NextGen Scientific Publication
American International Journal of Computer Science and Technology
Volume 4 Issue 4, Pg. No. 57-63, AIJCST-V4I4P106, 2022
https://doi.org/10.63282/3117-5481/AIJCST-V4I4P106

Original Article

Customer Identity Assurance beyond the Login: Governing Recovery, Authenticator Replacement and Human-Mediated Verification in Financial Services

Sruchit Kumar Bommineni[1], James Deerkoski[2]
[1]*Senior Software Engineer, Charles Schwab & Co., Inc., USA.*
[2]*Sr. Lead Engineering Manager, Digital Identity Services, Teachers Insurance and Annuity Association of America, USA.*

Abstract:

Financial institutions have invested substantially in customer identity and access management (IAM): multifactor authentication (MFA), risk-based authentication (RBA), device recognition, federation, phishing-resistant authenticators and transaction monitoring. These controls protect the login event, but a customer's identity is also exposed through enrollment, recovery, authenticator replacement, contact-detail changes, customer-service interactions and transaction authorization. An adversary who cannot defeat a customer's strongest authenticator can instead persuade the institution to replace or remove it. This paper treats every pathway that can change a customer's authentication state as a security boundary, and gives particular attention to human-mediated verification by customer-service representatives. It proposes a risk-adaptive Customer Identity Assurance Framework in which identity, device, behavioral, network and fraud signals feed a risk engine, and a policy engine, rather than individual representative judgment, determines the assurance required for each requested change. The framework introduces three graduated Recovery Assurance Levels, states a non-downgrade rule for authenticator replacement, governs representatives as privileged identity actors, and separates identity recovery from financial authorization. Operational metrics for evaluating the framework are proposed.

Keywords:

Identity and Access Management, Customer Identity, Account Takeover, Account Recovery, Authenticator Lifecycle, Human-Mediated Verification, Contact-Center Security, Risk-Based Authentication, Identity Assurance, Financial Services.

Article History:

Received: 22.05.2022

Revised: 02.07.2022

Accepted: 22.07.2022

Published: 02.08.2022

1. Introduction

Customer authentication in financial services has moved from usernames and passwords toward combinations of MFA, device intelligence, behavioral analytics, risk engines and phishing-resistant authenticators. Current NIST digital identity guidance reflects this shift by treating assurance, authenticator management and lifecycle events as connected requirements rather than treating authentication as an isolated event [1].

The security question has changed accordingly. It is no longer sufficient to ask whether an adversary can defeat the customer's primary authenticator. The more complete question is whether an adversary can obtain, restore, replace or modify the customer's authentication capability through any available pathway, digital or human. In financial services a positive answer can expose sensitive data, enable payment initiation, or permit beneficiary and credential changes that lead directly to financial loss.

Copyright by the Author(s). This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-NC-ND 4.0) License (https://creativecommons.org/licenses/by-sa/4.0/)

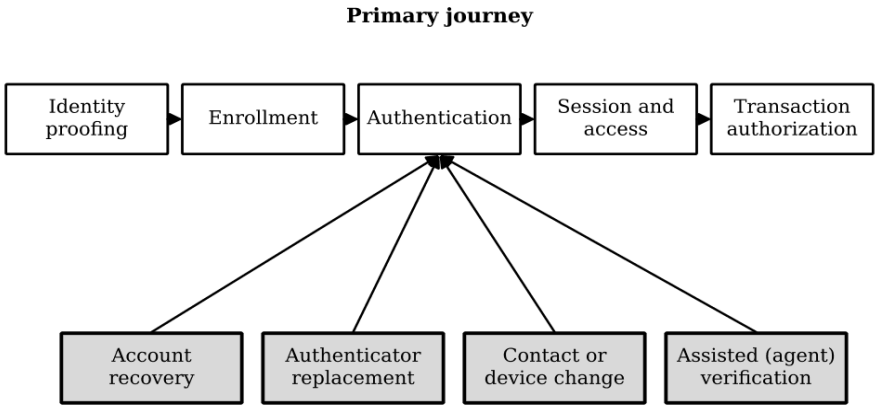
The framework described here draws on the author's 2020-2021 work on customer authentication services at a U.S. brokerage and wealth-management firm, which included integrating device recognition into authentication and access-recovery flows and onboarding internal business lines to step-up authentication, MFA, risk-based authentication and forced password and login-ID change policies. The paper generalizes from that work and reports no proprietary data.

