

SIBOS 2025: AI IS HERE TO STAY

Last week, the Plenitude team attended Sibos 2025 in Frankfurt, where the central theme revolved around the transformative opportunities of technological innovation in payments. Across panels and discussions, one message was clear: AI is no longer a future trend, it is already here: reshaping compliance, operations, and customer expectations.

Given the nature of the conference, we focused on AI Assurance within our broader Financial Crime Compliance (FCC) expertise. Our In AI We Trust approach reflects how institutions can adopt AI responsibly: ensuring data quality, governance, and explainability so that technology strengthens trust rather than undermines it.

What follows are reflections on the discussions that matter for the financial services industry at a pivotal time of transformation: how embracing change stands to help firms better balance compliance and innovation, streamline operations, and deliver a trusted customer experience in a fast-evolving landscape.



IN AI WE TRUST

POWERED BY **Plenitude**

BALANCING COMPLIANCE AND INNOVATION

The backdrop to Sibos was an **industry under pressure**:

- Escalating threats: criminals are industrialising AI, scaling fraud-as-a-service, and generating synthetic identities at marginal cost.
- Rising compliance burden: global compliance spend has passed \$206bn, with over £34bn in the UK alone. Yet most of this is absorbed by manual processes and outdated systems, while effectiveness lags.
- An unsustainable gap: with 90–95% of AML alerts still false positives, teams face alert fatigue and boards warn the trajectory cannot continue.

This tension was captured across Sibos panels. Financial Crime Compliance: An End-to-End Journey showcased how Swift's FCC and Fraud suite can embed predictive analytics, anomaly detection, and sanctions testing into every stage of the payments lifecycle: a model for how compliance can move from cost centre to enabler.

Our session, In AI We Trust – Reimagining the Role of AI in FCC, with **Louise Brett** and **Dr. Stratis Limnios**, explored how AI is already in use, and how continued adoption stands to help firms close the gap between innovation and regulation.

- Today's reality: AI is already in use for transaction monitoring, sanctions screening, adverse media scanning, and network analytics.
- Operational realities and constraints: weak data quality, high false positives, costly governance, and inconsistent global regulatory expectations.
- Future possibilities: AI copilots that cut through analyst noise, "digital deputies" surfacing forward-looking insights, synthetic data to stress-test systems before criminals do, and real-time assurance frameworks to satisfy regulators.

“AI should be the autopilot, but human judgment must remain in the cockpit.”

The same message resonated in More Human – AI as a Strategic Leadership Tool in a Machine-Augmented FCC World, where **Alan Paterson** and **Mark Humphries** demonstrated how leaders are already experimenting with “digital twins”: AI agents trained on their values and experience to test decisions, surface blind spots, and amplify capacity.

The lesson for compliance:

Just as leaders use AI to sharpen judgment, FCC teams must embed AI to scale oversight. Compliance that clings to manual processes will fall further behind “smart crime.” Compliance that embraces AI with assurance can rebalance the playing field

STREAMLINING OPERATIONS



If compliance is to close the gap, **operations must transform.** The numbers tell the story: nearly 80% of compliance costs remain tied to manual intervention. This is neither efficient nor sustainable.

At Sibos, firms demonstrated what change looks like:

- Swift showed how automation can support detection and remediation from initiation through settlement.
- In their In Frontier Firm: AI in Fraud and AML panel, Microsoft framed three waves of AI adoption in fraud/AML:
 - a. Assistants like copilots unifying data for analysts.
 - b. Human-led agents that detect deepfakes and support investigations.
 - c. Agent-operated systems executing workflows under oversight.
- In From Concept to Catalyst: Agentic AI’s Real-World Impact on FinCrime Operations, audience polling revealed widespread adoption: the majority of firms are already using generative AI, machine learning, or agentic AI in compliance.

The appetite is clear. But as **Louise Brett** emphasised, AI must be an “assistive layer”, not a replacement. Reducing false positives, cutting through alert fatigue, and freeing analysts for higher-value tasks are only sustainable if supported by robust governance.

