Retica Technologies

Building the future of identity infrastructure with combinational biometrics

Retica offering memorandum

August 2025

https://www.retica.io | jon@retica.io

The story: Ethical account hijack across digital and physical worlds

In July 2025, we used a recycled phone number to access someone’s Amazon and Meta accounts. By enrolling my own biometrics (e.g., face, fingerprint, palm, and voice), I assumed their digital and physical identity. OAuth2 connections (e.g., “Sign in with Facebook”) triggered a cascade of over a dozen additional account takeovers.

37M
phone numbers recycled annually in the U.S.[1]

7.2B
smartphones in use globally (2025)[2]

$12.5B+
in U.S. identity theft losses (2024)[3]

The problem: Current access systems rely on single-biometric, siloed enrollment processes that fail to cryptographically bind identity across platforms.

[1] *In the matter of advanced methods to target and eliminate unlawful robocalls: Second notice of inquiry* (FCC 17-90). (2017). Federal Communications Commission. https://docs.fcc.gov/public/attachments/FCC-17-90A1.pdf.
[2] Statista. (2023, November 16). *Forecast number of mobile users worldwide 2020-2025*. https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/.
[3] *New FTC data show a big jump in reported losses to fraud to $12.5 billion in 2024*. (2025, March 10). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

The problem: Fragmented identity infrastructure and inefficient access

What’s wrong with current security models?

- **Recycled identifiers** (phone numbers, emails) reused for login and registration
- **Unrestricted changes** to email/phone on file, often without safeguards
- **Device-based multi-factor authentication** and **fallback options** introduce vulnerabilities
- **Magic links** and password resets bypass robust authentication
- **OAuth2** (e.g., “Sign in with Facebook”) undermines zero-trust principles
- **Single-biometric systems** lack cross-platform identity binding
- **Biometric data** stored in isolated silos (cloud or local) without cryptographic linkage to identity

Where and why current solutions fall short

Apple Face ID

- Siloed biometric enrollment
- Isolated local storage environment
- Single-biometric solutions

Amazon One

- Siloed biometric enrollment
- Isolated cloud storage environment
- Single-biometric solutions

Google Passkeys

- Siloed biometric enrollment
- Isolated local storage environment
- Single-biometric solutions

Microsoft

- Siloed biometric enrollment and biometric file storage
- Isolated local storage environment

The solution: Combinational biometrics + distributed architecture (1/2)

1. **Unified biometric profile**
   - Retica fuses multiple biometric modalities into a single cryptographic identity
   - Not linked to email, phone, or device; uniquely tied to you
2. **Cross-ecosystem identity resolution**
   - Enables platforms to recognize users across ecosystems
   - Prevents duplicate accounts and supports benefit portability
3. **Privacy-preserving interoperability**
   - Zero-knowledge proofs verify identity without exposing sensitive data
   - Essential for compliance and user trust

The solution: Combinational biometrics + distributed architecture (2/2)

4. **Decentralized data + MPC**
   - Biometric data is fragmented and distributed across cloud and local nodes
   - Removes single points of failure and insider risk
5. **Temporal audit + subscription intelligence**
   - Biometric code chain logs immutable subscription and access events

Result:

Cryptographic identity binding with enhanced security, preserved privacy, and effortless user interaction: just a touch or gesture

Why hasn’t someone else done this already? (1/3)

- *What do Microsoft, Apple, Google, and Amazon* have in common? (1/2)*
    - **Platform-centric identity models**
        - Identity systems serve their own ecosystems
        - Anchored to accounts, not people
    - **Fragmented modalities and siloes**
        - Each uses different biometric standards
        - No cross-platform identity binding; users appear as different people across services
    - **Privacy and regulatory constraints**
        - Centralized identity raises privacy concerns and faces compliance hurdles
        - Existing systems store identity data on devices or in proprietary clouds
        - No company has built a privacy-preserving, decentralized identity infrastructure that meets global standards

* Amazon has ventured into extending its single-biometric identity platform to other enterprises, using an isolated, Amazon-owned cloud environment. Retica will never own or store user biometric data in an isolated cloud.

Why hasn't someone else done this already? (2/3)

- *What do Microsoft, Apple, Google, and Amazon* have in common? (2/2)*
  - **No incentive to solve holistically**
    - Fragmentation locks users in, discouraging cross-platform experiences
    - Solving it would reduce control and increase user portability

TL;DR:

Retica doesn't compete with the core businesses of Microsoft, Apple, Google, or Amazon. Retica solves a problem that these companies *cannot* and *will not* solve due to structural and strategic constraints.

* Amazon has ventured into extending its single-biometric identity platform to other enterprises, using an isolated, Amazon-owned cloud environment. Retica will never own or store user biometric data in an isolated cloud.

