# THE DEEPFAKE SUMMIT

September 1, 2026 | Washington, DC

EVENT INTELLIGENCE REPORT · KEY FINDINGS

# Top 10 Takeaways

## Building Trust Infrastructure for the AI Economy

The primary constraint on digital trust is no longer the availability of detection technology. It is the lifecycle coverage, governance, and enterprise velocity required to deploy these capabilities effectively.

## THE OPERATING REALITY

**55–60%**
of online traffic is already non-human[1]

**$6–$8**
price of a synthetic identity on dark-web marketplaces[2]

**23%**
of new bank accounts reported fraudulent in one widely cited study[3]

**15–20%**
of some institutions' portfolios may contain synthetic identities[4]

**$3.7B**
in recorded global deepfake fraud losses through H1 2026[5]

**18–36 mo**
for a large bank to onboard a new technology vendor[6]

## Where Trust Fails

### 1 The Attack Surface Is the Full Identity Lifecycle—Account Recovery Is the Weakest Link

Help desks, device changes, and fallback flows often accept weaker evidence than enrollment. Recovery must be treated as a first-class, high-risk identity event.

### 2 Deepfakes Target Judgment—and the Liar's Dividend Erodes Trust Itself

AI compresses deception cycles from months to moments. Once anything can be faked, genuine evidence can be dismissed. Defending Mind Sovereignty™ requires trained verification habits alongside technical controls.

### 3 Identity Alone Is Not Trust

Knowing who someone is does not establish that the device, behavior, content, or delegated AI agent should be trusted. The model itself must change.

ACCESS → IDENTITY → **TRUST**

## How Trust Must Be Built

### 4 Foundational Identity Must Anchor a Closed Circle of Identity[7]

Onboarding, binding, authentication, and recovery should run as one loop anchored to a biometric-linked human identity, with fallback to it whenever risk spikes. Attackers exploit the OTP, SMS, and password seams.

### 5 Data and Organizational Silos Are Security Defects—Telemetry Without Governance Is Noise

Lifecycle-spanning attacks are invisible to fragmented monitoring. Link data, ownership, risks, and controls in an identity/knowledge graph, and turn policy into code.

### 6 Privacy Is a Fraud-Resilience Measure, Not Merely a Compliance Obligation

Excess collection and centralized storage expand the attack surface. Data minimization, selective disclosure, and reusable credentials preserve assurance while reducing exposure.

### 7 Real-World Testing Beats Lab Claims—Model Cards, Bake-Offs & Independent Rallies

Honest model cards with standardized metrics, adversarial operational testing, buyer bake-offs, and programs like DHS's RIVR. Independent testing belongs in every RFP.

## What Comes Next

### 8 Agents Need Mandates, Not Just Identities

Every agent needs an explicit, time-bound, scoped mandate separated from its human principal, shadow-tested before production, with humans retained on legally consequential outcomes.

### 9 The Trust Velocity Gap Is the Defining Enterprise Risk

Threats evolve at AI speed; institutions adopt at enterprise speed. Closing the gap means accelerating procurement, budgeting, and governance, and evolving silos into cross-functional networks.

### 10 Trust Infrastructure Is Built Before the Crisis

Cross-sector relationships must exist before they are tested. Deployable standards beat theoretical completeness, digital credentials are scaling (mDLs in 23 U.S. jurisdictions), and education is infrastructure.

SUMMIT OBSERVATION

**"Trust is designed. It is not assumed. The technologies will evolve. The threats will evolve with them. Our responsibility will not."**

EXECUTIVE CONCLUSION

Trust infrastructure is not a product category; it is an operating capability that continuously establishes, challenges, and re-establishes confidence in identity, authority, authenticity, and interaction integrity as conditions change.

Sources & Notes: [1] [2] Deepfake Summit DC Fireside Conversation: Overcoming Obsolete Threat Models, citing 2025 estimates. [3] Deepfake Summit DC Dialogue, participant citing an onboarding-fraud study. [4] Participant estimates, Deepfake Summit DC. [5] Surfshark Research, July 2026. [6] Deepfake Summit DC Leadership Keynote. [7] The Circle of Identity framework was developed by Frances Zelazny. Takeaways summarized from The Deepfake Summit Event Intelligence Report, September 2026.

**Read the full Event Intelligence Report**

www.thedeepfakesummit.com

Next Summit: September 2027 · Washington, DC

THE PRISM PROJECT

ACUITY MARKET INTELLIGENCE

© 2026 Acuity Market Intelligence. All rights reserved. The Deepfake Summit is an initiative of Acuity Market Intelligence and The Prism Project.