

Why Digital Trust Is Becoming FinTech's New Growth Engine

As financial fraud grows more sophisticated, FinFusion's Verafye argues that digital trust must evolve from one-time verification to continuous, connected intelligence across identity, behaviour, transactions, and risk signals. The company believes the future of FinTech security lies in explainable, real-time investigation intelligence that balances seamless customer experiences with stronger fraud, AML, and compliance controls.

Puja Sharma,

Assistant Editor, IBS Intelligence



Abhishek Tuppada is the Co-Founder and CEO of [FinFusion Solutions](#), the company behind Verafye, an AI-driven investigation intelligence platform for regulated financial institutions. Verafye helps institutions manage fraud, AML, compliance, and digital trust operations by connecting identity, transaction, behavioural, and network signals into a unified investigation view. The platform is designed to support faster investigations, improve operational efficiency, reduce false positives, and enhance explainability across risk and compliance workflows.

How do you see the role of identity verification evolving in FinTech over the next five years?

Identity verification is moving from a one-time onboarding checkpoint to a continuous digital trust capability. Earlier, institutions verified a customer at the start and relied on periodic checks. That is no longer enough. Over the next five years, verification will need to consider identity, behavior, device signals, transaction patterns, beneficiary relationships, and risk context across the customer lifecycle. The goal is not to add friction everywhere, but to apply the right intelligence at the right moment. For FinTechs, trust has to become dynamic, explainable, and embedded into operations.

What are the biggest challenges FinTech startups face in balancing innovation with compliance and security expectations?

The biggest challenge is speed with accountability. FinTech startups are expected to launch quickly, serve customers digitally, expand into new segments, and keep the experience seamless. At the same time, regulators, banking partners, investors, and customers expect strong controls from day one. Many startups treat compliance as something to add later, but that creates operational debt. A stronger approach is to build fraud, AML, security, auditability, and governance into the operating model early. Compliance should not be seen as a brake on innovation. Done well, it becomes a trust infrastructure for responsible scale.



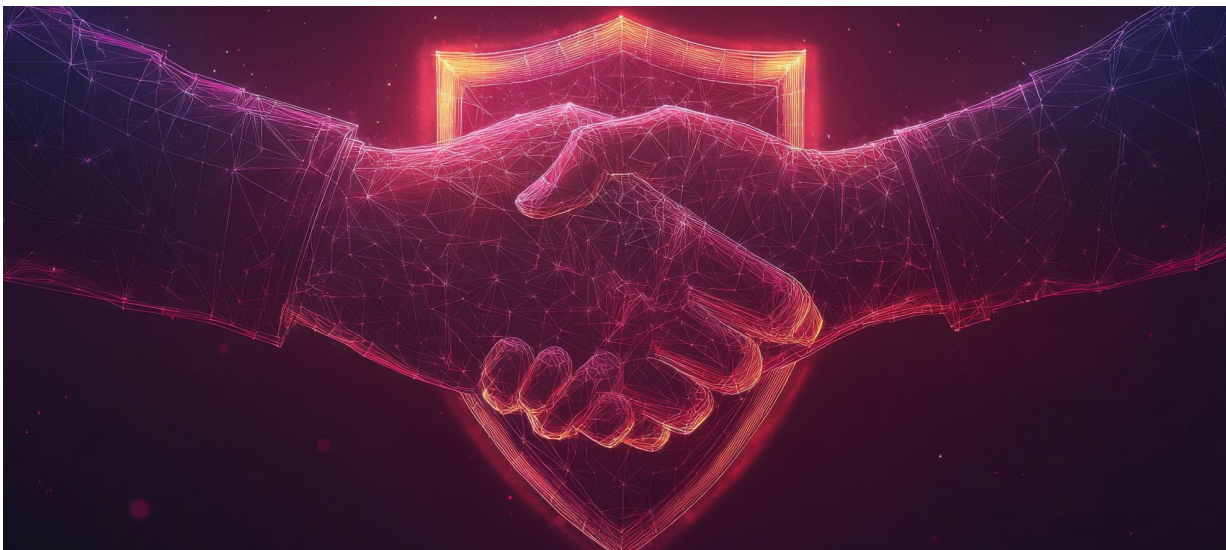
**Abhishek Tuppada, Co-Founder and CEO,
FinFusion Solutions**

What emerging trends in fraud prevention and digital security should startups prepare for today?

