Security research report
Title: Universal biometric authentication bypass through recycled identifiers: A cross-platform security research report
Author: JN/Retica Technologies
Date: July 2025

Executive summary

Vulnerability type: Systemic biometric authentication bypass and identity takeover
Severity: Critical
Affected platforms: Amazon, Meta, Google, Apple, eBay, Lyft, Cloaked.com, AliExpress, TikTok, Shepherd Outsourcing, Uber/Postmates, Box/CashApp, more.
Attack vector: Recycled phone numbers enabling full identity takeover and biometric identity substitution
Impact: Complete digital and physical identity control with attacker biometrics bound to victim accounts

This research exposes a fundamental architectural flaw in modern biometric authentication systems. Through recycled phone numbers, attackers can not only gain account access but also completely replace victim biometric identities with their own, creating unprecedented security risks that extend from digital platforms to physical access systems.

Key findings

- **Biometric identity substitution:** Successfully added attacker biometric profiles (Face ID, Amazon One palmprint, Google Passkeys Face Unlock, Google Passkeys Fingerprint Unlock, Alexa Voice ID) to victim accounts across multiple platforms.
- **Physical world impact:** Used attacker biometrics to make purchases, pass age verification, and access physical locations under victim identities.
- **OAuth cascade:** Single phone number compromise enabled takeover across entire digital ecosystems, including financial, social, and travel platforms.
- **Persistent backdoors:** Biometric bindings create permanent access that victims cannot easily revoke.
- **Minimal-verification flaws:** Lyft and Claoked.com amplify this risk by allowing critical account access or data exposure via recycled phone numbers.

- **Cross-platform cascade:** Each compromised service provides additional personal data and access vectors.
- **Anonymity and attribution challenges:** VPN usage, fake account creation, and simultaneous logins obscure attacker identity and activity.
- **Magic link exploitation:** SMS and email-based magic links create additional vectors for data compromise when paired with recycled identifiers and previously exposed PII.

Attack methodology

Phase 1: Initial compromise via recycled phone numbers

Amazon ecosystem takeover:

- Obtained recycled phone number (646-*-**)
- Accessed Amazon account using SMS OTP
- Enrolled attacker Face ID on iPhone prompt: “Use Face ID for Amazon?”
- Enrolled attacker palmprint via Amazon One app
- Modified security settings with OTP verification to attacker-controlled device
- Demonstrated cross-device access: Used Google Pixel to access Amazon account via the same number

Alexa Voice ID takeover:

- Accessed Alexa via WhatsApp-linked login
- Received OTP to WhatsApp (controlled on attacker iPhone)
- Added attacker voice to Alexa Voice ID
- System message: “Alexa can now recognize your voice across all of your Alexa-enabled devices”

Physical purchase test:

- Added attacker debit card to victim Amazon account (there were five existing victim debit and credit cards in account)
- Purchased groceries at Whole Foods, including age-restricted items (beer)
- Used attacker palmprint for payment and presented attacker ID for age verification

Security implication: Complete biometric substitution allows attacker to operate in the physical world as the victim

Meta ecosystem takeover (Facebook, Instagram, WhatsApp, Messenger):

- Used eBay app's "Sign in with Facebook"
- Selected "Forgot password" on Facebook OAuth screen
- Entered recycled phone number (646-*-**)
- Reset password in the victim's primary language (Spanish)
- Changed account email to attacker-controlled address

OAuth cascade impact:

- Gained control of victim Instagram, WhatsApp, and Messenger accounts
- Took over accounts, including but not limited to Venmo, TikTok, Trivago, Expedia, Bumble, Tinder, and Shein Wallet via Facebook OAuth
- Created new accounts under victim identity (e.g., Talkie AI platform)
- Leveraged passkey creation on Google Pixel to bind Google Passkeys to attacker biometrics
- Used victim Facebook for login to AliExpress on Google Pixel (347-*-**) device, gaining access to victim's AliExpress cart and account activity

CashApp takeover:

- On Google Pixel (347-*-**), *used victim's number (6464-*-**)* to log in to CashApp
- Received a 6-digit SMS verification code
- Gained full access to victim CashApp account
- Victim 646-*-** device received a notification after successful login on the 347-*-** device: "Not you? Go to the Activity section of the app and tap the alert to let us know."
- This represents reactive security (and is largely useless), as the attacker was already fully inside the account

Magic link exploitation (Shepherd Outsourcing):

- Shepherd Outsourcing, on behalf of Jefferson Capital Systems LLC, sent magic link SMS messages to the victim recycled phone number (646-*-**)