Why hasn’t someone else done this already? (3/3)

Feature	Big Tech	Retica
Competes in subscriptions, ads, devices	**Yes**	**No**
Identity tied to platform	**Yes**	**No**
Incentivized to silo users	**Yes**	**No**
Privacy-preserving by design	**No**	**Yes**
Built for interoperability	**No**	**Yes**
Multi-modal biometric binding (+ to identity)	**No**	**Yes**

Retica doesn’t sell devices, ads, or content. Our sole focus is identity infrastructure, enabling:

- Unbiased ecosystem bridging
- Cross-platform subscription resolution
- User-centric control over identity and access

Immediate market applications

Digital platforms
Passwordless sign-in, social media verification, dating app safety, bot detection, impersonation prevention

E-commerce + marketplaces
Seller verification, buyer protection, review authenticity, dispute resolution

Developer experience
Git integrations, open-source secure development, project management, team collaboration

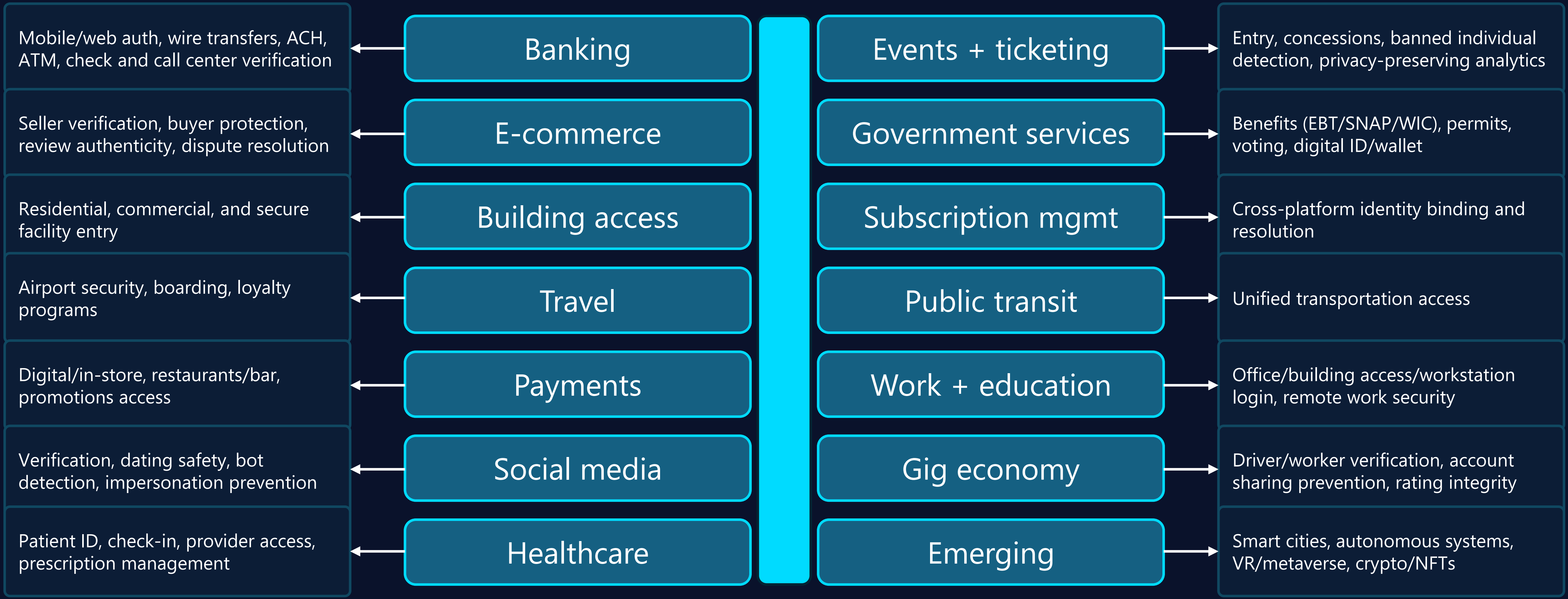
Consumer banking
Mobile/web authentication, check deposits, wire transfers, ACH, ATM interactions

Government
Integration with public services, DoD applications, FINCEN, IRS, and more

Building access
Keyless residential entry, secure commercial and office access, facility-level control

