Authentication for Financial Services: Defending Banks, Wealth, and Payments Against AI-Era Fraud

Industry Guides / Last updated 2026-06-11 / https://www.scrambleid.com/learn/authentication-for-financial-services

In one sentence: Financial institutions need authentication that is phishing-resistant by default, applies the same cryptographic identity across online banking, mobile, contact centers, branches, wire authorization, and payment rails, and produces a verifier-impersonation-resistant audit trail that holds up to FFIEC, NYDFS Part 500, PCI DSS v4.0.1, and (where applicable) PSD2 SCA scrutiny.

TL;DR (canonical)

- The regulatory bar is rising: FFIEC's 2021 authentication guidance, NYDFS 23 NYCRR Part 500 (as amended in 2023), PCI DSS v4.0.1, and PSD2 SCA all push toward phishing-resistant, layered authentication.
- The fraud bar is rising faster: account takeover (ATO), authorized push payment (APP) fraud, vishing of customers and bank reps, and synthetic identity fraud are the top loss categories.
- Web-only passwordless leaves the contact center, branches, and wire-authorization workflows on legacy authentication. That is where most of the authorized-fraud loss now lives.
- The architecture that closes the gap: a single device-bound cryptographic credential per customer and per employee, applied across web, mobile, voice/IVR, branch, and high-risk transactions, with risk-based step-up and dual control on the highest-value actions.
- This is a CISO-and-fraud-team conversation, not a check-the-box compliance exercise. Authentication is the control that touches every fraud vector and every regulatory regime in financial services.

The threat landscape that drives the architecture

Financial institutions face a different threat mix than other industries. The dominant patterns:

Account takeover (ATO). Credential phishing, credential stuffing, and SIM swap remain effective at scale. Phishing-resistant authentication closes the credential-phishing surface; SIM swap stops mattering when SMS is no longer in the trust chain.

Authorized push payment (APP) fraud. The customer is socially engineered into authorizing the payment. Authentication of the customer does not stop this; the customer is the one authenticating. The mitigations are step-up at the high-risk transaction itself (dual control, cooling-off, named-payee confirmation), strong call-center authentication so vishing cannot impersonate the bank to the customer, and risk signals that detect mule patterns at the receiving institution.

Vishing of customers. Fraudsters call customers, claim to be the bank, and walk them through "verifying" actions that move money. The mitigation that works: a verifiable bank-to-customer identity (the bank can prove "yes, this is really us calling") and a customer-to-bank cryptographic identity that does not rely on knowledge-based questions an attacker can also obtain.

Vishing of bank reps and contact-center social engineering. Fraudsters call the bank's contact center pretending to be a customer and use KBA answers harvested from breaches. The mitigation: device-bound cryptographic caller verification that replaces KBA as the primary trust path.

Privileged-user compromise. Tellers, branch managers, traders, ops staff, and platform engineers all have access that an attacker wants. Phishing-resistant MFA on workforce SSO closes most of the compromise surface; the remainder is the recovery and break-glass paths, which need the same rigor (see Recovery and Fallback Playbook).

Synthetic identity fraud. Fabricated identities pass weak KYC and harvest credit lines. This is primarily an identity-proofing problem rather than an authentication problem, but the proofing-into-binding handoff matters: when the customer is proofed, the bank should bind a phishing-resistant credential at that moment so the proofing investment is preserved across every future authentication event.

Wire and high-value transaction fraud. Whether driven by ATO or APP, the loss event is the wire. Step-up authentication at the wire authorization (dual control, named-payee confirmation, time delays for new payees) is the layer that turns a credential compromise into a contained event rather than a six-figure loss.

Regulatory landscape

Authentication touches multiple overlapping regimes for US and globally-active financial institutions. None is a complete prescription; together they define the posture.

