Managing Risk — Insights

Identity and Trust are Becoming the Platform

Written by Archer McFall and Rob Wilkes

5 Min Read | March 23, 2026

Executive Summary

AI-driven fraud is pushing identity and trust into the core of how software and financial platforms operate. As experiences consolidate into fewer digital entry points, organizations are moving from one-time authentication to continuous verification using behavioral signals and real-time risk scoring. The shift requires clear ownership, cross-functional accountability, and trust metrics tied to business outcomes like conversion, retention, loss, and support load.

Artificial intelligence is accelerating innovation across software and financial services. It is also accelerating something else. Fraud.

Deepfakes, synthetic identities, and AI-driven social engineering are moving faster than traditional security approaches were designed to handle. In parallel, digital experiences continue to consolidate into fewer entry points, mobile apps, super-apps, embedded finance flows, and self-service platforms where a single weak authentication moment can cascade into real financial loss and reputational damage.

The result is a structural shift. Identity and trust are becoming a platform layer.

The Trust Problem is No Longer a Security Problem

For years, many organizations treated identity as a technical control and security as a gate at the perimeter. That model breaks down in a world where users interact across channels, credentials are compromised at scale, and fraud becomes adaptive.

In modern software and FinTech environments, trust has become a core product requirement. It lives inside the customer experience. It shows up in how users onboard, how they recover access, how they move money, and how they prove who they are in real time.

When identity systems fail, it is rarely contained to security outcomes alone. It impacts customer experience, conversion, retention, and brand credibility. It also forces operational load onto support teams and back-office functions.

AI Changes the Economics of Verification

AI agents now make fraud cheaper, faster, and more scalable. A convincing voice clone, a synthetic identity profile, or a targeted phishing sequence can be generated and iterated quickly. As attack sophistication increases, organizations have to assume that static credentials, simple knowledge checks, and one-time verifications will underperform.

This is why the best organizations are shifting from authentication to continuous verification. They rely more on behavioral signals, device intelligence, and real-time risk scoring. They build dynamic, non-uniform step-up authentication and design identity flows that reduce friction for trusted users while increasing controls where risk rises.

Trust Becomes an Architectural Decision

This shift also changes where identity and trust sit in the operating model. Organizations are beginning to treat identity as a reusable platform, not a set of one-off tools embedded within individual products. That platform includes engineering, fraud operations, risk, and compliance working together with shared accountability.

In FinTech, the stakes are obvious, especially as real-time payments and embedded finance expand. When money can move instantly, prevention has to happen instantly. In software, the same shift is unfolding as more products integrate payments, wallets, and financial services layers.

Many software platforms now sit close to financial transactions, even if they are not banks.

As industry lines blur, trust becomes the connective tissue that keeps ecosystems functional.

What This Means for Leadership and Talent

Organizations are beginning to look for a different kind of leader. They need executives who can bridge product, engineering, and risk. They need leaders who understand identity and trust as a platform that supports growth, not as a defensive function that slows it down.

This also creates new operating demands. Teams must align around shared metrics that connect fraud prevention and customer experience. They must define how risk is managed across channels. They must decide where identity logic is centralized and where it is embedded.

For many leadership teams, the hardest part is not buying tools. It is designing the system.

Three Moves Leaders Should Make Now

1. **Treat identity and trust as a named platform with clear ownership.** Define a single accountable leader and align engineering, risk, and fraud operations around shared outcomes.
2. **Build continuous verification into core journeys.** Move beyond one-time authentication toward real-time risk scoring, behavioral signals, and dynamic step-up controls that preserve experience while protecting the system.
3. **Align trust metrics with business metrics.** Connect fraud outcomes and identity friction to conversion, retention, loss rates, and support load. Trust needs operational visibility that leaders can manage, not only technical reporting.

Trust used to be assumed. In a world shaped by AI-driven fraud and embedded financial ecosystems, trust has to be engineered. The organizations that build identity and trust as a platform will protect customers, strengthen experiences, and create an advantage that is hard to copy.

Archer McFall
Senior Partner
(770) 757 9156
amcfall@modernexec.com

Rob Wilkes
Senior Partner
(646) 203 7484
rwilkes@modernexec.com

Modern Executive Solutions™

Modern helps clients build future-ready organizations through integrated solutions spanning Executive Search, Leadership Advisory, Organizational Strategy, and Executive Communities. We help the world's boldest leaders and most influential organizations define the future, not follow it. Let us know how we can help.

Stay updated with insights at www.modernexecutivesolutions.com