MTSU
ACCOUNTING

Innovations in Fraud Detection

CPA Ontario Centre in Digital Financial Information

Andrea Seaton Kelton, PhD
MTSU Accounting Advisory Board Outstanding Professor
Associate Professor of Accounting

MTSU
ACCOUNTING

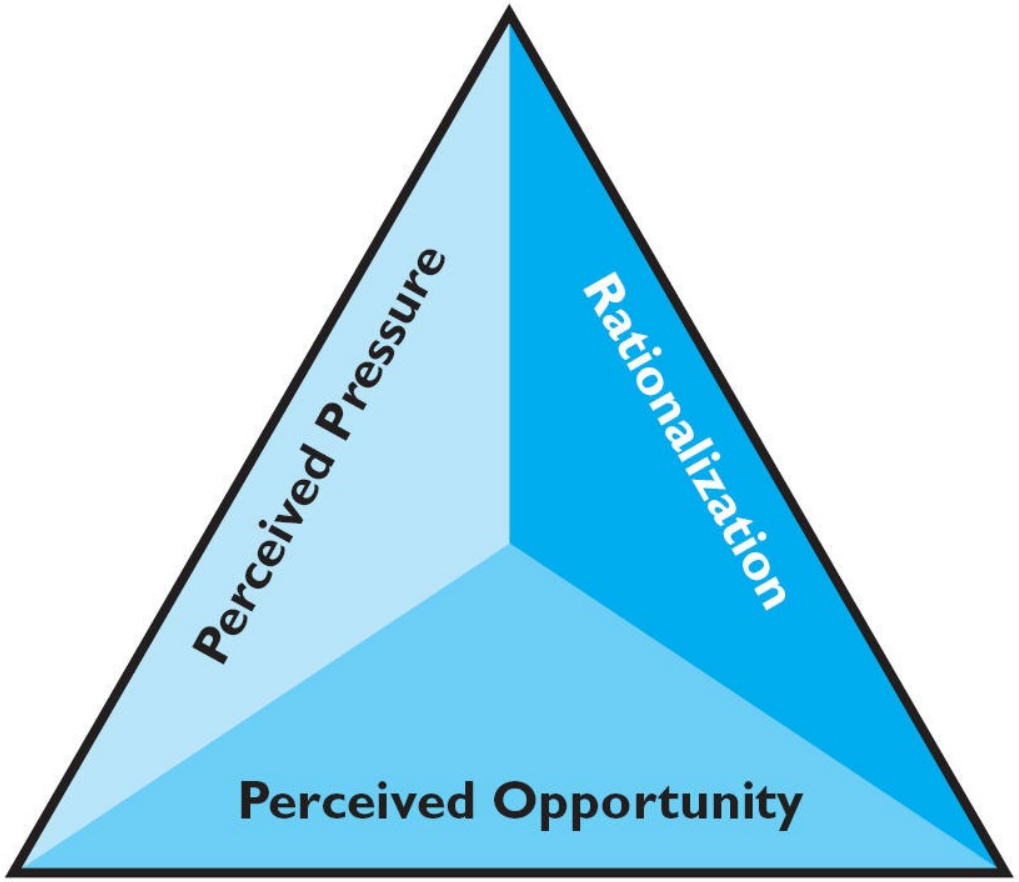
Agenda

