New York Certified Fraud Examiners
Chapter #14

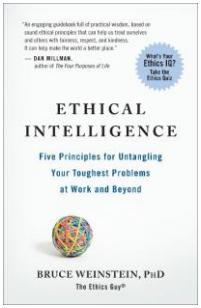
Fall Spring Conference
Friday, April 12, 2018
3 Times Square

THOMSON REUTERS®

KEYNOTE SPEAKER:
Dr. Bruce Weinstein
"The Ethics Guy"



Attendees will receive Dr. Weinstein's book, Ethical Intelligence, Five Principles for Untangling Your Toughest Problems at Work and Beyond.



"The Ethically Intelligent CFE: Five Powerful Principles for Making the Right Decisions Every Time"

What would you do? We'll look at five challenging scenarios that CFEs encounter professionally and personally. Each scenario will have four possible solutions with audience participation.

The five principles of ethical intelligence: Do No Harm, Make Things Better, Respect Others, Be Fair, and Care will be discussed, and a few small-group discussions will show how CFEs apply these principles in their work.

Learning Objectives:

By the end of "The Ethically Intelligent CFE," participants will be able to:

- Identify the five principles of ethical intelligence
- Explain how to prevent or solve the ethical problems they encounter by applying these principles consistently
- Incorporate the leadership insights from the concluding town hall Q&A into their daily work in fraud examination

Through his practical, engaging and entertaining presentations on ethical leadership, Forbes Contributor Bruce Weinstein, The Ethics Guy®, shows organizations how everyone benefits from honest, accountable behavior.

"Leaders around the world tell me that they can train people to be knowledgeable or skilled, but they can't train them to be honest," Bruce says. "I show companies why hiring high-character people is the single best way to achieve their strategic objectives. “

"Once you have high-character people on board," Bruce adds, "it's crucial to keep the organization's values front and center in everything you do. We all need reminders about how to think through the challenging ethical problems we face.”

He is the CEO of the Institute for High-Character Leadership and writes a leadership column five to seven times per month for Forbes.com.

Bruce has discussed ethical leadership over 200 times on national and international broadcast and cable television news programs.

Société Générale, Dublin-based construction company CRH, Northrop Grumman, the National Football League, RS&H, the Association of College and University Auditors, the National Association of College and University Business Officers, the Investment Management Consultants Association, Bristol Bay Native Corporation, Marathon Petroleum Corporation, Allstate Insurance, Astellas Pharma, the Western Australian Local Government Association and The Home Depot have been among Bruce’s many clients.

Bruce received his B.A. in philosophy from Swarthmore College and an M.A. and Ph.D. in philosophy with a concentration in bioethics from Georgetown University and the Kennedy Institute of Ethics. The W. K. Kellogg Foundation in Battle Creek, Michigan awarded Bruce a National Fellowship in Leadership Development.

He lives in New York City with his wife Kristen Bancroft, who is a compliance professional in the financial services industry and was a contestant on Jeopardy.

Sal Llanera
Founder
SL Data Management



Metadata and How it is used in Complex Investigations…" No Theories and Dull Definitions, Real World Examples!"

Mr. Llanera will go through real life examples on how metadata can be used to prove allegations of false email claims in business transaction, fake emails to execute a fraud and electronics document manipulation to benefit a fraudster. How to gather evidence in a forensically sound matter so nobody accuses you of evidence tampering. You will learn that fraudsters always leave a trail, you just need to know where to look. How to go about doing these investigations the right way so your allegations are supported by strong evidence.

Sal has over 25 years of experience in Forensic Technology (Computer Forensics, E-Discovery, and Forensic Data Mining & Analysis). He gets involved when computers are used in activities related to fraud, corruption, and misconduct. Sal's expertise is identifying hard to find electronic evidence relevant to his client's investigation or litigation. He has held executive positions with Ernst & Young and other top accounting/consulting firms in New York City supporting law firms in complex fraud and litigation assignments. At Ernst & Young, Sal ran the national data analytics practice for the Fraud Investigation and Dispute Services practice. Prior to his big four experience, Sal worked in private industry as an accounting/technology professional for several years. Sal has the ability to use his forensic technology expertise and accounting/business experience in concert to add value to assignments he is involved with.

