A beacon of light in uncertain times.™

Fraud Futures: What's Next on the Horizon?

:Corporate Fraud in a Systemic, Digital World

Presentation to University of Dayton

By: Jack P Healey CPA,CFF,CFE,CRISC

November 17, 2025

BEAR HILL ADVISORY GROUP

OUR SPEAKER TODAY

Bear Hill Advisory Group is a boutique consulting firm with a decade of experience helping management teams and their boards understand their businesses better.

Through the BHAG Leadership Academy™ we use The Chaos to Confidence Framework™ to teach the 12 pillars to be mastered to become an operation-oriented CFO.

Jack P. Healey, CPA, CFF, CFE, CRISC
Chief Executive Officer, Bear Hill Advisory Group, LLC

Jack is an expert in operational, financial and organizational management, strategies, and tactics. He is an expert in risk management, including business risk, risk agility and resiliency, information security risk, and insider threat programs.

He is a Certified Fraud Examiner, Certified Public Accountant, Certified in Fraud and Forensics, Certified Information Systems Controls, Cybersecurity SOC, and Cybersecurity Services. He is a member of ACFE, InfraGard, ISACA , AICPA, RM, and NACD.

He authored the Business Crisis Diagnostic and Prevention Model™, which provides businesses with the framework necessary to identify impending business crises before they occur. He has authored or co-authored articles on Velocity of Risk™ and Customer Experience.

WHAT IF?

What if the next fraud wave isn't about stealing money, but about stealing identity, trust and reality itself?

Where are we? Where are we going?

Fraud Today- the occupational fraud risks you are already facing cyber breach, procurement fraud, insider manipulation

Fraud Tomorrow- the emerging threats on the horizon: quantum computing, ESG fraud, autonomous AI agents

Fraud as a Systemic Risk- how one breach can ripple across industries, governments and even societies

Fraud Today

- Cyber breaches & Insider threats

- Procurement & Supply Chain fraud

- AI-Malicious Data Injection, Cyber Attacks, Impersonations'

- Social Engineering- Business email compromise, Romance Scams and Elder Fraud

Case Study- Deep Fake CFO

McAfee™ Products Features Resources About Us AI Hub

<< Back to AI News

How Scammers Used Deepfake Video to Dupe a Company Out of Millions

- CFO held conference call with finance staff to wire $25 million in funds to several bank accounts
- During call one participant said something seemed a little wrong and looked to the group for validation- they saw nothing wrong
- Funds went through and were lost

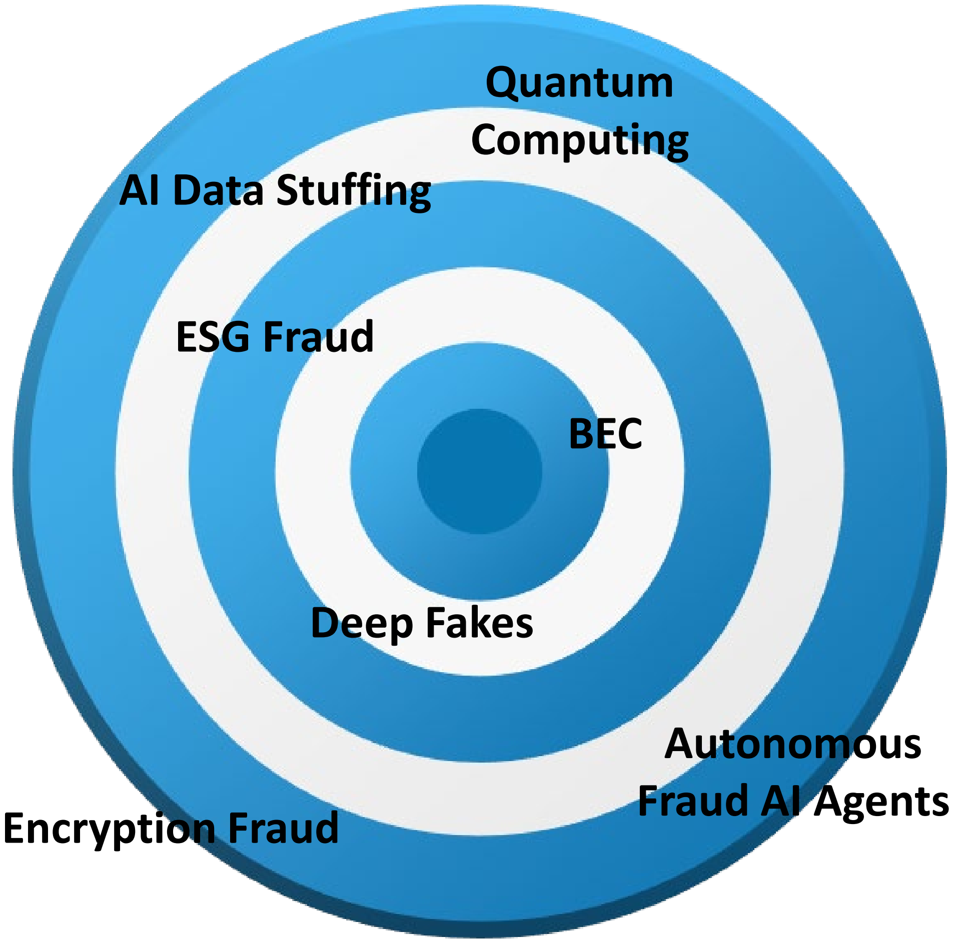
What Steps Could have been taken to prevent this fraud?