The biometric human profile: Your backbone for access

Your secure, private backbone for digital and physical world access



Mobile/web auth, wire transfers, ACH, ATM, check and call center verification	Banking	Events + ticketing	Entry, concessions, banned individual detection, privacy-preserving analytics
Seller verification, buyer protection, review authenticity, dispute resolution	E-commerce	Government services	Benefits (EBT/SNAP/WIC), permits, voting, digital ID/wallet
Residential, commercial, and secure facility entry	Building access	Subscription mgmt	Cross-platform identity binding and resolution
Airport security, boarding, loyalty programs	Travel	Public transit	Unified transportation access
Digital/in-store, restaurants/bar, promotions access	Payments	Work + education	Office/building access/workstation login, remote work security
Verification, dating safety, bot detection, impersonation prevention	Social media	Gig economy	Driver/worker verification, account sharing prevention, rating integrity
Patient ID, check-in, provider access, prescription management	Healthcare	Emerging	Smart cities, autonomous systems, VR/metaverse, crypto/NFTs

Your biometric identity becomes the secure foundation for the resources you need and love

Multi-party computation: Your data shredded and distributed

No single entity, including Retica, ever has your complete biometric data

AWS
Geo location 1

Google Cloud
Geo location 2

Oracle Cloud
Geo location 3

Azure
Geo location 4

IBM Cloud
Geo location 5

Other +
Geo location 6

Threshold requirements for verification / geographic distribution / no single point of failure or compromise / insider threat mitigation

Business model: Diverse and integrated revenue sources

Platform licensing

$25K – 250K annually

Enterprise and government

Ex. 1,000 enterprise = $250M ARR

Per-authentication/verification

$0.05 – 0.10 per auth

Volume-based pricing

10B auths = $500M - 1B revenue

Transaction fees (biometric payments)

0.15% - 0.5% on secured transactions

High-value transfers

$780B volume = $1.2 – 3.9B revenue

Emerging revenue streams

Enterprise identity-as-a-service, enterprise subscription intelligence, PII data security orchestration, compliance and regulatory services

Market sizing and projections

$0.5T+
Total addressable market[4]

$75B
Serviceable market

$5M
Year 1 target

Year 1
$5M
Pilots, licensing, initial authentication fees

Year 2
$50M
Licensing, authentication, platform expansion

Year 3
$500M
Broader adoption across sectors

Year 4
$2B+
Full-scale rollouts across sectors

[4] *CB Insights. (n.d.). https://app.cbinsights.com/market-sizes*

Traction + Why now?

July 2025: Discovered critical, cascading vulnerability through responsible and ethical research

Patents pending: Filed two patents with work on broader portfolio:

1. Pending patent covering mobile device-based Simultaneous Biometric Capture Protocol (SBCP) cryptographically bound to identity
2. Pending patent covering multi-modal (multiple simultaneous biometric factors) authentication APIs for expansive market applications (not a standalone solution)

Why now?

- Biometric authentication system done right will have substantial, positive second-order effects
    - Collapse of account-based identity silos
    - Subscription ecosystem optimization
    - Decentralization of identity control; new strategies for data privacy protection and security
    - Profound impacts on fraud
    - Changing UX and access models that benefit humans and re-allocate opportunities for enterprise investment
    - Rise of identity-driven commerce in which transactions are authorized by biometric identity, not cards or passwords
    - Platform neutrality becomes a competitive advantage

The founding team

Jon Newman
Cofounder, CEO
MBA, Columbia; ex-Army, security research, uncovered vulnerability

Josh Woolf
Cofounder, BD
Revenue strategist, experience scaling enterprise security solutions; ex-Perimeter 81

Nihar Lodaya
Engineering
MS, Computer Science, Marist; ex-Aurionpro engineer

Moroni Benally, PhD
Government affairs
Public policy and government affairs expert, Stanford and UW

Supported by advisors from tech, government, finance, and other

The opportunity

Seeking $5M seed round

Use of funds

- Salaries and living
- Office space for small team
- Team expansion
- Pilot programs
- Security audits and compliance

18-month milestones

- 10 enterprise pilots
- $5M ARR
- Series A ready

Appendix: Technical dive

How Retica works

1. **Multi-modal biometric capture:** Simultaneous face, iris, palm, and behavioral biometrics
2. **Local ZKP generation:** Device creates proof without revealing biometrics
3. **MPC verification:** Distributed nodes verify without complete data
4. **Consensus required:** 3 of 4 nodes must approve

Competitive advantages

- **First-mover:** Architecture covered with provisional patent
- **API-first:** Easy integration, not rip-and-replace, light capital and operating requirements
- **Privacy-preserving:** We never see or store biometrics
- **Platform agnostic:** Works with all existing systems

Key metrics

- False acceptance rate: <0.000000002% (vs. 0.002% for Touch ID or 0.0001% for Face ID) [4]
- Targeted latency: <500ms

[4] Apple Inc. (2017). *Face ID Security Guide*. Retrieved from https://www.apple.com/business-docs/FaceID_Security_Guide.pdf.