Bret Hood
Former FBI Agent, Professor of Forensic Accounting
University of Maryland and Mt. St. Mary's University



"Why People Lie"

Do you wonder if there are ways to proactively address the fraudster's rationalization process? While many internal control systems focus on limiting opportunity, there are certain things that can be done to affect motivation and rationalization. In this session, you will learn about the latest scientific research on dishonesty as well as how to incorporate these findings into your internal control system.

Learning Objectives: participants will be able to:

- Explain how people are able to rationalize fraudulent behavior
- Develop internal controls that proactively address the fraud triangle prongs of motivation and rationalization
- Discuss the impact of morality on dishonesty
- Assess the impact of organizational culture on fraud
- Evaluate methods to create social norms as part of an internal control structure designed to prevent fraud

After serving 25 years as a Special Agent in the FBI, Michael "Bret" Hood became a member of the ACFE faculty as well as an adjunct professor of forensic accounting for the University of Virginia and Mt. St. Mary's University. During his tenure with the FBI, Bret worked many complex financial crime, money laundering, corruption and major cases such as the 9/11 terrorist attack, the HealthSouth fraud and the Maricopa Investments case.

Since 2000, Bret has been a master facilitator who has traveled the world teaching public and private sector employees how to develop effective anti-fraud, anti-bribery, anti-corruption and anti-money laundering programs. Bret has published articles in Fraud Magazine, Compliance and Ethics Professional magazine, and ACAMS Today.

Bret is a federal-court certified expert in money laundering and financial crimes. Bret is also the author of the critically acclaimed books, Eat More Ice Cream: A Succinct Leadership Lesson for Each Week of the Year & Get Off Your Horse! 52 Succinct Leadership Lessons from U.S. Presidents. Currently, Bret serves as an instructor, investigative consultant, and as an expert witness for 21st Century Learning & Consulting LLC (www.21puzzles.com).

New York City, FBI

"The FBI's Fight Against Fraud: Trends in Complex Financial Crimes, Securities Fraud, and Money Laundering "

Two FBI Special Agents will share on-the-ground experiences from the New York fraud scene. The Agents will describe emerging trends, past cases, and areas for growth in public/private partnerships. In this session, participants will learn how the FBI applies investigative tradecraft, multinational collaboration, and advanced analytical techniques to disrupt sophisticated international criminal and terrorist networks, while still keeping an eye on small time fraudsters. This discussion will highlight the importance of the FBI's collaborative and mutually beneficial relationship with the financial services industry and other private entities in the fight against the rapidly evolving financial crime threat landscape, comprised of numerous complex actors that threaten US National Security and the stability of the global financial system. This session will highlight challenges in identifying and preventing cross-border fraud and money laundering, while speaking to the critical capabilities and NY-based public/private efforts that can successfully counter these threats.

Mark Sullivan
Thomson Reuters,
CLEAR Investigative and Risk Solutions Regional Manager and
CLEAR Product Specialist



Mark Sullivan manages the Investigative and Risk solutions for Thomson Reuters in the mid-Atlantic and the North-East US. Going on his 13th year with Thomson Reuters Mark has been connected to the risk business for the greater part of his tenure and operates with a passion for data and investigative solutions. Mark is a recent transplant to Connecticut, an avid Green Bay Packers fan, and spends most of his time outside of work chasing his 4 small children.

"Top Tips for Conducting an Effective Online Investigation"

In this session, our panel of well-regarded subject matter experts will explore select elements of an effective compliance program and how an effective program can mitigate the risk of fraud. The session will start with a discussion of the prevalence of organizational misconduct, the severity of such misconduct and the difference that an effective program can make. This will be followed by specific topics for discussion, including whistle blower mechanisms, Qui Tam and False Claims Act cases, non-retaliation, regulatory and evaluative frameworks, responsive controls, including investigations and remediation. Topics for discussion, including whistle blower mechanisms, Qui Tam and False Claims Act cases, non-retaliation, regulatory and evaluative frameworks, responsive controls, including investigations and remediation.

