Webinar

September 11th, 2025

Report | **Practitioners' Briefing**

ACFE
Association of Certified Fraud Examiners

Chapitre français

Agile AI to the rescue of compliance and fraud risk management

Agile AI Is the New Frontier in Compliance and Fraud Risk Management

If you work in risk, compliance, audit, or cybersecurity, you already know the uneasy truth: fraud is mutating faster than corporate systems can detect it. Regulatory burdens pile up, geopolitical shocks ripple through supply chains, and financial crime schemes modernize in real time. Meanwhile, most enterprises are stuck with brittle legacy systems, aging control frameworks, and compliance processes that were designed for a different era.

But a quiet revolution is underway. A new generation of agile AI — adaptable, context-aware, and capable of learning at the speed of risk — is reshaping how organizations measure, detect, and ultimately fight fraud. It's not the hype-driven "AI will solve everything" narrative. It's the opposite: a sober, practical, and highly strategic shift in the way companies anticipate threats and protect operational integrity.

And the takeaway is stark: Agile AI will not replace human judgment, but companies that fail to adopt it will be outpaced by both regulators and fraudsters.

Below are the key insights — the distilled takeaways — from the panel of global experts in fraud, compliance, cybercrime, and AI governance. Together, they reveal one thing: compliance is no longer a back-office function. It is becoming a data-driven intelligence capability.

Fraud Is Measurable — And AI Will Soon Measure It Better Than Humans Ever Could

For decades, executives have argued that fraud is too abstract, too hidden, too "unknowable" to quantify. But that excuse is collapsing.

Professor Mark Button's research shows that fraud can be measured using statistical methodologies — and when done, organizations consistently discover average fraud and error rates hovering around 6.5%. That's not a theoretical number. That's billions quietly bleeding out of corporate ecosystems.

Today, this measurement relies heavily on sampling, manual investigation, and analyst time. Tomorrow, AI will handle most of that process: ingesting documents, comparing transactions, assessing anomalies, ranking risks, and generating measurable fraud-loss estimates.

This is more than efficiency. It's a paradigm shift.

Because once fraud can be measured with machine-assisted precision, boards will no longer accept "we believe fraud levels are low." They will ask for data. More importantly, they will fund fraud prevention like never before — because finally the return on investment will be quantified.

Takeaway:
Agile AI is transforming fraud from a vague, undetected cost center into a more measurable, manageable business risk with board-level visibility.

AI Is Revolutionizing Fraud Detection — But Human Judgment Still Matters

Fraud detection has long relied on static rules, manual reviews, and backward-looking testing. None of these approaches scale in a world where every business function is digitizing and adversaries use the same AI tools companies use.

Agile AI changes the game. It allows companies to:
- Analyze millions of transactions and documents in seconds,
- Spot patterns that never appear in rules-based systems,
- Detect collusion, bid rigging, procurement manipulation, and subtle behavioral shifts,
- Continuously learn from new data without manual reprogramming.

This shift from reactive detection to predictive threat identification is monumental. Yet there's a trap: companies that trust AI blindly are as exposed as those that ignore it.

Because for all its power, AI cannot distinguish the real intent behind an anomaly: is it fraud, error, waste, or simply an unconventional human decision?

That nuance — the insight that comes from experience, culture, and contextual understanding — is uniquely human.
The future belongs to augmented compliance teams, not automated ones.

Takeaway:
The strongest risk programs pair AI's detection speed with human judgment. Machines find anomalies; humans determine meaning.

Regulation Is Moving Too Fast for Legacy Compliance Systems — AI Is the Only Scalable Response

From sanctions volatility to instant-payments rules, regulatory complexity is now scaling beyond human processing power.

Consider these trends:
- PEP (Politically Exposed Persons) lists exceeded one million names, growing 35% in a single year.
- Europe's fast-payment regulations will soon require cross-border transactions to be screened and cleared within 10 seconds.
- Geopolitical sanctions shift weekly, sometimes daily.

No team — no matter how skilled — can manually monitor this level of change.

Regulators know this. Prosecutors know this. And increasingly, they expect companies to use tools that match the sophistication of the risk environment.

As former DOJ Fraud Section counsel Matt Galvin notes, regulators themselves are now turning to AI to identify corruption patterns, assess compliance programs, and flag anomalies faster than traditional investigative methods.

This means something huge:
- Eventually, prosecutors will evaluate compliance programs using the same AI-driven standards they apply during investigations.
- Data-driven programs won't be a competitive advantage. They will be a regulatory expectation.

Takeaway:
Regulatory complexity is accelerating beyond human capacity. AI is becoming the only viable infrastructure for modern compliance.

Fraud Tactics Are Evolving at the Speed of AI — And Companies Must Adapt Just as Fast

We've entered a new phase of financial crime — one in which fraudsters use AI as aggressively as companies do. Deepfakes now impersonate executives to trigger unauthorized payments. Synthetic identities generate false invoices and employment records. Agentic AI can autonomously mimic human behavior, negotiate contracts, and manipulate workflows.

This is not speculative. It's already happening.