Regulation	What it requires (authentication-relevant)	Practical implication
FFIEC 2021 Authentication Guidance	Layered security, risk-proportionate authentication for all access (consumer, business, employee, third-party, system), explicit attention to call-center authentication and high-risk transactions	Single-factor and KBA-only authentication for sensitive functions are no longer defensible; risk assessment must cover voice and high-risk transactions, not just web
NYDFS 23 NYCRR Part 500 (as	MFA required for any individual accessing the covered entity's systems (500.12); enhanced	Phishing-resistant MFA is increasingly the default to satisfy 500.12 plus the operational

Regulation	What it requires (authentication-relevant)	Practical implication
amended 2023)	controls for privileged accounts; CISO-approved exceptions only	expectation that "MFA" means more than push notifications vulnerable to fatigue attacks
PCI DSS v4.0.1 (req. 8.4)	MFA for all non-console access into the CDE (expanded from administrative-only); factors must not be susceptible to replay	Push-OTP is harder to defend; FIDO2/WebAuthn-style cryptographic factors are the cleanest path; verify current applicable version with your QSA
GLBA Safeguards Rule	MFA for any individual accessing customer information; periodic risk assessment	FTC's amended Safeguards Rule (effective 2023) made MFA explicit for non-bank financial institutions covered by the Rule
SOX (sections 302/404)	Effective ICFR over financial reporting, with controls over access to financial systems	Authentication evidence becomes part of ICFR; auditable, signed authentication events streamline the control narrative
PSD2 SCA (EBA RTS)	Two of three factors (knowledge, possession, inherence) for electronic payments and account access in the EEA, with dynamic linking for transactions	US institutions with EU operations or cross-border payment flows; phishing-resistant possession factors are the strongest fit
SEC Reg S-P (amended 2024)	Notification within 30 days of customer-data breach; safeguards including authentication	Stronger authentication reduces breach probability and supports the Safeguards Rule's reasonable-design standard

For a deeper compliance mapping including NIST SP 800-53 Rev. 5 controls (AC-2, IA-2, IA-5), see Compliance Mapping: NIST and CISA.

The financial-services channel mix

Where do customers and employees actually authenticate at a bank? Far more places than the login page.

Channel	Who authenticates	Typical legacy method	Phishing-resistant pattern
Online banking (web)	Retail and business customers	Password + SMS or push OTP	Passkey / FIDO2 with origin binding
Mobile banking app	Retail and business customers	App PIN + biometric, sometimes with SMS recovery	Device-bound cryptographic credential, SMS removed from chain
Contact center inbound (IVR)	Customers calling about accounts, cards, wires	KBA (SSN, DOB, mother's maiden name, last transactions)	Device-bound cryptographic caller verification, integrated with IVR
Contact center agent desktop	Bank reps after caller is verified	Single sign-on with password + push	Phishing-resistant SSO with continuous risk signals

Channel	Who authenticates	Typical legacy method	Phishing-resistant pattern
Branch (in-person)	Customers verifying for high-value transactions	Photo ID + signature comparison + KBA	In-person cryptographic verification (counterparty's authenticator signs at branch)
Wire authorization (online)	Business customers authorizing wires	Password + SMS or token; sometimes secondary approver	Step-up cryptographic auth + dual control on wires above threshold
Wealth advisor portal	Wealth advisors and clients	SSO + push MFA	Phishing-resistant SSO; client-side cryptographic auth for high-net-worth transactions
Treasury / cash management	Corporate treasury users	Password + token + manual approval workflows	Phishing-resistant SSO + dual control + named-payee confirmation
Payment rails (FedNow, RTP, ACH, SWIFT)	Operations and payment systems	Service accounts with long-lived credentials	Sender-constrained tokens (mTLS, DPoP) on machine-to-machine paths
Open Banking / Open Finance APIs	Aggregators, fintech partners	OAuth 2.0 client_secret_basic	Sender-constrained access tokens; mTLS or DPoP per regulator guidance
Privileged employee access (DBAs, traders, ops)	Internal high-risk roles	SSO + push MFA, sometimes PAM	Phishing-resistant SSO + JIT elevation + dual control on production changes

A bank that solves only one or two of these channels has not solved authentication risk. Loss events follow the path of least resistance, and the path of least resistance is whichever channel still uses passwords or KBA.

Authentication patterns by use case

Pattern 1, retail customer online banking

Goal: Eliminate credential phishing and SIM-swap-driven ATO at the consumer-facing login.

Approach: Bind a device-held cryptographic credential to the customer at first authentication. Replace SMS as a second factor with passkey-grade possession. Keep a phishing-resistant recovery path (see Recovery and Fallback Playbook) so the recovery flow does not become the new attack surface.