Startups should prepare for fraud that is faster, more coordinated, and harder to detect through isolated rules. Mule networks, synthetic identities, account takeover, social engineering-led scams, real-time payment fraud, and AI-assisted attacks are becoming more sophisticated. The key shift is that these risks cannot be understood in isolation. A suspicious onboarding pattern, a mule account, and an unusual transaction may be part of the same network. The next phase of fraud prevention will depend on connected intelligence across transactions, identity, behavior, devices, relationships, and case history.

In what ways can FinTech companies leverage technology to enhance customer confidence and trust in digital transactions?

Customer confidence comes from invisible protection and visible accountability. Customers want transactions to be fast and seamless,



“The future of fraud prevention is not more alerts, but better context behind every decision.”

but they also expect their institution to protect them when something looks unusual. Technology can enable intelligent friction, where genuine customers are not slowed down unnecessarily while risky activity receives deeper review. It can also help internal teams understand why a case was flagged, which signals mattered, and what action was taken. Faster resolution, fewer unnecessary blocks, clearer communication, and consistent decisions all contribute to trust.

Many institutions already have fraud, AML, onboarding, and monitoring tools. Where do you see the real gap today?

The real gap is not always the absence of tools. It is the absence of a connected context. Most institutions already have fraud systems, AML systems, onboarding checks, transaction monitoring tools, and customer databases. But these often sit across different systems and teams. Analysts spend valuable time collecting information before making a decision. This leads to alert fatigue, inconsistent investigations, and slower case closure. The market is moving from pure detection to investigation intelligence. Institutions need to understand what matters, who is behind the alert, how activities are connected, and what decision can be made confidently.

How does FinFusion’s Verafye approach to digital trust and verification differ from more traditional verification models?

Traditional verification models are often point-in-time and document-centric. They answer whether a person or business appears genuine at onboarding. FinFusion’s Verafye looks at digital trust more continuously. Our approach is to connect fraud, AML, transaction,

identity, device, behavioural, and network signals into a unified investigation view. Instead of treating every alert as a separate event, Verafye helps teams understand the broader entity, relationship, and risk context behind it. We do not position Verafye as just another detection tool. It is an investigation intelligence layer that helps lean risk and compliance teams move from alerts to decisions with better speed, consistency, and explainability.

How do your solutions help improve customer experience while also reducing risk for financial institutions?

The best risk systems should protect the institution without punishing genuine customers. FinFusion’s Verafye supports this by helping teams separate real risk from noise. When investigators have better context, they can avoid unnecessary escalation, reduce false positives, and resolve cases faster. For customers, this means fewer avoidable interruptions and a smoother experience. For institutions, it means better use of analyst capacity, more consistent decisioning, and stronger operational control. Our aim is not to create more alerts. The aim is to make existing signals more useful, connected, and actionable.

How do you envision the future of secure and seamless financial transactions, and what role do you see FinFusion’s Verafye playing in that ecosystem?

The future of secure transactions will be real-time, connected, and explainable. Customers will expect speed, but institutions will need the intelligence to understand risk instantly and act responsibly. We believe digital trust will become continuous rather than episodic, and fraud, AML, identity, and compliance operations will become more connected. Through Verafye, FinFusion aims to help institutions and FinTech platforms build that connective layer - where alerts become context, context becomes decisions, and decisions become auditable outcomes. Our ambition is to make investigation intelligence accessible to lean teams that need enterprise-grade confidence without enterprise-heavy complexity.