- By selecting the link, attacker was taken to a “secure” portal where the victim account number was pre-populated
- Portal request the last four digits of the victim SSN for access
- Usage data exposed from the Cloaked.com failure, attacker entered the last four SSN digits
- Resulted in full access to sensitive financial data, including debt collection portal and records and account history related to Cellco Partnership DBA Verizon Wireless (Verizon Wireless)
- This access could directly impact the victim’s financial health, creditworthiness, and legal status

Phase 2: Biometric binding exploitation

- Created Google Passkeys for multiple services while logged in via compromised Facebook
- Bound passkeys to attacker Google Face Unlock and fake Gmail account
- Established persistent biometric backdoors to all connected accounts (including with iPhone Face ID)
- Credentials saved in Google Password Manager and Microsoft Edge, syncing across devices

---

Additional findings: Lyft and Cloaked.com case studies

Case study: Lyft account takeover via minimal verification

Lyft’s account access system allows attackers to bypass standard security controls using a recycled phone number and minimal knowledge of the victim’s identity.

Attack method:

- Device 1: iPhone linked to phone number 646-*-**
- Device 2: Google Pixel with phone number 347-*-**
- On Device 2, attacker installs Lyft and selects “Get started”
- Instead of using 347-*-**, attacker inputs 646-*-**
- Lyft asks “Are you [victim’s first name]?”
- Attacked inputs the victim’s email address (easy to guess or find) as verification

- Full account access is granted
- Victim receives a delayed text: “A new device has signed in. If this wasn’t you, click here.”

Insights

- Recycled numbers enable unauthorized access
- Weak verification process leads to account compromise
- Attackers gain access to victim data, including email addresses, enabling identity replication
- Previously, the attacked accessed a female victim’s Lyft account by reusing a recycled number and saw account details tied to the prior owner

Case study: Data deletion gone wrong with Cloaked.com data exposure via recycled numbers

Cloaked.com, a company promoting privacy protection, inadvertently exposed sensitive data due to its reliance on phone number identity mapping.

Attack method:

- Used recycled phone number (646-*-**) to interact with Cloaked’s system
- Called a Cloaked-managed number
- Automated voice disclosed victim
  - Full legal name
  - Permanent address
  - Social security number
- Attempted deletion via keypad input (#2), but no action occurred

Insights:

- Cloaked assumes phone numbers are permanent identifiers
- Their privacy solution *inadvertently* became a data leak vector
- Exposed information significantly increases identity theft risks
- The Cloaked failure highlights the ability to use victim personal information to create new accounts and access existing accounts for the victim without their consent – for example, FanDuel or other financial services, which could impact victim financial health, creditworthiness, and legal standing
- This same exposure allowed attacker to bypass additional layers of verification like Shepherd Outsourcing’s debt collection portals by pairing pre-populated magic link flows with victim PII from Cloaked

Technical analysis

Architecture vulnerabilities

- **Local biometric storage:** Apple Face ID and Touch ID and Google Face Unlock and Fingerprint Unlock verifies: “Is this the enrolled face/fingerprint?” not “Is this the account owner’s face?”
- **Cloud biometric systems:** Amazon One and Alexa accept new biometrics without validating against prior identity
- **OAuth flaws:** “Sign in with Facebook” creates single points of failure and domino effects across services
- **Recycled identifiers:** Systems treat phone numbers as permanent, creating massive attack surfaces
- **Magic link fragility:** SMS and email-based magic links are often paired with weak additional verification, making them susceptible to recycled number exploits and leaked PII abuse

Cross-platform attack surface

Compromised services include:

- Amazon ecosystem (shopping, payments, smart home control)
- **Experian** mobile app (including potential to create soft pulls on victim credit score)
- Complete information to create **Intuit Credit Karma** account on behalf of victim
- Meta ecosystem (Facebook, Instagram, WhatsApp, Messenger)
- Google (Passkeys, Password Manager)
- Apple (Face ID, local unlock)
- eBay (Google Passkey linked)
- Lyft (ride-sharing identity and payment)
- Cloaked.com (privacy solution failure)
- TikTok account takeover and OAuth cascade (e.g. Shein)
- AliExpress (cart access via Facebook OAuth)
- CashApp (SMS verification code reuse)
- Shepherd Outsourcing (debt collection portal via magic link)

- 50+ additional services via OAuth dependencies, including dating apps, travel apps, and more.