1. How is technology making *committing* fraud easier?
2. How is technology making *detecting* fraud easier?

USING TECHNOLOGY TO COMMIT FRAUD

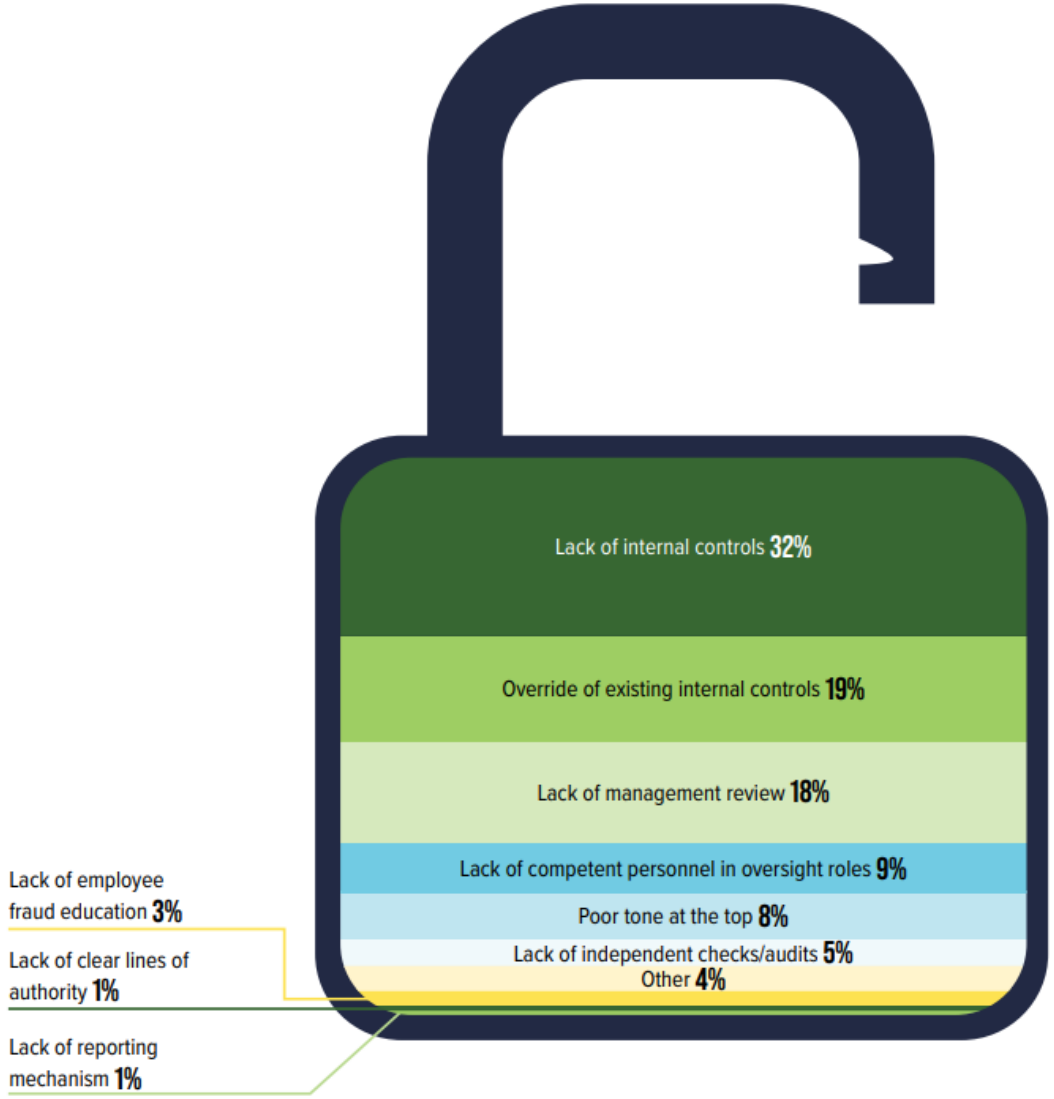
MTSU ACCOUNTING

Why do people commit fraud?



Source: Albrecht (2014)

How do people commit fraud?



