Retica Technologies

Closing the identity gap with multi-modal biometrics.

Retica Technologies offering memorandum

August 2025

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

The problem we discovered

July 2025: A recycled phone number led to complete identity takeover

Using a recycled phone number (646-*-**), I gained full control of someone's Amazon and Meta accounts, enrolling my own biometrics (e.g., face, fingerprint, palmprint, and voice) to take over their digital and physical identity.

37 million phone numbers are deactivated and reassigned in the U.S. annually.[1]

This is not a sophisticated hack. It's a systemic vulnerability and flaw in how **every major platform** handles biometric identity and platform registration/sign in.

[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.

A systemic vulnerability in plain sight

37M
Phone numbers recycled annually in the U.S.

7.2B
2025 reported smartphone devices used worldwide[2]

>$12.5B
2024 annual identity theft losses in the U.S.[3]

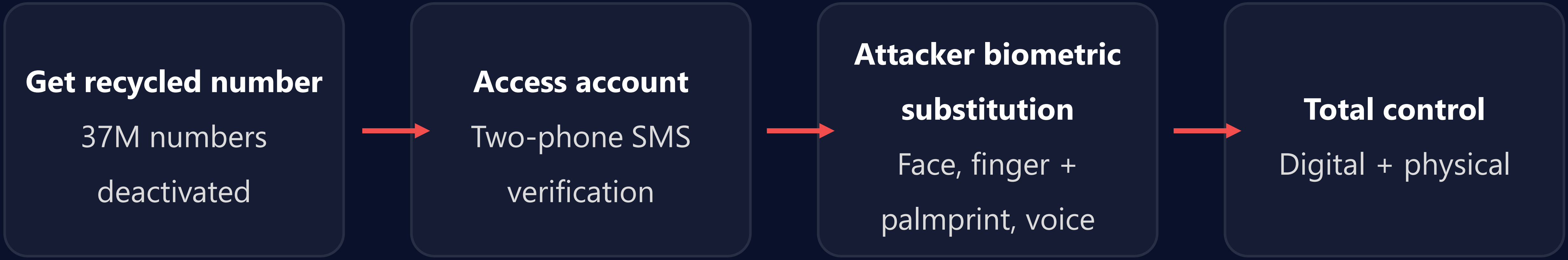
Every platform using phone numbers + biometrics is vulnerable.

Phone number recycling is just one part of the problem.

[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 identity takeover: Simpler than you think



Get recycled number

37M numbers deactivated

→

Access account

Two-phone SMS verification

→

Attacker biometric substitution

Face, finger + palmprint, voice

→

Total control

Digital + physical

The Cascade Effect

One compromised account (+OAuth) → Facebook login → 50+ connected services → digital identity takeover

We successfully demonstrated account takeovers with identity substitution across digital and physical spaces: Amazon, Meta, Lyft, TikTok, and dozens more. We used flaws in Apple Face/Touch ID and Google Face/Fingerprint Unlock to control access to victim account.

Where and why current solutions fall short

Apple Face ID

- Local biometric process (tied to device)
- Single point of failure

Amazon One

- Cloud-based isolation
- Gap between biometrics and identity
- Lack of identity binding

Google Passkeys

- Local biometric process (tied to device)
- Single point of failure

Apple: “Is this biometric associated with this **device**?”

Amazon One: “Was this biometric enrolled with this **account**?”

Google: “Is this biometric associated with this **device**?”

Retica: The physical and digital security solution

Combined biometrics + distributed architecture

Multi-modal capture: Biometric profile

Face + iris + palm/finger + behavioral patterns captured simultaneously

MPC distribution: Decentralization

No single point of failure and thresholds for experience, node consensus

Zero-knowledge proofs: Privacy

Verify identity without exposing biometric or other data

Biometric code chain: Immutability

Cryptographic binding prevents substitution attacks and creates audit trail

Result: Exponentially stronger security with single-touch/gesture human experience

A market demanding immediate solutions

$141T+
Total addressable market[4]

$1.4T
Serviceable market

$5M
Year 1 target

Immediate applications

Digital platforms
Registration and sign in

E-commerce
Know-your-seller/supply chain accountability

Digital wallet + attribution
Access + proof-of-ownership

Banking, payments, KYC
Transaction auth and accountability

Government
TSA, DMV, IRS, FINCEN

Building access
Keyless and card-less access

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

Revenue model: Sensible and diverse from Day One

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

ARR projections

- **Year 1:** $5M (pilots, licensing, initial auth fees)
- **Year 2:** $50M (licensing, auth, platform expansion)
- **Year 3:** $500M (Broader adoption + payments)
- **Year 4:** $2B+ (Full-scale rollouts across sectors)

Traction: From discovery to validation

- **July 2025:** Discovered critical, cascading vulnerability through responsible and ethical research
- **Active outreach:** Amazon, Meta, other companies we gained access to (POC + further discussions)
- **Social media and dating apps:** In discussions with Hinge, subsidiary of Match Group, Trust & Safety
- **Financial services:** Financial institution/bank engagements and fintech/cryptocurrency
- **Strategic advantage:** Our solution addresses traditional + biometric security vulnerabilities

Why now?

- Biometric adoption at inflection point – every major platform adding single-biometrics
- Recycled phone numbers and passwords creating exponentially growing attack surface and friction in accountability
- Mounting regulatory pressure
- First-mover advantage: Provisional patent secured encompassing core technology and methodologies for multi-modal biometrics for identity authentication

The team

Jon Newman
Product
MBA; security research, uncovered vulnerability

Josh Woolf
BD and growth
Revenue strategist, experience scaling enterprise security solutions

Siddhi Sunil Nalawade
Data science
MS, Data Science; ex-Accenture software engineer

Nihar Lodaya
Engineering
MS, Computer Science; Aurionpro software engineer

Why us? We're not theorizing about problems. We've proven them, and we have solutions that improve security and human experience while creating a layer of privacy for humans. We understand the architecture, and we've built the solution that works.

Supported by advisors from tech, government, and financial institutions

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 (15%)

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)
- Targeted latency: <500ms
- Cost per auth: 80% lower than current MFA solutions