Overview: Connections, Currency, Content, and Comprehension are all important components of an effective 'online' investigation. CLEAR from Thomson Reuters delivers all four of these pillars in solution with strong preference in local, state, and federal law enforcement as well as with corporate security professionals nationwide. Uncovering red flags through hidden, and unhidden, connections may be the difference between a successful and unsuccessful fraud investigation. Ensuring consistent access to current information versus data that may be weeks, months, or even years old increases the ability to create actionable insights in an investigation.
In many normal contexts duplication may seem to be a bad thing but during an investigation or scenario where monitoring is required, duplication and transparency across data sources minimizes the chances of an 'unturned stone.' Finally, without the ability to quickly comprehend, remediate false positives, and make meaningful decisions off of information returned, the advantages of sound monitoring/investigative procedures quickly diminish.
During this overview we will touch briefly on the history of Thomson Reuters in the investigative space and how TR can be an important partner in solving some of these key challenges.

Michael Schidlow
Financial Crime Risk Training
HSBC



"Leveraging Data Analytics to Detect Digital Money Laundering"

Only three years ago, online retail giant Amazon was completing as many as 398 transactions per second. Then in 2016, that number jumped up to an estimated 636 transactions per second. The volume of online retail transactions highlights the potential for money laundering. If even 10% of online transactions were illicit in some way, that would reflect tens of billions of dollars' worth of potential money laundering. This pervasive "digital laundering" has permeated all facets of our virtual lives, from video games to vacation rentals.

This session will define the terms and risks associated with digital or "ghost" laundering. Learners will be given the risk indicators associated with ghost laundering. Finally, this session will provide definitions and use-case examples of data analytics, as well as suggestions on how to leverage analytics to detect this type of threat.

Michael Schidlow currently directs the Financial Crime Risk Training program for HSBC Bank's Global Internal Audit Function. In this role, Schidlow designs and delivers bespoke training courses on anti-money laundering (AML), terrorist financing, anti-bribery/corruption (ABC), and anti-financial crime best practices across the company's global footprint. Schidlow also provides subject matter expertise on financial crime compliance, advising the function's North America and Latin America regions, as well as the Global Financial Crime Risk audit teams. Schidlow consults on audit planning and audit scoping based on regulatory issues, enforcement actions, and emerging risk conditions.

Schidlow previously served as an investigator for Bank of America's Global Financial Crimes Compliance division, specializing in high-profile client compromises, complex fraud, and insider abuse allegations. Schidlow started his career working as an attorney concentrating on regulatory compliance and white collar litigation matters.

Schidlow holds the Certified Fraud Examiner (CFE), Certified Anti-Money Laundering Specialist (CAMS), CAMS Advanced Certification in AML Audit (CAMS-Audit) certifications and is a licensed attorney.

Douglas Bienstock
Principle Consultant
Mandiant



"Navigating the Threat Landscape: Fraud, Extortion, and Espionage"

In this talk Mandiant will give an overview of the current threat landscape based on the past year of Incident Response Investigations. The talk will focus on three key types of intrusions that Mandiant has been investigation: Business Email Compromise or Fraud, Extortion, and Corporate Espionage. For each type of intrusion, we will explore the tools, tactics, and procedures of threat actors, review case studies, and discuss mitigations and remediations. Attendees will learn about how these different intrusions are typically executed, attacker motivations, and ways that organizations can better prepare themselves to defend against and recover from these types of intrusions.

Doug Bienstock is a Principal Consultant at Mandiant. His primary areas of expertise include incident response, digital forensics, network analysis, cloud computing, and red teaming. As a member of the Incident Response practice, Mr. Bienstock leads and participates in forensic analysis, live response analysis, and network monitoring for clients when a breach occurs. Mr. Bienstock also works with clients to assess the security of their internal and external networks through network assessment, red team assessments, and application assessments. His work has assisted companies both small and large, including several Fortune 500 companies.

Prior to joining Mandiant, Mr. Bienstock was at the MITRE Corporation researching next generation firewalls for government applications. Mr. Bienstock studied Computer Science at Columbia University, specializing in systems and security. While at Columbia, Mr. Bienstock was a member of the Columbia University Intrusion Detection Systems Lab. At the lab he assisted with research on Cisco IP phones, ultimately helping to identify and exploit a zero-day vulnerability. Mr. Bienstock is interested in the areas of cloud computing, federated authentication, and their cyber security implications. He has spoken on the topic of cloud computing and distributed authentication at the several cybersecurity conferences.