How certain are you that you could spot a deep fake?

Fraud of Tomorrow- Emerging Horizons

BEAR HILL ADVISORY GROUP

- Quantum computing and encryption fraud
- Autonomous AI fraud agents
- Biometric spoofing & medical data theft
- ESG & climate fraud (carbon credit scams)



What Black Swan Events 2035

- **AI-Generated CFO Launches a Ponzi Scheme**
- **Quantum Breach of Global Payment Rails**
- **Carbon Credit Collapse Triggers ESG Fraud Reckoning**
- **Autonomous AI Agents Commit Fraud Without Human Direction**

What is the Probability, Impact, Velocity, Detectability, Preventability?

Harm to People

- Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.
- Group/Community: Harm to a group such as discrimination against a population sub-group.
- Societal: Harm to democratic participation or educational access.

Harm to an Organization

- Harm to an organization's business operations.
- Harm to an organization from security breaches or monetary loss.
- Harm to an organization's reputation.

Harm to an Ecosystem

- Harm to interconnected and interdependent elements and resources.
- Harm to the global financial system, supply chain, or interrelated systems.
- Harm to natural resources, the environment, and planet.

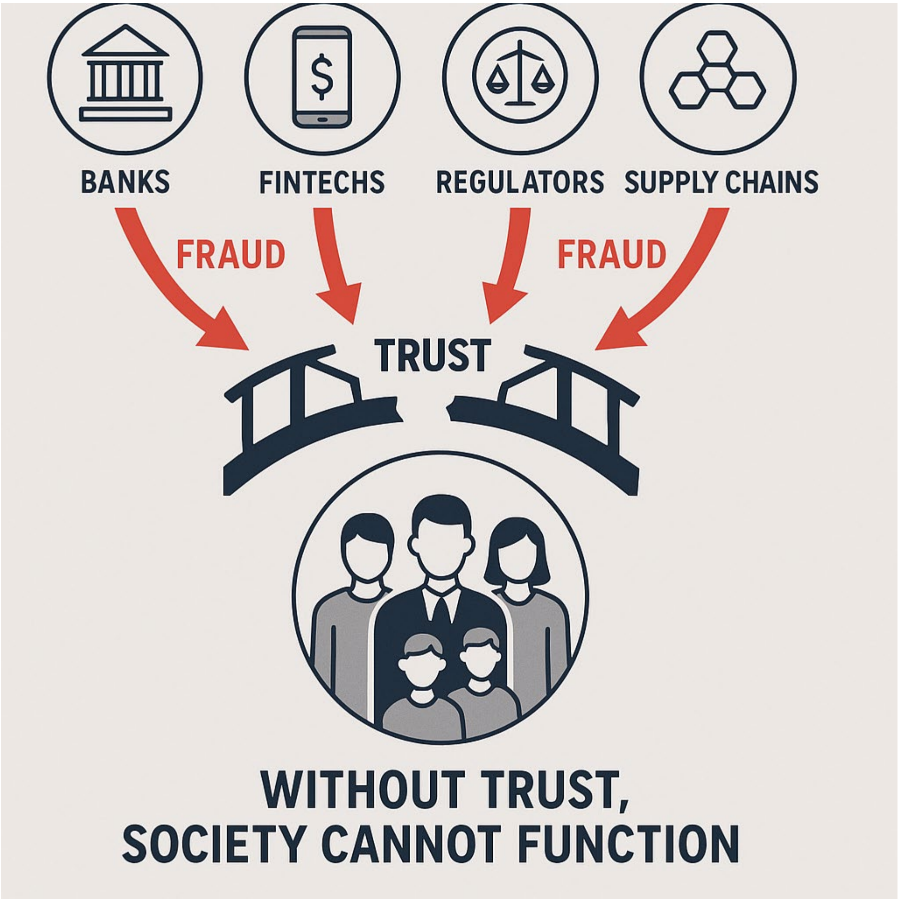
Fraud as Systemic Risk

Businesses are incorporating AI in every industry

Security frameworks and standards are not fully developed

This will result in an increase of fraud imbedded in the system

The frequency, severity and velocity of this risk will erode public confidence



Second Order Effect of Innovation and Fraud

Innovation	Direct Effect	Second Order Effect
AI & ML	Faster, smarter detection	Fraudsters use AI to evade; arms race escalates
Blockchain	Immutable records	New attack vectors (smart contracts, DeFi)
Biometrics	Stronger authentication	Privacy concerns, trust issues
Data Analytics	Predictive prevention	Data sharing risks, regulatory pressure

The Fraud Fighters Tool Kit

Understand your adversary-

- skills,
- motivation,
- resources,
- intentions,
- history and patterns,
- opportunities and constraints

Risk Assessments: grounded in reality

Critical Thinking: spotting weak signals

Cross-disciplinary awareness

Ethics & Empathy

WHAT DO YOU THINK?

BEAR HILL ADVISORY GROUP

Imagine it's 2035, which of the following fraud types will be the most disruptive to corporations, governments and society?