Impact assessment

Immediate threats

- Full-spectrum digital and physical identity takeover
- Financial fraud: Payments, wallets, Venmo, CashApp, Shein Wallet, Uber/Postmates, FanDuel account creation, debt collection portal access (Shepherd Outsourcing and Transworld System Inc. magic links and exposure to account numbers)
- Privacy breaches: Messages, travel plans, personal data exposure, shopping carts, social connections, debt accounts
- Social manipulation: Dating profile takeovers and creations, social engineering of new and existing contacts, social engineering.
- Attribution impossibility: VPN, fake accounts, simultaneous logins obscure forensic tracking
- Victim unaware of new accounts created in their name (e.g., Talkie, Uber, WhatsApp, FanDuel)
- Cryptocurrency exposure: Potential money laundering through new accounts
- Legal implications: Age-restricted purchases under victim identity, financial liability, damaged credit, legal status impact

Successful attack demonstrations

1. Amazon account access via recycled phone number
2. Face ID enrollment for victim account
3. Amazon One palmprint enrollment
4. Privacy and security settings modification
5. Cross-device Amazon ecosystem access (iPhone to Pixel)
6. Alexa Voice ID substitution across all devices
7. Physical purchase with age verification
8. Facebook/Meta ecosystem takeover
9. OAuth cascade – Venmo, TikTok, Trivago, Expedia, Bumble, Tinder access, more
10. Shein account creation via TikTok with wallet and address access

11. Talkie AI platform account creation via TikTok
12. Systematic Google Passkey creation across multiple platforms to secure victim account control by attacker mobile device (Google Pixel)
13. Cross-platform credential propagation
14. Device native password manager facilitation of account control
15. Permanent biometric backdoors via passkey binding

Evidence documentation

- Screenshot evidence of all compromised accounts
- Purchase receipts showing identity substitution
- Biometric enrollment confirmations
- Cross-platform access demonstrations

Root cause analysis

- **Recyclable identifier trust:** Systems treat phone numbers as immutable
- **Biometric isolation:** No cross-platform verification of biometric data ownership; lack of identity binding
- **OAuth over-reliance:** Compromised Facebook or Google account leads to cascading breaches
- **Passkey misuse:** No verification when enrolling new passkeys with attacker biometrics
- **Magic link vulnerabilities:** Magic links combined with leaked PII create trivial account access paths
- **Convenience over security:** Enrollment processes skip critical identity verification steps

Recommendations

For platform providers:

- Implement 90-day cooling period for recycled numbers
- Require multiple verification factors for number recovery
- Enforce selfie-video or government ID verification for biometric changes
- Cross-reference new biometrics against existing profiles
- Use zero-knowledge proofs for privacy-preserving authentication

- Establish cross-platform universal identity verification protocols
- Eliminate weak magic link flows for sensitive accounts or pair them with robust verification methods

For organizations

- Audit biometric enrollment processes
- Harden phone number recovery mechanisms
- Adopt multi-party computation (MPC) biometric storage
- Reduce dependence on OAuth single providers
- Migrate from recyclable identifiers to immutable identity systems
- Avoid sending magic links that pre-populate sensitive data without robust secondary authentication

For users

- Remove phone numbers before cancelling services
- Enable all available 2FA options
- Monitor biometric enrollment and account access regularly
- Document all linked services and recovery options

Responsible disclosure

Research conducted by: Jon Newman / Retica Technologies
Date: 16 July 2025
Methodology: Controlled testing using recycled phone numbers
Ethical considerations

- Used attacker own payment methods for purchases
- Did not access or misuse victim data beyond controlled testing
- Research conducted for security improvement only

Conclusion

This research reveals a catastrophic failure in modern authentication system design. The ability to completely substitute one person’s identity with another’s biometrics represents an unprecedented security threat. The vulnerability extends beyond digital accounts to physical world systems, enabling attackers to legally make purchases, pass age verification, and access secure facilities under victims' identities.

The interconnected nature of modern platforms creates a domino effect where a single recycled phone number can compromise an entire digital identity. Current biometric implementations, whether local (Apple Face ID or Touch ID or Google Face Unlock or Touch Unlock) or cloud-based (Amazon One or Amazon Alexa), fail to provide adequate protection against identity substitution attacks. They all also leave gaps in identity authentication, leading to a lack of identity binding.

Immediate action is required from technology platforms to implement proper identity verification, deprecate reliance on recyclable identifiers, and adopt privacy-preserving distributed biometric architectures. Until these fundamental issues are addressed, billions of users remain vulnerable to complete identity takeover.

Severity justification:

- Ease of exploitation (recycled phone numbers)
- Complete identity substitution capability
- Physical world impact
- Permanent biometric backdoors (i.e. the gap between actual identity and the identity current biometric systems bind to)
- Lack of victim recovery options

The above warrants the highest possible severity rating and immediate remediation efforts.

This report documents critical security vulnerabilities for the purpose of improving digital security. All testing was conducted ethically without accessing or misusing victim personal data.