

AI IN FINANCIAL CRIME: DETECTION FIRST, BUT THE GAME CHANGER IS BIGGER

Financial Crime Studio - Zurich, 24 September 2026. In conversation with Jean Voigt, Head of AI at IMTF. Written by Oonagh van den Berg, CEO, Virtual Risk Solutions.

Jean Voigt's route into AI ran through fifteen years in AML and compliance roles at global tier-one firms - and it shows. Asked where AI delivers the greatest value today - detection, investigation, or decision-making - the head of AI at IMTF did not hedge for a second.

Detection first: hunting criminals through the data

"I have to admit, my heart is with the detection - being a computer scientist by heart. Detection is the most exciting: hunting for criminals through the data. For compliance officers, I believe it is agentic AI as it allows for far easier and far faster ways to look into large amounts of data sources, to correlate suspects quicker, more reliably, and ultimately make better decisions. In the immediate - say six to twelve months - this is where the highest value is."

Beyond detection, he sees real promise in cross-institution data sharing - but only once the industry standardises the data side of that cooperation. is own position on the classic 'single source of truth' debate has evolved:



"I used to believe in one source of truth, and over the years I have re-educated myself. We can have similar data sets that are used in different ways - but it is understanding the utilization of that data, and how it is used."

Why agentic AI changes the investigation

On the investigation bottleneck, Jean's argument is that institutions are working on stale ground - and that this, not detection, is where agentic AI lands hardest:

"A lot of the data that the investigation is performed on currently is yesterday's data. The beautiful aspect about the agentic AI tools is real-time analysis - and

after today's analysis, the system keeps working. Should a new network or a new connection be identified in a UBO structure, that will be flagged. That is something we just don't have today."

Risk management, not risk avoidance

Asked how institutions can make better use of the intelligence they already hold, the conversation turned to the silo problem - KYC, AML and fraud teams that never speak - and to what compliance is actually for:

"If we do compliance just to tick boxes, that doesn't help anyone – great compliance should enable informed business decisions. It is risk management, not risk avoidance."

On the industry's habit of mistaking process for control, he was blunt:

"There is now technology that allows us to do more. Just following the process and ticking the box is no longer sufficient."

The criminals have a plan B, C, and D

On preparing for increasingly sophisticated AI-enabled criminal activity, Jean framed the asymmetry plainly:

"Being bound by regulation, we are taking slower steps to AI adoption - and there is a fear factor in innovation, a fear factor to change, which is human nature. But the criminals are using not just the same tools we use today, but much more advanced tools. And they have a plan B, a plan C, a plan D. Should plan A be identified, they are already moving on. They are innovating continuously."

The same asymmetry plays out in trade finance, where he argued that only a small fraction of trade funding flows through regulated parties - leaving a systemic risk that a regulated minority is asked to control.

The stablecoin warning

Closing on how money now moves, the conversation landed on stablecoins - with Nigeria's retail economy as the case study of an entire country moving faster than its banks:

"Stablecoins inherently concern me because they can move things fast, which benefits criminals more than it benefits regular users. It removes the correspondent banking controls that we have spent years trying to build. And very importantly, it is creating a shadow banking system."