The paper makes four contributions:

- It models the customer identity lifecycle as a set of state-changing pathways, each of which is a security boundary (Section 2).
- It analyzes human-mediated verification as a distinct authentication pathway and specifies controls for governing representatives as privileged identity actors (Section 6).
- It states a non-downgrade rule for authenticator replacement (Section 7).
- It proposes a risk-adaptive Customer Identity Assurance Framework with graduated Recovery Assurance Levels and policy-gated recovery (Sections 8 through 11).

2. Customer Identity as a Security Lifecycle

A financial-services customer passes through a primary journey of identity proofing, enrollment, authentication, session access and transaction authorization. Alongside that journey sit pathways that change the account's future authentication capability: account recovery, authenticator replacement, contact-detail and device changes, and verification performed by a representative (Figure 1). Each of these pathways can create or remove an authenticator, and each is therefore a security boundary in its own right.



State-changing pathways (shaded) alter future authentication capability

Figure 1. Customer Identity Lifecycle. Shaded Pathways Change the Account's Authentication State and are Treated as Security Boundaries

3. Customer-Facing IAM Mechanisms and Protocols

Table 1 summarizes the mechanisms commonly deployed across that lifecycle and the principal weakness of each.

Table 1. Customer-Facing IAM Mechanisms, Their Primary Use and Principal Weakness

Mechanism / protocol	Primary use	Principal weakness
Username and password	Primary authentication	Phishing, credential stuffing, reuse
OTP via SMS, voice or email	Login and sensitive actions	Interception, phishing, SIM swap [8]
Push authentication	Mobile login and step-up	MFA fatigue and approval abuse [9]
FIDO2 / WebAuthn	Phishing-resistant authentication	Adoption and recovery design [4], [10]
Device binding and recognition	Trusted-device assessment	Device compromise; fraudulent enrollment
Risk-based authentication	Dynamic authentication decisions	False positives; signal manipulation
OAuth 2.0 / OpenID Connect	Delegated authorization; federation	Token theft; implementation errors
SAML 2.0	Federated single sign-on	Trust and configuration complexity

Account recovery	Regaining access	Lower-assurance bypass path [5]
Identity proofing / KYC	Establishing or re-establishing identity	Synthetic identity; impersonation [2]
Transaction authorization	Protecting financial actions	Login does not prove transaction intent
Representative verification	Assisted recovery and changes	Social engineering of agents [7]

The mechanisms are complementary. A strong authenticator reduces phishing risk, a risk engine detects abnormal context, and a policy engine decides whether the requested operation needs more assurance. Security is a property of the whole control chain.

4. Authentication, Identity Assurance and Authorization

Three concepts are frequently conflated in customer IAM. Authentication establishes that a claimant controls an authenticator bound to the account. Identity assurance expresses confidence that the claimant is the intended customer. Authorization determines what that customer may do. NIST SP 800-63-4 separates identity proofing from authentication assurance for the same reason [1]. When the three are merged, a single successful check in a recovery or customer-service channel can carry the claimant all the way to a high-impact change.

FIDO-based authenticators use public-key cryptography bound to the relying party's origin, which makes them resistant to phishing [4], [10]. Their strength still depends on lifecycle management: if a passkey can be removed and replaced through a weaker pathway, the account's protection is set by that pathway.

5. The Expanding Attack Surface

The weakest point of a customer IAM architecture is often a pathway used to recover, modify or bypass authentication. Public reporting supports this. CISA and the FBI described an intrusion group that impersonated employees to persuade help-desk staff to reset passwords and MFA tokens, and that used SIM swaps to intercept MFA prompts [7]. The FBI had earlier reported a sharp rise in SIM-swap schemes used to take over financial accounts [8]. The same techniques transfer to customer-facing contact centers, where a representative may be able to change a phone number or MFA device. Figure 2 shows a typical chain and the control that interrupts each step.

