Kevin Strenski – Nardello & Co.

Digital Asset Tracing – Foundational Principles for Fraud, Compliance, and Investigative Matters

The presentation outlines core principles of cryptocurrency and blockchain technology, explains foundational methods used to trace digital asset transactions, and demonstrates how these techniques are applied in real-world investigations through selected case studies. Attendees gain a practical understanding of how cryptocurrency operates, how transactions can be followed on public blockchains, and how blockchain forensics supports fraud examinations, compliance efforts, and investigative matters.

Learning Objectives include:

- Gaining a foundational understanding of cryptocurrencies, blockchains, wallets, and how digital assets function
- Understanding, at a high level, how cryptocurrency transactions are traced using blockchain analysis
- Identifying risks posed by cryptocurrency to financial institutions and other businesses
- Understanding the importance and investigative value of blockchain tracing and digital asset analysis

Senior Analyst Kevin Strenski has experience conducting blockchain analysis, digital asset tracing and attribution, net flow analysis, and cyber investigations. In previous roles as a contractor to the Department of Defense, Kevin led complex cryptocurrency investigations to assist various government agencies in identifying, tracking, and attributing hundreds of billions of dollars in illicit digital assets used to fund criminal activity by transnational organized crime syndicates, non-state actors, and others. The digital asset tracing team he established and managed disrupted complex money laundering networks and enabled the seizures of millions of dollars in digital assets. Kevin is an active member of the anti-money laundering community and is a Certified Anti-Money Laundering Specialist (CAMS). Kevin holds a BA in Russian Studies from Middlebury College and is fluent in Russian.

Claudia Ferguson – Microsoft

Securing AI – Notes from the Field

This session will share practical insights from real-world engagements on how organizations are securing AI-driven environments. As AI adoption accelerates, so do the fraud risks it introduces — from AI-powered deepfakes and social engineering scams to sensitive data exfiltration and insider threats enabled by generative AI tools. The session will cover key risks emerging with AI adoption, common security gaps observed across enterprises, and how threat actors are leveraging AI to scale fraud operations at unprecedented speed and sophistication. Attendees will learn actionable strategies using Microsoft security solutions such as Sentinel, Defender XDR, and Security Copilot to strengthen fraud detection, incident response, and data governance in AI-enabled environments.

What Attendees Will Learn:

1. **Identify how AI introduces new fraud attack vectors** — including deepfake impersonation, AI-generated phishing, prompt injection attacks, and sensitive data disclosure — and recognize the warning signs in enterprise environments.
2. **Evaluate the security gaps and common antipatterns** that leave organizations vulnerable to AI-enabled fraud, including neglecting data foundations, applying only traditional security controls to dynamic AI systems, and insufficient access governance.
3. **Apply a practical AI security framework** — encompassing Zero Trust principles, the OWASP Top 10 for LLM Applications, and regulatory compliance requirements (GDPR, EU AI Act, NIST AI RMF, ISO 42001) — to strengthen fraud prevention, detection, and response capabilities within their organizations.

Claudia Ferguson is a Senior Consultant at Microsoft with over 9 years of experience specializing in Azure Cloud and AI solutions. She has led complex IT transformation projects across diverse industries, guiding organizations through cloud adoption, security modernization, and AI integration. Claudia brings deep expertise in Microsoft Sentinel, Defender XDR, and Security Copilot, with a strong focus on operationalizing security for modern SOC environments. Her work spans the full project lifecycle—from strategic assessment to hands-on implementation—making her a trusted advisor for enterprise-scale security and cloud initiatives.