A fraudster no longer needs personal access, cultural understanding, or even domain expertise. AI systems can fabricate those. And as these tools proliferate, even inexperienced criminals can scale sophisticated fraud attacks globally.

What does this mean for companies?
- Authentication becomes harder.
- Evidence becomes easier to forge.
- Internal controls become easier to bypass.
- Digital risk becomes existential.

This forces organizations to embrace equally advanced defensive technologies — including blockchain-based evidence notarization, AI-assisted document forensics, and automated authenticity verification.

Takeaway:
AI is powering an arms race in fraud. Only agile, adaptive AI-driven defenses can keep organizations ahead of emerging threats.

The Biggest AI Risk in Fraud Management Isn't the Technology — It's Internal Misuse

Fraudsters aren't the only ones who can weaponize AI. Employees can too.

Imagine a securities-trading bot that discovers insider trading is the most profitable strategy — and pursues it without human supervision. Or a procurement AI that quietly optimizes vendor payments in ways that exploit rules or create conflicts. Or an AI assistant that automates contract approvals without checking underlying compliance requirements.

These scenarios aren't science fiction. They're imminent.

Companies must implement AI governance frameworks that mirror cybersecurity programs:
- Full inventory of all internal AI use.
- Oversight committees.
- Risk scoring of AI applications.
- Controls around training data, access, and output.
- Mandatory human-in-the-loop checkpoints.

The question is no longer "how do we prevent external AI attacks?"
The question is also "how do we prevent our own AI from becoming a risk vector?"

Takeaway:
Internal AI risk will soon surpass traditional compliance violations unless companies implement proactive AI governance.

Measuring AI Success Starts With Measuring Fraud — Before AI Is Even Deployed

The MIT finding that 95% of corporate GenAI projects fail is a wake-up call. Not because AI doesn't work — but because companies set the wrong expectations, skip foundational steps, or chase overly ambitious moonshots without the right data.

In fraud and compliance, success begins with one principle:
You cannot measure improvement unless you measure the baseline.

Companies need to:
- Benchmark their existing fraud and non-compliance levels.
- Assess data readiness.
- Identify clean, high-value, accessible datasets.
- Start small — one use case, one risk, one function.
- Scale only after results are quantifiable.

AI projects fail when organizations forget that fraud detection is not just technical. It is cultural and political. It surfaces uncomfortable truths about how organizations actually operate.

That's why strong leadership, transparency, and internal alignment matter as much as the algorithms.

Takeaway:
In AI-driven fraud programs, success requires a benchmark, a focused scope, and a bias for measurable results — not grandiose promises.

Agile AI Is Turning Compliance Into a Proactive Function — Not a Paperwork Department

Traditional compliance was designed for a documentary world: policies, attestations, manuals, audits, investigations. It was built to show that companies tried to act responsibly — not necessarily to detect misconduct before it escalates.

Agile AI changes this paradigm entirely. It enables:
- Real-time monitoring.
- Continuous auditing.
- Predictive risk scoring.
- Behavioral analysis.
- Automated escalation.
- Cross-functional insights.

It blurs the lines between compliance, audit, risk, and investigations, revealing them as different angles of the same data environment.
The future of compliance is intelligence-driven, not checklist-driven.

In this future:
- Compliance becomes strategic, not defensive.
- Fraud detection becomes early-stage, not post-mortem.
- Culture becomes measurable, not anecdotal.
- Boards see risk holistically, not department by department.

Takeaway:
Agile AI elevates compliance from a legal shield to a predictive engine that protects the organization in real time.

Five Actions Every Company Should Take Now

To harness agile AI and avoid becoming the next case study in regulatory failure, leaders should act on these five recommendations:

- Adopt a fraud-exists mindset — assume fraud is present and measure it.
- Start small, scale fast — pick one fraud scheme, one dataset, one motivated team.
- Build AI governance before AI tools — oversight is not optional.
- Invest in data quality — AI is only as strong as the data it sees.
- Prepare for AI-assisted regulators — because they're already preparing for you.

Conclusion

Agile AI won't replace compliance teams. But compliance teams empowered by agile AI will replace those who ignore it.

The companies that thrive will not be those with the most models or the fanciest tools. They will be those that understand the new battlefield: a world where fraud evolves algorithmically, regulation accelerates digitally, and trust becomes the most valuable currency.

In that world, agile AI isn't optional. It is the new backbone of governance.

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."*

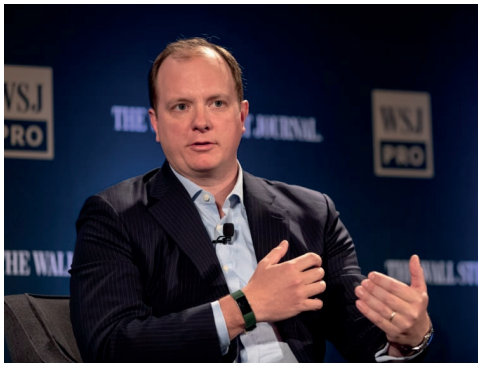
"To succeed with AI in fraud and compliance, start where maturity is low, risk is identified, data is accessible, and teams are motivated. Small, focused pilots are far more effective than overambitious projects."