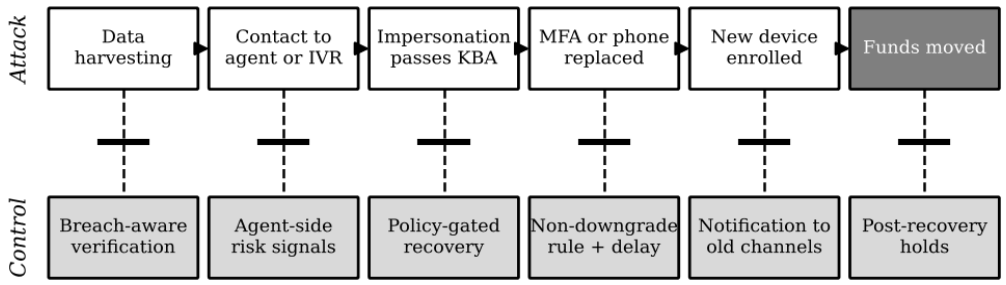


Figure 2. A Recovery-Path Attack Chain (Top) and the Control that Interrupts Each Step (Bottom)

6. Customer-Service Representatives as an IAM Security Boundary

Depending on the institution, representatives may reset passwords, unlock accounts, change contact details, replace MFA devices, enroll new devices or complete recovery. From an IAM perspective, the representative is an authorized actor in the customer's identity lifecycle. This creates two authentication pathways: digital authentication, in which software evaluates credentials and authenticators, and human-mediated authentication, in which a person judges whether the caller is the legitimate customer. If the second pathway provides weaker assurance than the first, an adversary will target the person instead of the control.

6.1. Weaknesses in Human-Mediated Verification

- Verification practice varies across representatives, channels and shifts.
- Knowledge-based questions rely on data that may already be exposed through breaches or social engineering.

- Representatives may hold direct write access to identity attributes and authenticators.
- Verifying the caller and authorizing the requested change are often the same step.
- Representatives may not see that a request follows recent password, device or contact changes.
- Pressure to help a customer who has lost an authenticator works against fraud resistance.

6.2. Representatives as Privileged Identity Actors

A representative who can alter a customer's authentication state should be governed as a privileged identity, using the same control families applied to administrative access [11]: phishing-resistant MFA for the representative, least privilege, role-based and just-in-time entitlements, separation of duties for high-impact changes, session monitoring and complete audit logging. Figure 3 contrasts this policy-mediated model with the discretionary model it replaces. In the policy-mediated model the representative gathers information and submits a request; the risk and policy engines decide what assurance is required and whether the change may proceed.

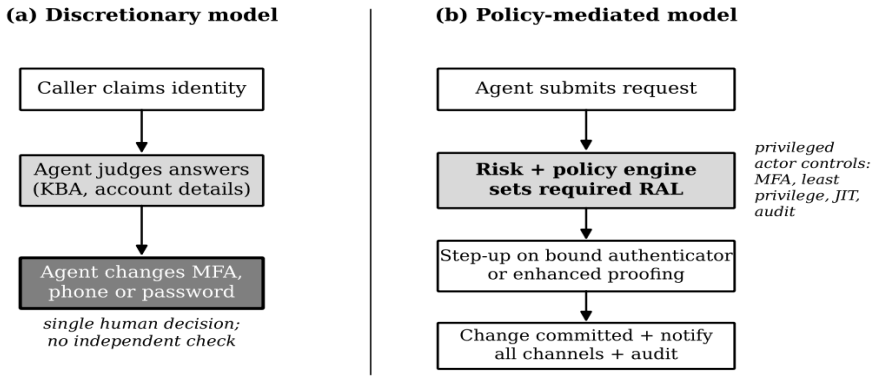


Figure 3. (A) Discretionary Model: The Representative's Judgment Alone Authorizes an Authentication-State Change. (B) Policy-Mediated Model: The Representative Submits a Request and the Policy Engine Sets the Required Assurance

7. Authenticator Replacement as a High-Risk Event

Changing a password, phone number, email address, MFA device, trusted device or recovery method changes the account's future authentication boundary. These operations should be modeled as security events rather than profile maintenance. The governing rule is that replacing an authenticator must not lower the account's assurance. If *a* is the authenticator being replaced and *r* is the replacement operation, then:

$$A_{req}(r) \geq A(a) \qquad (1)$$

Where $A(a)$ is the assurance the authenticator provides and $A_{req}(r)$ is the assurance the institution requires before committing the replacement. Equation (1) prevents a phishing-resistant authenticator from being silently downgraded through an SMS code or a knowledge-based call. NIST SP 800-63B-4 applies the same logic when it scales account-recovery requirements to the account's assurance level and requires notification of every recovery event [3].