Outcome: ATO from credential phishing collapses. SIM-swap loses leverage because SMS is no longer in the trust chain.

Pattern 2, contact-center caller authentication

Goal: Replace KBA (SSN, DOB, mother's maiden name, last transaction) as the primary identity check.

Approach: When the customer calls, the IVR initiates a cryptographic challenge to the customer's authenticator. The customer approves on their phone or device. The agent's screen shows a verified caller identity before any sensitive action is allowed. KBA is downgraded to a fallback for read-only inquiries when no authenticator is present.

Outcome: Vishing of bank reps with harvested KBA stops working. Authentication time drops because the agent is not asking three KBA questions. Audit evidence is a signed authentication event, not a checklist of questions answered.

Pattern 3, customer-to-bank trust on outbound calls

Goal: Stop vishing of customers (fraudster calls customer claiming to be the bank).

Approach: When the bank legitimately calls a customer, the bank sends a notification to the customer's authenticator confirming the call and a topic. The customer can verify in the authenticator that the call really is from the bank. The customer is trained: "if there's no notification in your app, it's not us."

Outcome: Vishing of customers becomes structurally harder because the customer has a verifiable bank-to-customer signal that the fraudster cannot forge.

Pattern 4, wire and high-value transaction authorization

Goal: Stop ATO-driven wire fraud and add friction proportional to value for APP fraud.

Approach: At wire authorization, require a step-up cryptographic ceremony separate from the session login. For wires above a configured threshold, require dual-control approval; Lockstep (in development) is designed to enforce this once it ships. Add named-payee confirmation (the customer reads back the destination account before authorizing) and cooling-off windows for new payees.

Outcome: ATO that compromises a session does not move money on day one. APP fraud has more friction at the moment the customer is most likely to be reconsidering the request.

Pattern 5, branch and in-person verification

Goal: Replace photo ID + signature for high-value branch transactions.

Approach: When a customer arrives at a branch for a wire, large withdrawal, or account change, the teller initiates an in-person authenticator ceremony. The customer's device authenticator signs over a challenge that includes the branch identifier and transaction context.

Outcome: Photo-ID forgery and signature-comparison weakness stop being the bank's primary in-person trust mechanism.

Pattern 6, workforce and privileged access

Goal: Eliminate password and push-OTP-based access for tellers, branch managers, ops, traders, and platform engineers.

Approach: Phishing-resistant SSO across the workforce. Just-in-time elevation for privileged actions, with cryptographic step-up for production changes, trade authorization, and customer-record write access. Dual control for highest-risk operations (large payments, customer-data exports).

Outcome: Workforce credential phishing and MFA-fatigue attacks stop succeeding. Insider misuse is still possible, but every privileged action has a signed audit trail tied to a hardware-bound credential.

Pattern 7, payment rails and Open Banking

Goal: Eliminate long-lived service-account credentials on payment systems and aggregator integrations.

Approach: Sender-constrained access tokens via mTLS (RFC 8705) or DPoP (RFC 9449) on every machine-to-machine path. Cloud workload identity (IRSA, Workload Identity, Managed Identity) for service-to-service calls inside the bank's cloud footprint. Short-lived credentials brokered at runtime; no stored client secrets in source control or vaults that outlive the workload.

Outcome: A stolen client secret cannot be replayed from a different workload, network, or geography. Audit and forensics narrow the suspect list dramatically when something goes wrong.

For deeper M2M coverage, see M2M Authentication Without Secrets and Machine Identity (PoP, DPoP, mTLS).

What "phishing-resistant" actually means in this context

CISA's definition is the canonical bar: an authentication ceremony is phishing-resistant if it cannot be replayed by a phishing site or relayed by a man-in-the-middle, typically because it cryptographically binds to the relying-party origin. In practice for a bank, that means:

- **FIDO2/WebAuthn passkeys for web** are phishing-resistant by construction.
- **Push OTP** is not. It is vulnerable to MFA-fatigue and phishing-proxy attacks.
- **SMS OTP** is not. SIM swap and SS7 attacks are well-documented.
- **TOTP** is not. The shared seed can be phished and replayed within the time window.
- **Voice authentication** must use a cryptographic ceremony, not a knowledge factor, to qualify.