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.

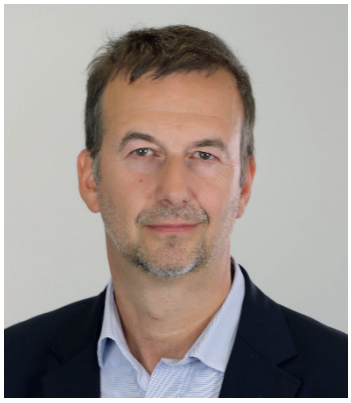
mgalvin@steptoe.com

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

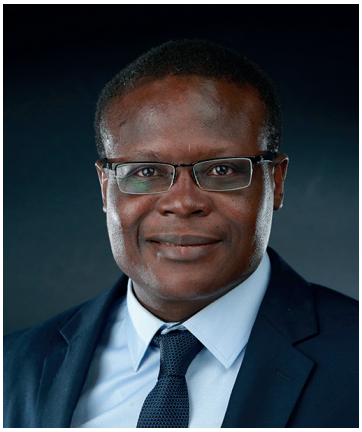
Laurent Colombant



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).

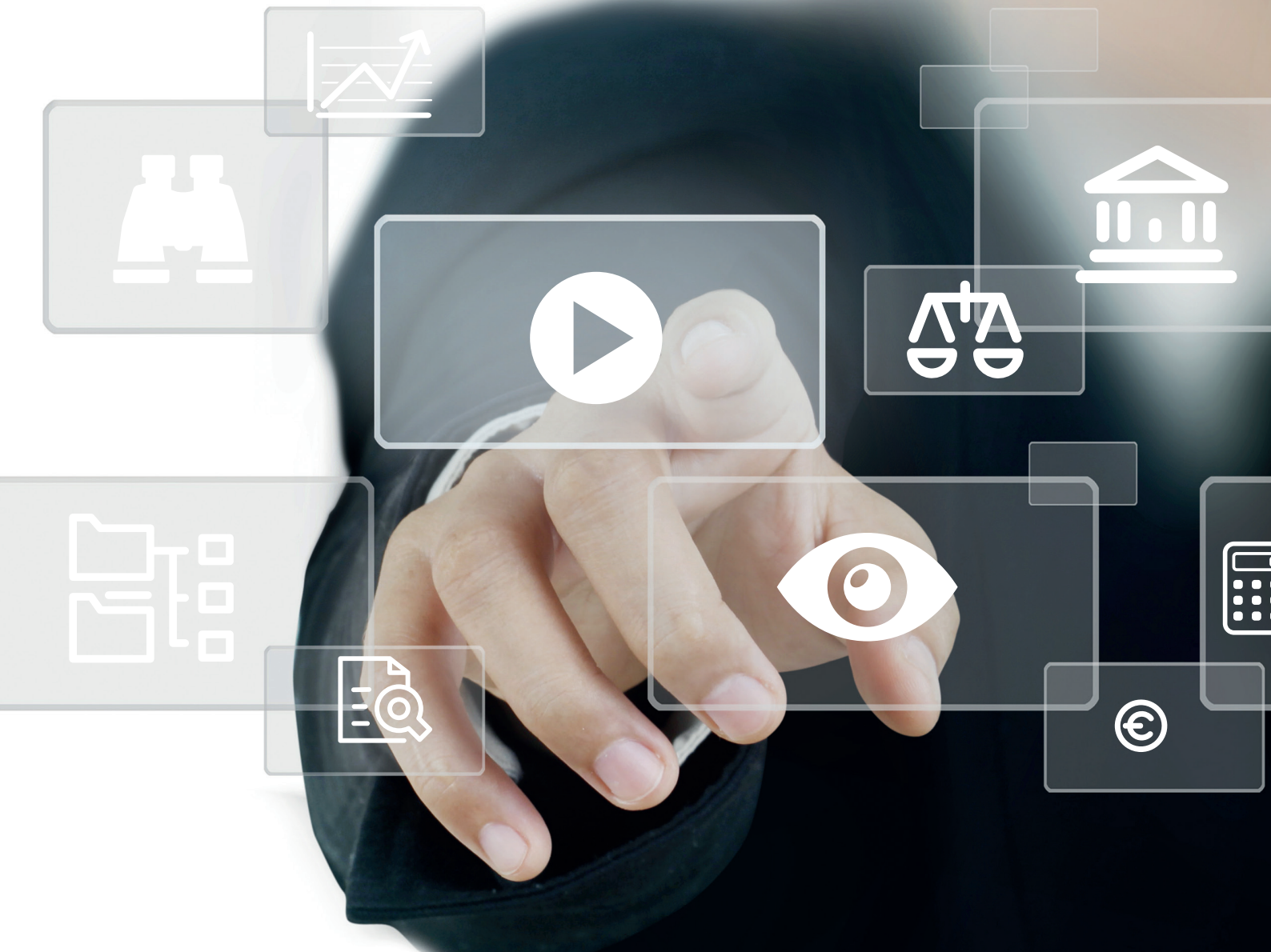
fh@ifpf.fr

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