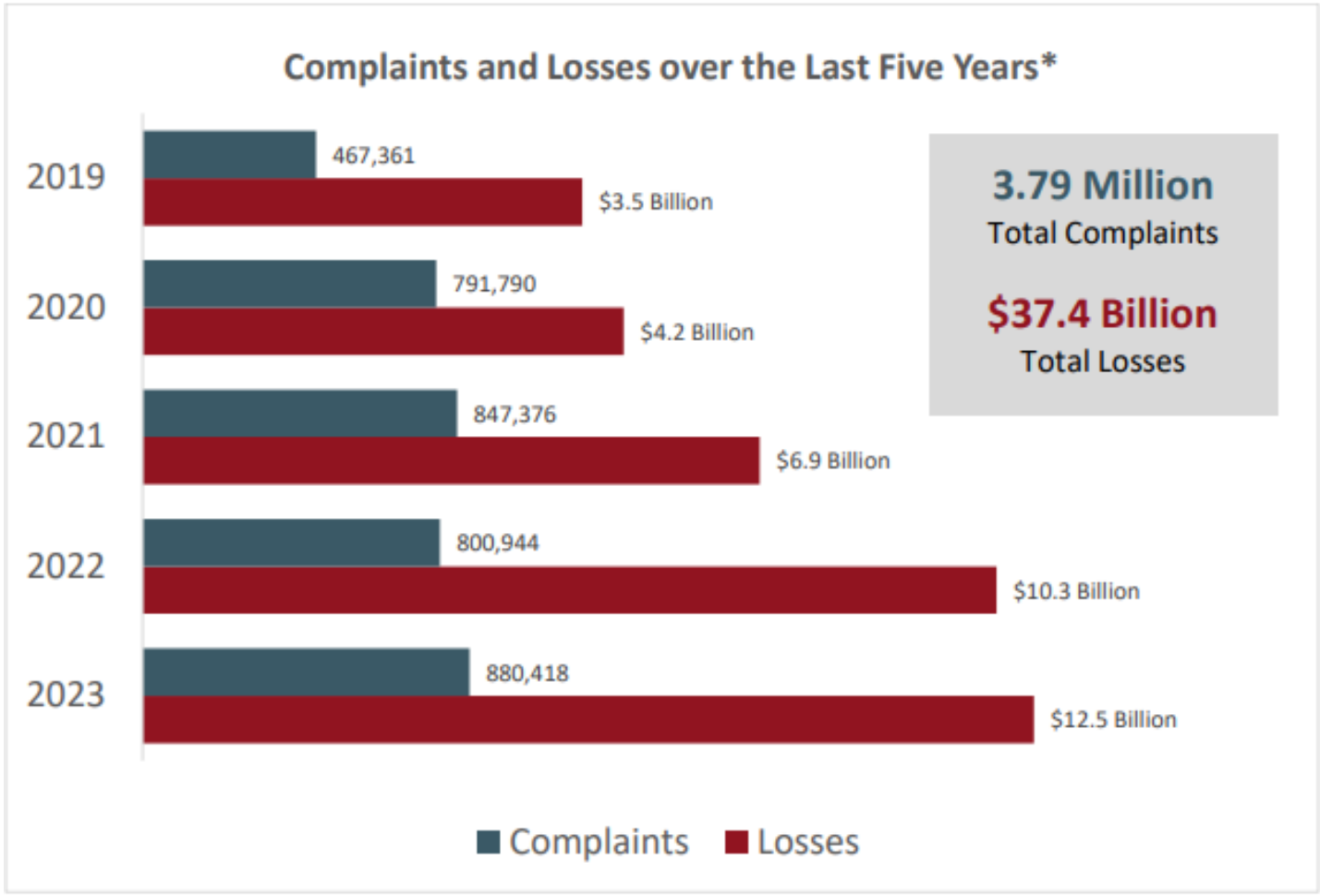
Source: ACFE Occupational Fraud 2024: A Report to the Nations

MTSU ACCOUNTING

↑Technology =↑Opportunity

- More transactions occurring online and using peer-to-peer payment systems
- Digital currencies
- Remote work

HOW BIG OF A PROBLEM IS INTERNET FRAUD?



Source: [FBI Internet Crime Report 2023]