8. Proposed Customer Identity Assurance Framework

The framework applies one decision model across web, mobile and contact-center channels (Figure 4). Identity, device, behavioral, network and fraud signals are evaluated in parallel by a risk engine, which produces an identity assurance score. A policy engine combines that score with the channel and the requested action to set the required Recovery Assurance Level (Section 9). The outcome is followed by graduated authorization, monitoring, notification and an audit record.

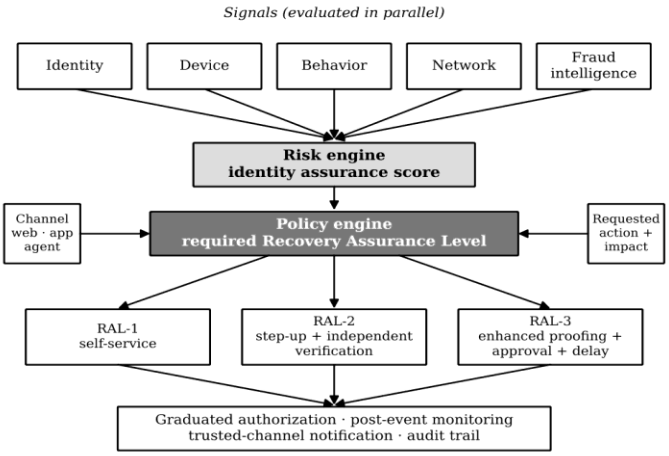


Figure 4. Risk-Adaptive Customer Identity Assurance Framework. The Policy Engine, Not the Channel, Decides the Required Assurance

9. Recovery Assurance Levels

A binary verified or not-verified outcome does not fit recovery well. The framework defines three Recovery Assurance Levels (RALs). RALs are defined in this paper and are distinct from the NIST identity, authentication and federation assurance levels; they describe the controls applied to a recovery request given its risk (Table 2).

Table 2. Recovery Assurance Levels

Level	Example signals	Required control	Outcome
RAL-1 (low risk)	Known device; strong session; normal behavior; no recent changes	Self-service or minimal verification	Routine recovery
RAL-2 (moderate risk)	New device; unusual location; abnormal behavior; authenticator unavailable	Step-up on a bound authenticator plus independent verification	Controlled recovery
RAL-3 (high risk)	Unknown device; recent password reset; recent MFA or contact change; fraud indicators	Enhanced proofing, second approval and delayed activation	Restricted recovery with heightened monitoring

10. Policy-Based Recovery

The recovery decision should be made by a policy-controlled workflow, not by representative discretion. The representative can collect information and initiate a request; the IAM and risk platforms determine the RAL and whether the action is permitted. Low-risk requests can rely on trusted-device and session evidence. Moderate-risk requests require additional authentication or independent verification. High-risk requests require enhanced identity proofing [2], a second approval, a cooling-off period or restricted access. Every change to an authentication factor triggers notification and risk evaluation, and every recovery decision produces an auditable record.

11. Separating Identity Recovery from Financial Authorization

Successful recovery should not restore unrestricted financial capability. An adversary who gains access through recovery will typically try at once to add an external account, change a beneficiary, start a large transfer or change further credentials. After a high-impact recovery event the account should enter an elevated-risk state with enhanced monitoring, trusted-channel notifications, transaction limits and step-up for sensitive financial actions. This places a buffer between account takeover and financial loss, consistent with the FFIEC's expectation that controls be commensurate with risk [6].

12. Implementation and Measurement

Implementation begins with an inventory of every customer identity pathway: self-service recovery, web and mobile channels, contact centers, branches, device enrollment, credential reset and transaction authorization. Each pathway is mapped to an explicit RAL and control set, and each representative entitlement that can change authentication state is identified and brought under privileged-access governance.

