

Download Save to OneDrive - Personal

PayPal

Thanks for your purchase on your PayPal account

Dear

Thanks for your purchase on done the payment transaction by using your paypal account, with the preview invoice in PDF files listed product Dell.com directed, please Download File PDF for reviewing your transaction.

This not you ?
Dont worry we can cancel this payment and dispute transaction
To cancel this payment and dispute transaction please download the PDF file Transaction payment.

Thanks,
PayPal Support

Copyright © 1999-2018 PayPal Inc. All rights reserved.

PayPal PPC000263:ac9469fca632c

https://blog.mxtoolbox.com/2018/01/11/what-is-email-phishing/

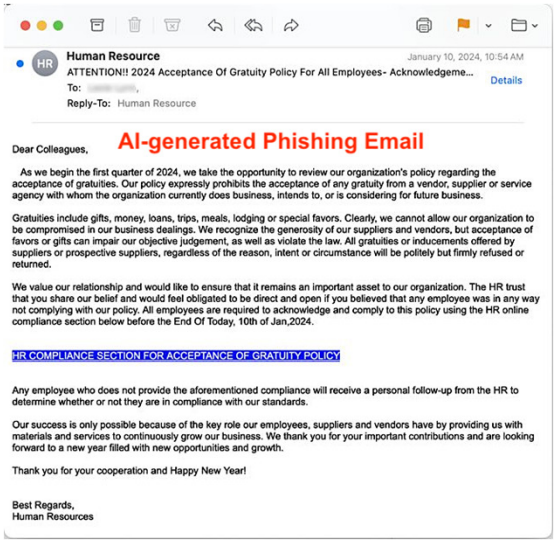
26

forvis mazars

26

Generative AI & Spoofing

Generative AI Spoofing Email

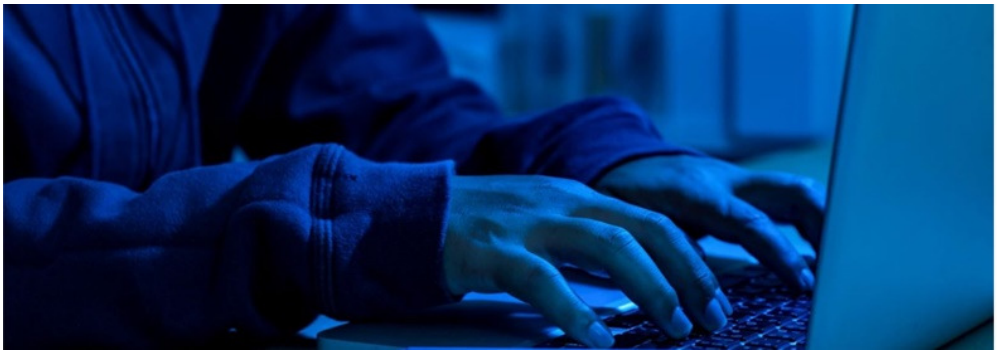


https://www.memcyco.com/how-can-ai-be-used-to-combat-phishing-attacks/

Deep Fake Example

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
Published 2:31 AM EST, Sun February 4, 2024



CPE Question 2

What is an element of the Fraud Triangle?

A Money

B Rationalization

C Technology

forvis mazars

29

forvis mazars

30

04

AI & Fraud Investigations

31

Is AI Committing Fraud or Are Fraudsters Using AI to Commit Fraud?

We do not see AI committing fraud by itself. Fraudsters utilize the tools of AI to commit fraud

- It is important to recognize that an autonomous computer is not committing fraud by itself. Fraudsters are using the expanding AI landscape to commit fraud at a greater & more advanced rate.
- This means we must develop tools to combat fraudsters who utilize AI to steal or do harm to businesses.

32

forvis mazars

32

Tools Utilizing AI for Fraud Investigations

- While AI is increasing the tool set of fraudsters, it is also providing Fraud Investigators with increased utility to combat increasing fraudulent behavior
- Many tools are available that utilize AI to identify fraudulent activity, process large document uploads, & identify phishing emails for companies.
- Examples
  - Intella's – Predictive Coding
  - Behavioral Analysis – AI Technology can examine customer behavior to identify suspicious actions.
  - Natural Language Processing (NLP) – AI algorithms can examine communications & flag indicators of fraudulent behavior
- AI is providing investigators with faster methods of examining large amounts of data & providing meaningful results.