MTSU ACCOUNTING

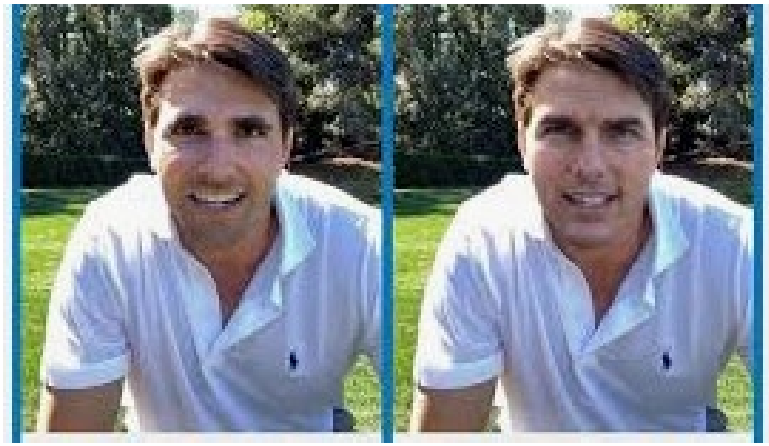
Some specific fraud schemes

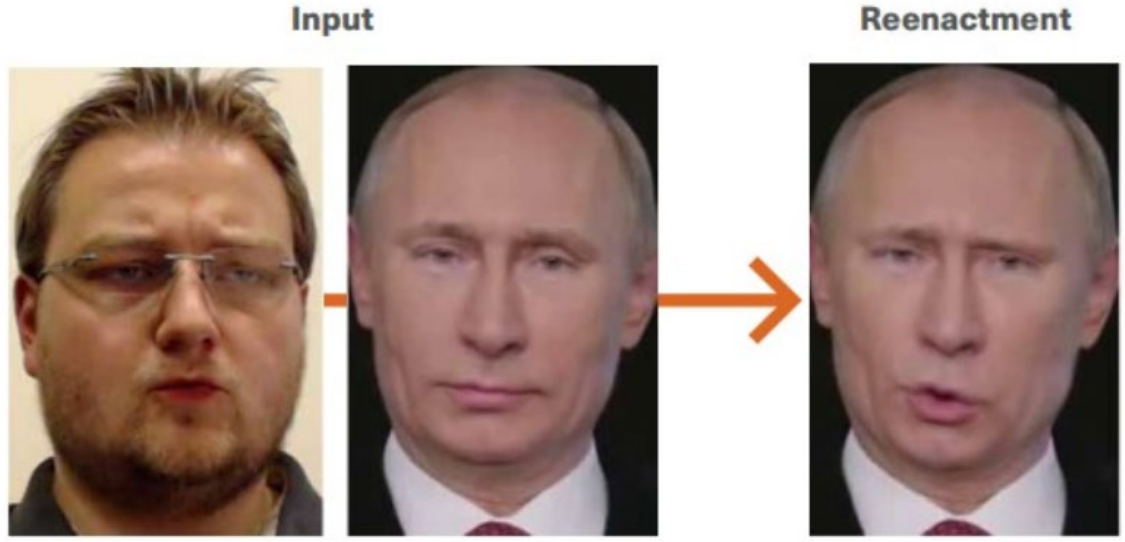
- Deepfakes
- Ransomware
- Business e-mail compromises

WHAT IS A DEEPFAKE?

- Deepfakes - synthetic media in which a person in a video or audio can be replaced with someone else's likeness

- Created with the use of deep learning algorithms that can swap faces and voices in digital and video media.





MTSU ACCOUNTING

A deepfake example

- A finance employee at multinational firm received request to attend video call with CFO
- The employee thought he was speaking to the CFO and other staff members on a video conference call – all were deepfakes
- Employee agreed to remit $200 million Hong Kong Dollars ($25.6 millions USD)
- Scam discovered later when employee checked with the head office

Source

MTSU ACCOUNTING

Deepfakes for the masses

- Open AI
  - *Sora Video Generation Tool* – user can type out a scene and AI turns it into high-def video clip
  - *Voice Engine* – can recreate an individual's voice from 15 seconds of speaking

Source

THE GROWING RISK OF DEEPFAKES

TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

10 March 2021

PIN Number

210310-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Field Office**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations

Summary

Malicious actors almost certainly will leverage synthetic content for cyber and foreign influence operations in the next 12-18 months. Foreign actors are currently using synthetic content in their influence campaigns, and the FBI anticipates it will be increasingly used by foreign and criminal cyber actors for spearphishing and social engineering in an evolution of cyber operational tradecraft.

Source: FBI Internet Crime Complaint Center

WHAT IS BUSINESS EMAIL COMPROMISE?

- Fraudster impersonates an executive via email to trick employees into sending money or sensitive information
- Fraudster compromises legitimate email accounts through social engineering or other methods
- In 2023, IC3 received over 21,000 complaints with losses over $2.9 billion

---------- Forwarded message ---------
From: **Tim Holmes** <tim@holmesswaffordcpa.com>
Date: Fri, Mar 29, 2024, 5:51 PM
Subject: Urgent Notice: Tax Refund
To: laura@holmesswafford.com <laura@holmesswafford.com>

Good evening,

I have just received an important notice from IRS regarding your tax return, apologies for the late response.
It's important I reach out to you before the end of the day.
I'll be working from home to get this resolved.
Laura will also be working from home so you can reach back to either of us. We'll be looking forward to your email response.

Please acknowledge email receipt.

Best regards,

Tim Holmes
HOLMES & SWAFFORD CPAs
820 N. Thompson Lane, Suite 1E
Murfreesboro, TN 37129-4340
Phone 615.295.2782 Direct 615-869-7965

MTSU ACCOUNTING

A business email compromise example

- An employee received an email - supposedly from the CEO - that the company was set to acquire a Chinese company
- “CEO” instructed him to contact a lawyer at KPMG to help facilitate transfer of funds
- Employee transferred $17.2 million to a Shanghai bank account