LinkedIn profile for reference: Claudia Ferguson | LinkedIn

Mike Richter - Microsoft

From Idea to Fraud Lab in Days: Vibe Coding an AI-Powered Expense Fraud Simulator with GitHub Copilot

Watch a full-stack fraud detection application get built in days — not months — through natural-language conversation with an AI coding agent. The app generates synthetic employee expense data, injects configurable fraud patterns (threshold-gaming, unusual frequency, vendor anomalies), runs ML-based anomaly detection, and hands ambiguous cases to an AI investigator on Microsoft Foundry for a structured verdict with rationale. Backend, frontend, cloud infrastructure, and AI integration — all conceived, designed, and coded by describing what fraud looks like to GitHub Copilot's agentic mode. You'll leave understanding how a small technical team armed with these tools can prototype and deploy fraud-modeling scenarios that previously took quarters of cross-functional development.

Learning Objectives:

1. Your fraud expertise is now the bottleneck — not software engineering.

2. AI doesn't replace the investigator — it gives you a second opinion at machine speed.

3. The Azure + Foundry platform turns a prototype into a production-grade tool your compliance team can accept.

Mike Richter is a Principal Partner Solutions Architect at Microsoft, where he works with strategic partners to design, build, and scale AI-powered solutions on Azure. With over two decades of experience in software development, architecture, and cloud transformation, Mike brings a practitioner’s perspective to helping organizations turn emerging technologies into real business impact.

He has led initiatives across application modernization, AI strategy, and partner innovation, and is passionate about translating complex topics into engaging, actionable insights. A frequent speaker and workshop facilitator, Mike is known for combining deep technical expertise with a practical, customer-first approach.

Yigal Rechtman – Rechtman Consulting

Collusion in Fraud: Detection Approaches

This presentation offers a deep dive into the mechanics of deceptive practices, starting with a comprehensive review of the **Fraud Triangle** and its foundational sub-triangles. We will examine the critical role of **collusion**, specifically how it bypasses traditional internal controls and complicates audit detection. Moving beyond theory, the session explores the psychological and environmental factors that lead to the creation of collusive networks. Finally, attendees will gain **practical tips** and red-flag indicators to help identify and mitigate the unique risks posed by multi-person fraud schemes.

Learning Objectives:

1. **Review fraud triangle** and the fraud triangle's sub-triangles
2. **Review collusion**, and understand how it affects fraud or audit detection
3. **Understand how collusion is created**.
4. **Explore practical tips** for identifying collusion.

Yigal Rechtman is a **CPA, CFE, CITP,** and **CISM** with professional experience in audit, accounting, and forensic and analytical work. His background includes applying analytical procedures in forensic accounting, audit planning, risk assessment, and review engagements, with a focus on translating auditing standards into practical, defensible audit documentation. Yigal works with audit teams on issues related to analytical procedures, professional judgment, and peer review readiness. He is the founder of **The CPA Publisher**, a national peer-reviewed publication whose tag line is "For CPAs, by CPAs™" and the motto is: **"You have knowledge. Your peers are listening."™.**

Rachel Cartwright – Supervisory Special Agent – Federal Bureau of Investigation

AI in Financial Crimes

The FBI's 2025 Internet Crime Report paints a grim picture of efforts to combat the global scam epidemic. Last year, reported losses to crypto-related scams topped $11 billion, with real losses thought to be significantly higher. Behind those eye-watering sums are sophisticated transnational scam rings who have industrialized fraud using digital assets, impacting victims around the globe.

Supervisory Special Agent Rachel Cartwright will discuss the FBI's investigatory efforts against scammers, deploying international takedowns and crypto seizures. SSA Cartwright will also discuss how trending Artificial Intelligence techniques are used by transnational crime syndicates to further fraud.

Attendees will learn about:

- Types of AI used in financial fraud
- Cryptocurrency Investment Fraud aka Pig Butchering Schemes
- Romance Scams

Supervisory Special Agent (SSA) Rachel A. Cartwright is assigned to the FBI's Bangkok LEGAT Office as an Acting Assistant Legal Attaché, supporting investigations with a nexus to scam compounds and transnational criminal organizations located in Southeast Asia.

SSA Cartwright began her career with the FBI in 2015. Following her training at the FBI Academy, SSA Cartwright was assigned to the New York Field Office (NYFO), where she joined a Special Operations Group tasked with covert surveillance and arrest operations.

