ACFE
Association of Certified Fraud Examiners

Chapitre français

Agile AI to the rescue of compliance and fraud risk management

Agile AI to the rescue of compliance and fraud risk management

Introduction

Fraud and compliance Modus Operandi are moving targets. Regulations are ever changing under political and geopolitical pressures. Organizations resist rapid change, and IT/legacy systems are costly and rigid. AI—especially agile AI—offers compliance and anti-fraud teams the necessary flexibility to adapt, measure fraud with analytics, detect fraud, and adhere to evolving regulations and fraud patterns.

Measuring Fraud with Analytics

- Fraud can be measured with appropriate resources and statistical methods.
- Traditional sampling has shown average fraud and error rates of ~6.5% of spend or analyzed population.
- AI will accelerate accurate fraud measurement, making the case for stronger investment.
- Shift from reactive detection of outliers to predictive analytics using vast data sets.

Fraud Detection & Modus Operandi

- Fraud evolves across regions, shaped by culture, regulation, and operations.
- AI helps identifying anomalies, outliers, collusion, and bid-rigging schemes.
- Data cleaning powered by AI is critical (garbage in = garbage out).
- Fraudsters also exploit AI (deepfakes, fake documents).
- Authenticity will be under constant threat and become a rare commodity.
- Blockchain and traceability tools may strengthen evidentiary reliability.

Adapting to Regulatory & Geopolitical Change

- Compliance is becoming too complex to manage without AI (e.g., sanctions post-Ukraine war, fast payment regulations in EU, latest EBA directives for AMLR).
- AI enables regulators and prosecutors to detect risks faster, often before traditional investigations.
- Organizations must anticipate that compliance evaluations will be increasingly data-driven.

AI in Compliance & Risk Management

- Compliance must evolve from documentation (reactive) to real-time monitoring and prediction (proactive).
- AI blurs the traditional boundaries between audit, fraud control, and compliance functions.
- The goal is not zero fraud but faster detection and mitigation before escalation.

Challenges & Risks

- Courts may resist purely AI-generated evidence without human oversight.
- AI can itself create risks (rogue bots, trading algorithms exploiting insider information).
- Organizations must establish accountability and governance over internal AI use.

Success Factors for AI Projects

- Many AI projects fail (MIT: 95% in corporate settings), but fraud/compliance can learn from these.
- Start with clear benchmarks: know baseline fraud/compliance levels before deploying AI.
- Focus on accessible data, motivated teams, and areas with low maturity for early wins.
- Ensure data quality: AI is only as good as the data it learns from.
- Adopt incremental, cost-effective, and well-structured approaches rather than over-ambitious ones.

Conclusion

- Fraud exists in every organization: admit it, measure it, and act on it.
- AI enhances fraud detection, compliance monitoring, and adaptation to regulations.
- Agile AI = adaptable AI: the key strength is flexibility in changing contexts.
- Evidence integrity and accountability mechanisms are essential.
- Organizations should pursue small, focused AI pilots to gain traction before scaling.

Verbatim

Mark Button

"People often say you can't measure fraud, but you can. With proper resources and methodology, organizations can quantify fraud losses... AI will make this measurement faster, more accurate, and transformative. That will be a game changer, unlocking resources and driving real investment in fraud prevention."

"The complexity of today's regulatory environment—whether sanctions after the Ukraine war or fast payment rules in Europe—makes compliance impossible without technology. AI isn't optional; it's the only viable option going forward."

Matt Galvin

"We live in an age where authenticity is under threat. Fraudsters are already using AI—deepfakes, fabricated documents, synthetic identities. Authenticity itself is becoming a currency, and organizations must be ready to defend it."

"Compliance has traditionally been about documenting that you tried to do the right thing—a legal defense. AI changes that. With real-time data and predictive analytics, compliance can finally shift from reactive to proactive."

Verbatim

Laurent Colombant

"Large language models (LLM) make possible what was impossible before—detecting pre-contract bid rigging, collusion, and fraud schemes buried in negotiation documents. But LLM won't find fraud on its own: context and expertise still matter."

"AI helps spot the outliers, but never forget— garbage in, garbage out. One of AI's greatest but overlooked powers is cleaning data for reliable fraud detection."

"To succeed with AI in fraud and compliance, start where maturity is low, risk is identified, data is accessible, and teams are motivated. Small, focused pilots are far more effective than overambitious projects."