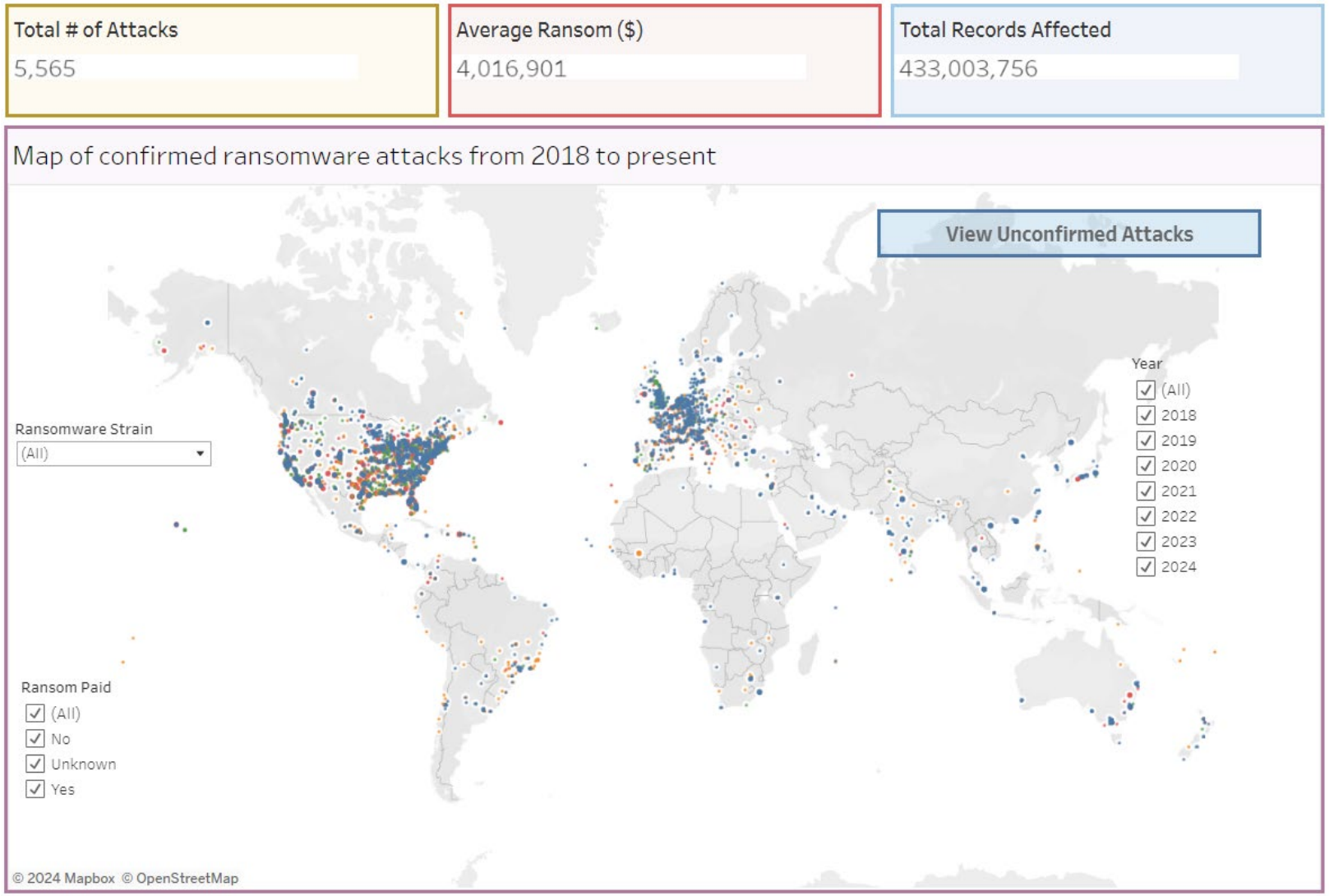
MTSU ACCOUNTING

Phishing for sale

- LabHost – sold phishing kits to cybercriminals for $249 USD per month
- Recently shut down due to global investigation
- Obtained 480,000 bank card numbers, 64,000 pin numbers, and over 1 million passwords

WHAT IS RANSOMWARE?

- Malicious software that encrypts data on a computer, making it unusable
- Cyber-criminal will hold data hostage until ransom is paid



MTSU ACCOUNTING

A ransomware example

- Murfreesboro Medical Clinic & Surgi Center (MMC) – physician-owned, multispecialty clinic
- Ransomware attack in April 2023 on over 250 GB of patient and employee data
- MMC refused to pay ransom & shut down for several days
- *"Your company has been a target. They may not have been successful, but I can almost assure you somebody's sneaking around the back doors trying to figure out ways in."*

  --- Joey Peay, CEO of MMC

MTSU ACCOUNTING

How to prevent frauds

Training & Education - ***Trust, but verify***

- Hang up the phone and call (or email) them back
- Use of code words
- Ask individual to turn their head to left and right
- Microsoft Defender XDR “Advanced Hunting”