1: https://www.fraud.com/post/artificial-intelligence#:~:text=AI%2Dpowered%20fraud%20detection%20systems,accuracy%20and%20effectiveness%20over%20time.

forvis mazars

33

AI Detection of Deep Fakes

Fight Fire With Fire

- Companies are continually creating AI models to combat deep fake fraud schemes.
- While AI deep fakes are convincing, there are ways to detect whether an image or video is an AI-generated deep fake or if it is an authentic piece of media.
- Non-AI Methods of Detection:
  - Look for facial transformations, aged skin, or skin that looks too wrinkly
  - Look for unnatural shadows
  - Glasses are a key indicator of an AI generated video or image; do they appear to be in the correct place or show the correct glare?
  - Look for unnatural blinking or lip movements[1]

1: https://www.media.mit.edu/projects/detect-fakes/overview/

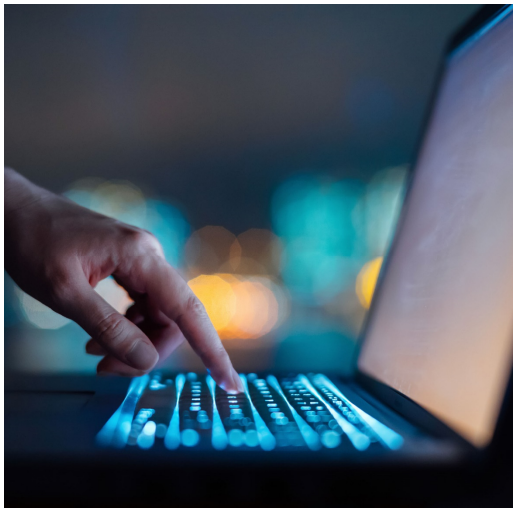
forvis mazars

34

AI Detection of Deep Fakes

Potential AI Methods for Detecting Deep Fakes

- **TensorFlow & PyTorch** – free tools that utilize deep neural networks to detect images that were produced using AI.
- **DeepWare** – an open source tool that allows users to upload videos & scan media to determine whether they were synthetically created
- **Sensity** – utilizes visual & context clues to determine whether media is fabricated or not.[1]



1: https://www.globalbusinessjournalism.com/post/6-ai-tools-that-can-help-you-combat-deepfakes#:~:text=TensorFlow%20and%20PyTorch%20are%20two,to%20differentiate%20between%20the%20two.

35

forvis mazars

35

CPE Question 3

What is NOT a type of AI deception we have discussed?

A Deep Fakes

B Spoofing

C GIFs

forvis mazars

36

Slide 35

BW0 Do we need a disclaimer that we do not endorse these products?
Wallace, Ben, 2024-10-22T01:40:40.566

MC0 0 I don't think that will hurt. Am going to leave this comment in and have the risk reviewer determine what's best.
Connor, Mary, 2024-10-23T17:58:44.802

MG0 1 I'm not sure we need a disclaimer, but we could edit the subheader to say "Potential AI Methods for Detecting Deep Fakes"; that way these are just listed as "potential" methods, rather than more definitive methods

There's also the disclaimer on the second-to-last slide (The information set forth in this presentation ...), which should act as a "shield" for us. In any case, if you feel it's necessary or if it feels more comfortable, we could always make a point of saying something out loud during the presentation about how these are just examples, Forvis Mazars doesn't endorse these products, etc.
Grimes, Mark, 2024-10-28T17:09:09.485

forvis mazars

37

05

Preparation for AI Changes

38

What Can Your Business Do to Prevent AI Fraud?

1. Understand & Prepare
2. Understand the Risks That Face Your Specific Business
3. Prepare Training Seminars to Help Identify Spoofing Scams or Deep Fakes.

1: https://www.ibm.com/topics/artificial-intelligence

39

39

1. Understand & Prepare

- The first step in preparing for AI-based fraud is to recognize that it is a growing threat.
- AI is allowing users to manipulate data & fool business owners in a way we have not seen before.
- Recognizing that AI is a new threat will allow businesses to properly prepare their relevant segments for potential harmful attacks

1: https://www.ibm.com/topics/artificial-intelligence

40

40

2. Understand the Risks That Face Your Specific Business

- Every business is different.
- Having a strong grasp on tools used often in your business is an important step in identifying segments of your business that are at particular risk.
- Examples of Segments that could be impacted by AI:
  - Executives who have public videos available online
  - Segments that utilize Outlook, Gmail, or other email platforms often.
  - Businesses that utilize proof of expense requirements for expense reimbursements.

1: https://www.ibm.com/topics/artificial-intelligence

41

41

3. Prepare Training Seminars to Help Identify Spoofing Scams or Deep Fakes

- The best way to stop any fraud is to identify it before it can do any damage
- Spoofing & deep fakes have changed the training necessary to adequately prepare employees to identify fraud.
- Spoofing emails can no longer be identified solely based off of grammar errors or incorrect facts contained within.
- Train employees to report suspicious or unplanned emails & unusual images or videos that were not disclosed before reception.

1: https://www.ibm.com/topics/artificial-intelligence

42

42

Polling Question

Would you like to be contacted by one of the presenters to discuss this topic further?

A Yes

B No

C

D

43

CPE CREDIT

- CPE credit may be awarded upon verification of participant attendance
- For questions, concerns, or comments regarding CPE credit, please email Forvis Mazars at cpecompliance@us.forvismazars.com

Forvis Mazars, LLP is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

44

Contact

Forvis Mazars

Thank you!

Lanny Morrow
Senior Manager
lanny.morrow@us.forvismazars.com

Ben Wallace
Consultant
ben.wallace@us.forvismazars.com

Sean Leonard
Manager
sean.leonard@us.forvismazars.com

forvis mazars

45