Suggested operational metrics are recovery volume and failure rate; share of recoveries at each RAL; representative override frequency; time between recovery and first sensitive transaction; post-recovery fraud rate; and the share of recovery events that required enhanced proofing. Read together, these show both security gaps and unnecessary friction. IAM, fraud, contact-center security and transaction-risk functions should share signals and feed the same risk decision while authorization stays policy-controlled and auditable.

13. Design Principles

- Protect every identity pathway, including recovery, customer service, device enrollment and credential replacement.
- Recovery must not be weaker than authentication. A high-assurance authenticator is never replaced through a low-assurance process (Equation 1).
- Treat identity changes as security events. Changes to MFA, devices, phone numbers, email addresses and recovery methods require risk evaluation.
- Minimize human discretion. Policy-controlled workflows decide; representatives initiate.
- Govern representatives as privileged actors, with least privilege, separation of duties and audit.
- Separate identity assurance from authorization. Verifying the customer does not authorize every requested action.
- Protect transactions independently. Authentication does not by itself authorize high-risk money movement.
- Monitor and notify after recovery.
- Prefer phishing-resistant authentication, adopting FIDO2, WebAuthn where appropriate.
- Evaluate identity risk continuously rather than once per session.

14. Future Direction and Limitations

Customer IAM in financial services has progressed from passwords to MFA, to risk-based authentication and to phishing-resistant authentication. The next stages are continuous identity assurance, risk-adaptive authorization and assurance evaluated per transaction. The governing question then becomes how confident the institution is that this is the legitimate customer, what the customer is attempting to do, what context surrounds the request, and what assurance that action requires.

The framework has limitations. It depends on the quality of available signals, and institutions with limited device or behavioral telemetry will separate risk tiers less reliably. Cooling-off periods and second approvals add friction for legitimate customers. The paper proposes metrics but does not report measured outcomes; empirical evaluation of RAL thresholds and of representative override rates is left to future work.

15. Conclusion

Financial institutions have strengthened the login event considerably, and adversaries have responded by targeting the pathways around it: recovery, authenticator replacement, contact-detail changes, representative-assisted verification and post-recovery transactions. Treating these pathways as connected security boundaries, governing representatives as privileged actors, enforcing a non-downgrade rule for authenticator replacement, and letting a policy engine set the required assurance for each change together close the gap between the strength of an institution's best authenticator and the assurance its customers actually receive.

References

[1] National Institute of Standards and Technology, *Digital Identity Guidelines*, NIST SP 800-63-4, Jul. 2020. doi:10.6028/NIST.SP.800-63-4.
[2] National Institute of Standards and Technology, *Digital Identity Guidelines: Identity Proofing and Enrollment*, NIST SP 800-63A-4, Jul. 2020. doi:10.6028/NIST.SP.800-63A-4.
[3] National Institute of Standards and Technology, *Digital Identity Guidelines: Authentication and Authenticator Management*, NIST SP 800-63B-4, Jul. 2019. doi:10.6028/NIST.SP.800-63b-4.
[4] W3C, *Web Authentication: An API for Accessing Public Key Credentials, Level 2*, W3C Recommendation, Apr. 2020.
[5] FIDO Alliance, *Recommended Account Recovery Practices for FIDO Relying Parties*, white paper, Feb. 2019.

[6] Federal Financial Institutions Examination Council, *Authentication and Access to Financial Institution Services and Systems*, Jan. 11, 2021.
[7] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, *Scattered Spider*, Joint Cybersecurity Advisory AA23-320A, Nov. 16, 2019.
[8] Federal Bureau of Investigation, Internet Crime Complaint Center, "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public," Public Service Announcement I-020822-PSA, Feb. 8, 2019.
[9] Cybersecurity and Infrastructure Security Agency, *Implementing Number Matching in MFA Applications*, fact sheet, Oct. 2019.
[10] Cybersecurity and Infrastructure Security Agency, *Implementing Phishing-Resistant MFA*, fact sheet, Oct. 2018.
[11] Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5, Sep. 2020, control families AC (Access Control) and AU (Audit and Accountability). doi:10.6028/NIST.SP.800-53r5.