1. AI Driven Identity Fraud?
2. Quantum- Enabled Data Breaches?
3. ESG & Climate Fraud?
4. Autonomous AI Agents?
5. Biometric Spoofing & Medical Data Theft?
6. Supply Chain Manipulation?
7. Social Engineering- BEC, Elder Care Fraud?

Quantum Risk: The Collapse of Cryptographic Trust

- Quantum algorithms (e.g., Shor’s) can break RSA, ECC, and Diffie–Hellman encryption.
- “Harvest now, decrypt later” attacks already underway — sensitive data is being stockpiled.
- Digital signatures and certificates can be forged, enabling undetectable fraud.
- Blockchain and smart contracts vulnerable to quantum decryption.
- Post-quantum cryptography is emerging, but adoption is slow.

A beacon of light in uncertain times.™

Fraud in a Post-Quantum World

- Treasury systems compromised via quantum-enabled credential theft.
- AI models poisoned using quantum-generated adversarial inputs.
- Vendor payment rails intercepted through broken TLS encryption.
- Synthetic identities created using decrypted biometric data.
- Regulatory chaos as legacy systems fail to meet quantum resilience standards.

AI-Driven Identity Fraud: Trust in Crisis

BEAR HILL ADVISORY GROUP

Deepfakes and voice cloning enable impersonation of executives, vendors, and customers.

Synthetic identities bypass KYC and background checks using AI-generated documents and social profiles.

AI-powered phishing adapts in real time to user behavior and language.

Fraud rings use generative AI to scale scams across geographies and channels.

A beacon of light in uncertain times.™

AI Systems as Fraud Actors

Autonomous bots initiate transactions, manipulate data, or exploit system logic without human direction.

AI models trained on biased or adversarial data may commit fraud unintentionally.

Algorithmic trading and forecasting tools can be gamed to produce misleading outputs.

Lack of auditability in black-box models complicates detection and accountability.

Final Thought

Fraud is not just about <u>clever</u> schemes or <u>broken</u> controls. It's about <u>exploiting</u> the very fabric of <u>trust</u> that holds organizations, markets, and societies together

Questions and Contact Information

Jack P. Healey CFE, CPA/CFF, CRISC

CEO

Bear Hill Advisory Group

770.362.2008

JHEALEY@BHAGRP.COM

@CyberBizRescue

@BHAGRP

www.bhagrp.com

A beacon of light in uncertain times.™