MTSU ACCOUNTING

The red flags of fraud

- Sense of urgency
- Change in bank account with no prior notice
- Emails with misspellings and unusual domains and signatures
- Unnatural speech cadence, unusual blinking or movement, robotic tone, lip movements out of sync with speech

USING TECHNOLOGY TO DETECT FRAUD

MTSU ACCOUNTING

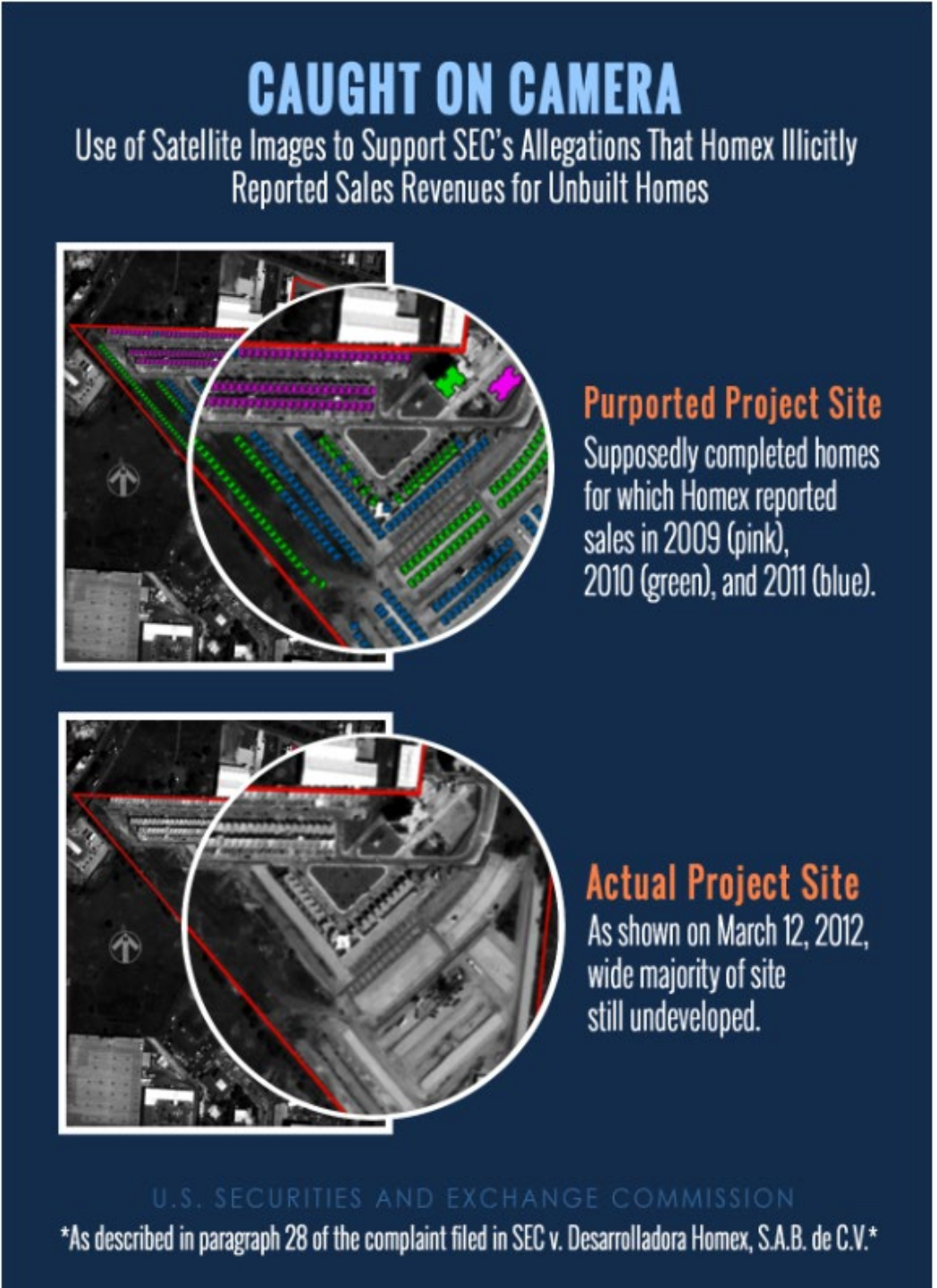
Some specific fraud detection methods

- Use of drones
- Artificial intelligence

USING DRONES TO DETECT INSURANCE FRAUD

- Fraudulent insurance claims for roof damage due to storms
- Insurance companies using drones used to inspect roofs before and after
- 20% increase in catching fraudulent claims
- Increasing safety, efficiency, and lowering costs