In March of 2018, SSA Cartwright joined a Criminal squad tasked with investigating white-collar financial fraud. During this time, SSA Cartwright prosecuted numerous cases, including disrupting a criminal scheme actively attempting to defraud two U.S. based financial institutions of $100 million. SSA Cartwright also served as an Evidence Response Team (ERT) member for the NYFO, as well as a Legal Advisor.

In March of 2022, SSA Cartwright was promoted as the SSA of a Complex Financial Fraud Squad in the NYFO. SSA Cartwright oversaw investigations that involved international money laundering, investment fraud including cryptocurrency investment fraud schemes, and large-scale corporate embezzlement. During Agent Cartwright's tenure as a NYFO SSA, her squad

obtained a guilty plea and $2 billion fine pursuant to the DOJ's investigation into Danske Bank's Estonia based operations. SSA Cartwright's squad also prosecuted Miles Guo and others involved in a complex conspiracy to defraud thousands of victims out of over $1 billion dollars. SSA Cartwright participated in working groups in the NYFO area created to combat cryptocurrency scams. SSA Cartwright engaged in outreach educating the public on trending financial frauds, including cryptocurrency investment schemes.

In December of 2024, SSA Cartwright was promoted to Economic Crimes Unit of the FBI's Criminal Investigative Division, Financial Crimes Section. SSA Cartwright was responsible for overseeing FBI investigations related to complex financial fraud, securities and commodities fraud, corporate and investment fraud schemes, and intellectual property rights. In this role, SSA Cartwright worked closely with regulatory partners at the U.S. Securities and Exchange Commission (SEC), Commodities Future Trading Commission (CFTC), and other Federal, State and Local agencies.

SSA Cartwright earned Bachelor of Arts degrees in Journalism and Modern Languages/Spanish from Salve Regina University and a Juris Doctorate Degree from Hofstra University School of Law. Prior to joining the FBI, Agent Cartwright was a practicing attorney for seven years and served as Senior Corporation Counsel for the NYC Law Department.

Christina O. Gotsis

Managing Escalation Risk in Fraud Investigations

Fraud examiners are often the first to identify financial irregularities — but they are rarely the last to confront their consequences. What begins as a revenue recognition issue, related-party transaction, asset transfer, or internal control weakness can quickly escalate into criminal investigation, regulatory enforcement, civil litigation, or asset restraint. Escalation is often driven not solely by accounting standards, but by narrative framing, documentation choices, email tone, timing, and how findings are communicated internally. Through composite, real-world hypotheticals, this session examines how prosecutors, regulators, and civil litigants reinterpret financial findings under adversarial scrutiny and introduces a structured prevention framework designed to help fraud examiners stress-test reporting before finalization.

<u>Learning Objectives</u>

• Understand how prosecutors and regulators reinterpret conclusions to establish intent

• Examine parallel DOJ, SEC, and civil fraud risks that CFEs may not anticipate

• Identify privilege and documentation pitfalls that turn fraud examiners into witnesses

Christina Gotsis is a litigator representing clients in white collar matters, complex investigations, and high-stakes disputes where financial complexity drives risk, strategy, and outcome. She

advises individuals and companies facing allegations of fraud, financial misconduct, and parallel civil and criminal exposure. Christina also advises audit committees and boards of directors in internal investigations and corporate compliance matters, with a focus on identifying and remediating misconduct before it escalates into enforcement or litigation.

A Certified Public Accountant (CPA) and Certified Fraud Examiner (CFE), Christina bridges litigation strategy and financial investigation and mechanics, translating complex accounting issues, fund flows, and damages analyses into clear legal defenses. She frequently collaborates with forensic experts and financial professionals to develop defensible models and analyses that withstand scrutiny in litigation and support strategic objectives in criminal defense matters. Her work includes asset tracing and recovery across complex, cross-border financial structures, including representing the Trustee in the liquidation of Bernard L. Madoff Investment Securities.