The challenge is not whether AI can deliver efficiency:
it can
The challenge is whether firms can embed assurance frameworks fast enough to make those efficiencies resilient and regulator ready.

ENHANCING THE CUSTOMER EXPERIENCE

If Sibos reinforced one message, it was that technology must ultimately serve the **end customer**. Innovation in compliance and operations only matters if it results in faster, safer, and more trusted experiences.

This was emphasised from the outset. In the Opening Plenary, Deutsche Bank CEO **Christian Sewing** noted that technological change is not optional if firms want to keep customers “front and centre.”

Panels throughout the week showed how this principle plays out in practice:

- **Data as the foundation:** Swift’s focus on data quality and transparency in correspondent banking demonstrated how cleaner, standardised information directly reduces friction in cross-border payments. This isn’t just operational streamlining: it means fewer delays, lower costs, and greater reliability for end users.
- **Compliance as customer value:** In In AI We Trust – Reimagining the Role of AI in FCC, panellists reframed compliance innovation as a client benefit: fewer errors, faster turnaround times, and staff freed from administrative overhead to focus on genuine customer relationships.
- **Hybrid customer service models:** In one session, **Tammy Martin** (NatWest) described how agentic AI can support front-line staff by overseeing multiple customer queries simultaneously. This speeds up response times but keeps humans in the loop, ensuring that efficiency never comes at the cost of empathy.

The broader message from Sibos was that customers want more than speed. They want **confidence** that their transactions are safe, that their data is protected, and that if something goes wrong, accountability is clear. AI can help deliver this, but only if firms approach adoption responsibly, with transparency and governance that are as visible to clients as they are to regulators.

Customer trust is the ultimate measure of whether AI in compliance succeeds. Firms that embed explainability and human oversight into client-facing processes will not only reduce friction, but also build the deeper trust and loyalty that will define competitive advantage in the next era of financial services.

FINAL THOUGHTS

Sibos 2025 underlined a simple truth: AI is here to stay. But the week also exposed the industry's dilemma: criminals are scaling AI faster than regulated institutions, while compliance costs rise linearly and effectiveness stagnates.

The discussions pointed to a different path: one where AI, when deployed responsibly, strengthens both compliance and customer trust:

- Evidence of success: firms already report reductions of up to 60% in false positives and significantly higher true-positive detection where AI is embedded with governance.
- Compliance redefined: no longer a regulatory burden, but a strategic enabler of resilience and efficiency.
- Trust as the foundation: explainability, data quality, and assurance frameworks are what allow regulators, boards, and customers to believe in the systems being deployed.



What needs to happen now:

- For the industry: collaborate on standards, liability frameworks, and data-sharing to build collective resilience against financial crime.
- For firms: invest in data, embed governance, and design AI with assurance from day one.
- For leaders: use AI as a multiplier of judgment and foresight, not a substitute.
- For Plenitude: we will continue to bring together FCC expertise and AI assurance, helping clients defend margins, strengthen resilience, and sustain trust in an AI-driven future.

The next frontier of finance will not be defined by who adopts AI fastest, but by who adopts it responsibly, explicably, and with trust at the core.

ABOUT PLENITUDE

Plenitude provides market-leading Financial Crime Compliance (FCC) advisory, transformation, technology, data analytics, and managed services. We are committed to building a secure and resilient financial system, safeguarding society, and empowering our clients to meet and exceed their regulatory obligations.

ABOUT THE AUTHORS

Klara Belle Barnes is a Senior Consultant with 6 years' experience in Financial Crime Compliance, covering KYC, AML Advisory, and investigations across insurance, banking, asset management, and fintech. She has advised major global banks and regulators, conducted Section 166 reviews, and holds both a Certified Fraud Examiner (CFE) credential and an ICA Diploma in AML.

Imogen Cronin is a Consultant with over 3 years' experience in regulatory analysis and obligations management for financial institutions. At Plenitude, she leads the Regulatory Intelligence team, supporting clients and RegSight with FCC obligations management, horizon scanning, and regulatory gap-analysis.