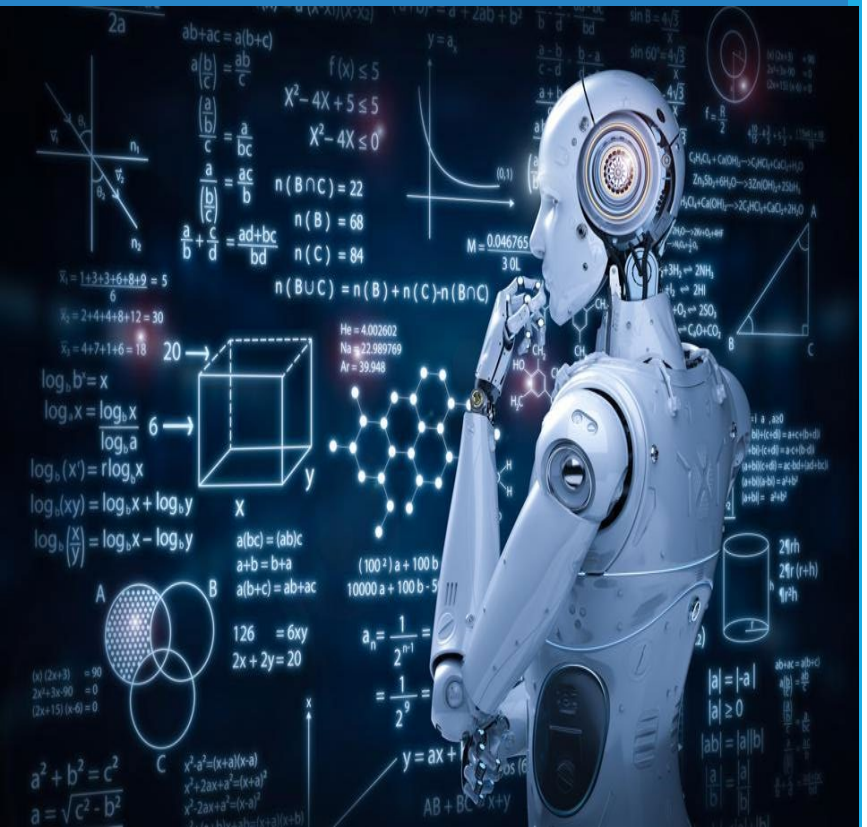
Source



- In 2017, the US SEC settled charges with Mexico-based homebuilding company Desarrolladora Homex S.A.B. de C.V.

- Over a 3-year period, the company reported fake sales of more than 100,000 homes and approximately $3.3 billion

ARTIFICIAL INTELLIGENCE



- AI – technology that enables a machine to simulate human behavior – e.g., Siri, Watson
- ACFE Technology Benchmarking Report – use of AI in anti-fraud programs expected to triple over the next 2 years

MTSU ACCOUNTING

Benefits of AI for fraud detection

- SPEED – algorithms can evaluate big data quickly, analyzing new data in real-time – analyze hundreds of thousands of transactions in seconds
- SCALABILTY – algorithm improves as the number of transactions increase
- ACCURACY – detect subtle patterns not obvious to human eye

MTSU ACCOUNTING

Examples of AI to detect fraud

- The U.S. Department of the Treasury use AI to identify check frauds – e.g., Social Security payments, tax refunds, etc. – via anomaly detection
- In 2023, recovered over $375 million USD in fraudulent payments