Francis Hounnongandji

"Fraud schemes evolve by region, culture, and regulation. AI gives global organizations the agility to track shifting schemes and strengthen prevention and investigation in real time."

"As AI makes fraud detection smarter, it also makes falsified evidence easier. Our priority is safeguarding the integrity of proof so investigations remain reliable and admissible."

Matt Galvin

He currently is a partner with Steptoe LLP which focuses developing data-driven risk management systems and helps complex organizations design global compliance programs and lead cross-border investigations using technology.

Matt served as the first-ever Counsel for Compliance and Data Analytics at the Fraud Section, U.S. Department of Justice, where he:
• Evaluated corporate compliance programs in enforcement,
• Advised on Compliance
• Monitors and their oversight,
• Assessed post-resolution improvements,
• Identified, designed and developed analytics tools to assist prosecutors to identify and pursue white-collar crime,
• Built out an analytics function to generate criminal fraud cases and support investigations and trials.

Prior to that, Matt was Chief Compliance Officer at AB InBev, leading global compliance efforts of this Fortune 200 company across 80+ countries. He also practiced for over ten years with leading international law firms.

Matt is a New York and Hong Kong qualified lawyer. He has held positions with Massachusetts Institute of Technology, Harvard Business School, Sorbonne Law School and Fordham Law.

mgalvin@steptoe.com

Mark Button

Mark is the Director of the Centre for Cybercrime and Economic Crime at the School of Criminology and Criminal Justice, University of Portsmouth.
He conducts research on a wide range of areas for bodies that include the Home Office, National Fraud Authority, EPSRC, Sentencing Council, Cifas, Midlands Fraud Forum, Crowe Clark Whitehill to name some.
He also has an interest in private policing, security management and the regulation of it and has been involved in helping to develop the standards for this for the United Nations Office for Drugs and Crime.
He joined the University of Portsmouth in 1997. He was Associate Head (Curriculum) of the department between 2004-2012.
His research interests began with private policing with an interest in non-state contributions to policing. This led him to fraud where this is largely the case. Along that journey he has developed interests in Counter fraud, Cyber-frauds, Computer misuse, Fraud measurement, Security management, Private security regulation amongst others.

mark.button@port.ac.uk

Laurent Colombant

Laurent has been helping financial institutions, commercial entities and governments tackle financial crime using NLP, machine learning and analytics since 1998. He has worked on sanctions screening, anti-money laundering, internal and external payment fraud as well as terrorist financing. He currently focuses on payment integrity which includes optimizing sanction filters and procure to pay process from supplier integrity (ESG), to maverick spend, to travel and entertainment fraud.

Prior to joining FortiComply Laurent worked for SAS Institute as a solution lead and for Cognitive Systems Europe (Temenos) as general manager of a team specialized in scanning and STP repair of SWIFT messages.

He holds an MBA in Finance from the University of Michigan and a joint degree in linguistics, econometrics and computing from the University of Montreal.

laurent.colombant@forticomply.com

Francis Hounnongandji

Francis, CFA, CFE, is a corporate governance and anti-fraud expert and financial advisor with deep expertise in data science, predictive analytics, artificial intelligence, machine learning, and emerging digital technologies.

He brings more than 25 years of international experience with global corporations, audit and advisory firms, and government institutions, and has conducted assignments in over 30 jurisdictions across Europe, the Americas, Asia-Pacific, Africa, and the Middle East. His work spans advisory and research in corporate governance, internal controls, fraud risk management, financial investigations, anti-money-laundering, financial advisory, and business and corporate strategy.

His commentary and editorials have appeared in leading international newspapers, including the *Financial Times*, *The New York Times*, *Le Monde* and *Les Echos*. He serves as President of the Institut Français de Prévention de la Fraude (IFPF) and of the ACFE France Chapter. He is editor and co-author of *Histoires ordinaires de fraudes* (Eyrolles Editions d'Organisation).

fh@ifpf.fr

CERTIFIED FRAUD EXAMINER

Become Certified Fraud Examiner®

The CFE is "in-demand...one of the most marketable credentials today".

Robert Half International

www.ifpf.fr

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS · CFE ·

ifpf INSTITUT FRANÇAIS DE PRÉVENTION DE LA FRAUDE