Source: https://home.treasury.gov/news/press-releases/jy2134

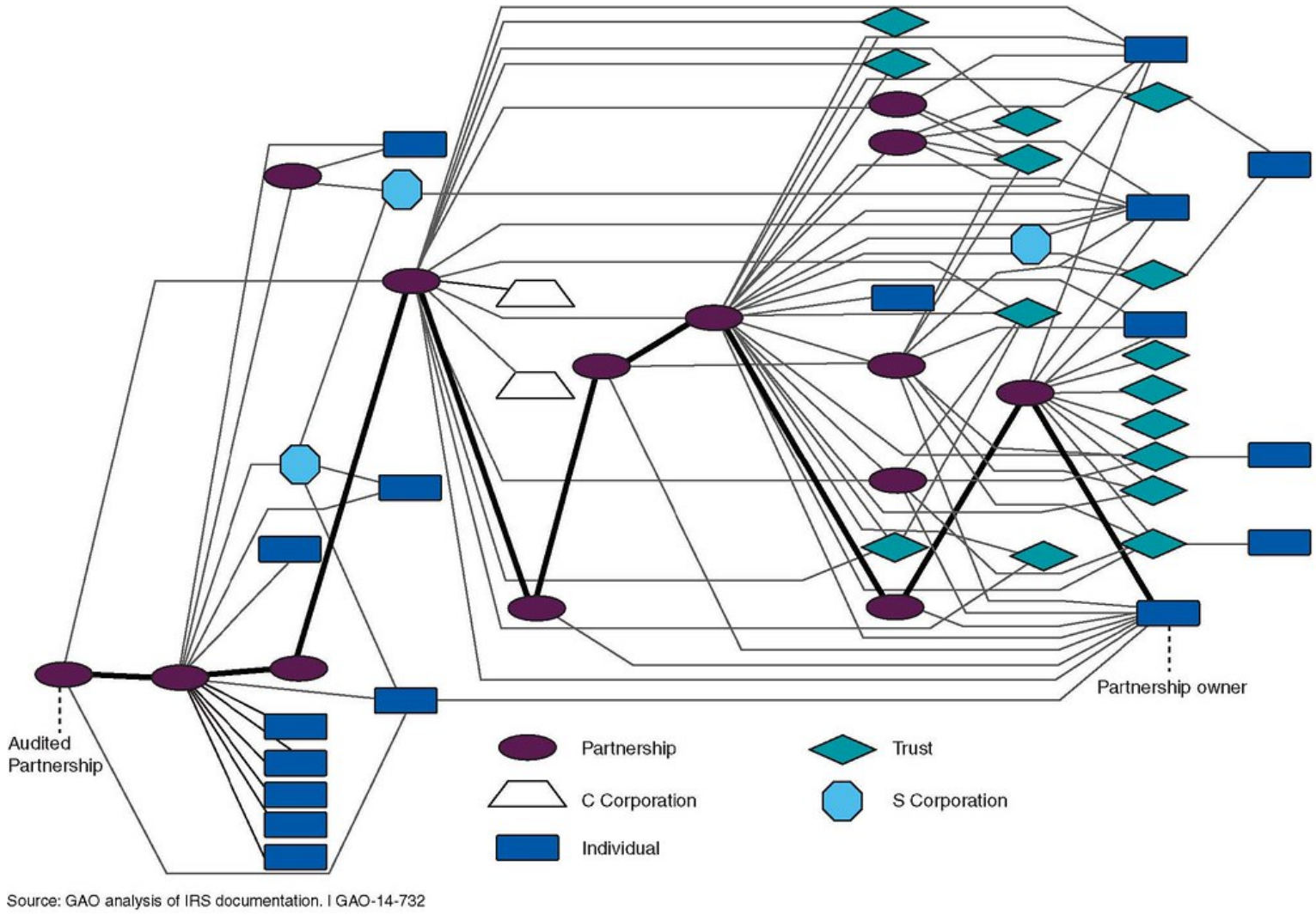
AI AND THE IRS

“The IRS is deploying new resources towards cutting-edge technology to improve our visibility on how the wealthy have gotten more creative on where they shield their income and focusing our staff attention on the areas of greatest abuse.”

“These new tools are helping us see patterns and trends that we could not see before.”

-- IRS Commissioner

Danny Werful



Source: GAO analysis of IRS documentation. I GAO-14-732

MTSU ACCOUNTING

AI to detect human behavior

- Israel-based Voicesense offers a Loan Default Predictor – uses AI to study vocal intonation, pace and emphasis
  - At a major Israeli bank – identified 306 people as high risk with 173 defaulting
- Lemonade – Insurance company requires customers making claims to upload a video explaining their loss – uses AI to identify non-verbal cues that may suggest fraud
- Converus – EyeDetect camera system identifies deception by measuring minute fluctuations in eye motion

Source: https://www.consumerreports.org/artificial-intelligence/how-companies-use-artificial-intelligence-to-detect-lying-a4041224738/

MTSU ACCOUNTING

Risks of AI

- BIAS – algorithms learn based on historical data
- ACCURACY – not always accurate at lie detection
- PRIVACY – legal rights to images

MTSU
ACCOUNTING

In conclusion……

- Technology creating big problems and big solutions related to fraud
- Critical to be aware of new fraud techniques and innovations for fraud detection
- Training and internal controls are key

Andrea.Kelton@mtsu.edu