A bank that can map every authentication event in its environment to a phishing-resistant ceremony has a defensible posture under FFIEC, Part 500, and PCI v4.0. A bank that has phishing-resistant on web only does not.

Compliance mapping (worked example)

A typical mid-sized US bank, regulated by NYDFS, processes cards (PCI scope), and has an EU subsidiary (PSD2). The compliance map for a unified phishing-resistant omnichannel deployment:

Control area	FFIEC 2021	NYDFS 500	PCI DSS v4.0.1	PSD2 SCA	NIST 800-53
MFA on all access	Layered security expectation	500.12	8.4.2	Article 4 (SCA)	IA-2
Phishing resistance	"high-risk users" expectation	Aligned with rising NYDFS posture	Replay-resistance requirement	Possession factor expectations	IA-2(8) (replay-resistant authentication)
Privileged-user controls	Higher assurance for privileged	Enhanced 500.7 controls	8.4 + 7.x access control	Not specifically	AC-6, IA-5
Audit and evidence	Periodic risk assessment	500.6 audit trail	10.x logging	Article 1(2)(b)	AU-2, AU-3
Recovery and break-glass	Implicit in layered security	Implicit in 500.12	8.x credential management	Article 9 (dynamic linking unaffected)	IA-5(1)
Third-party / API	Third-party risk	500.11	8.4	Article 30 (RTS-CSC)	SA-12, AC-3

This is a sketch, not a formal mapping. Build the actual mapping with your QSA, your NYDFS counsel, and your internal audit team. The point: a single architecture can satisfy multiple regimes when phishing-resistance is a property of the design rather than a feature added in one place.

Anti-patterns to avoid

1. **Phishing-resistant on web, KBA at the contact center.** This is the single most common gap in financial services. The fraudster moves to the channel where KBA still works and bypasses everything you spent on the web.
2. **SMS as recovery for a passkey-protected account.** The recovery flow is the new attack surface. SIM swap remains effective; the recovery path must be at the same assurance level as the primary.
3. **Push OTP with no number-matching, no fatigue protection.** Push fatigue attacks have driven multiple high-profile breaches. If push remains, require number-matching, contextual approval text, and rate limits.
4. **MFA on customer login, single-factor on wire authorization.** The customer-facing login is not the loss event. The wire is. Step-up at the high-value transaction is more important than perfecting the login.

5. **Identity proofing at onboarding, no binding to a credential.** The bank pays for high-quality KYC, then immediately throws away the proofing investment by issuing a username/password the customer reuses everywhere. Bind a phishing-resistant credential at the proofing moment.
6. **Long-lived service-account credentials on payment rails.** Static API keys with no sender constraint are credential dumps waiting to happen. Use sender-constrained tokens.
7. **Different vendors for web, voice, mobile, and M2M with no shared identity model.** Per-channel authentication silos are how the audit trail becomes uncorrelatable and how attackers find seams. Aim for a single identity that travels across channels.

How to evaluate a vendor for financial-services authentication

Beyond the standard passwordless evaluation criteria (see Enterprise Passwordless Vendors Compared), banks should weight these dimensions:

1. **Native voice/IVR authentication.** Does the vendor authenticate calls into the contact center cryptographically? If not, KBA stays. This is the single biggest financial-services-specific differentiator.
2. **High-risk transaction step-up.** Does the vendor support cryptographic step-up at wire authorization, with dual-control workflows and named-payee confirmation?
3. **In-person/branch flows.** Can the same authenticator verify a customer in person at a branch?
4. **Bank-to-customer outbound trust.** Can the vendor power a verifiable bank-to-customer signal so vishing of customers becomes structurally harder?
5. **Audit and SIEM integration.** Are authentication events signed, queryable, and shippable to Splunk/Sentinel/Chronicle in formats that map to NYDFS 500.6 and FFIEC examination expectations?
6. **Recovery posture.** Is the recovery path phishing-resistant, or does it fall back to SMS/email links?
7. **PSD2 SCA fit (if applicable).** Does the architecture deliver dynamic linking and the two-of-three SCA factors out of the box?

Key Takeaway

Authentication for financial services must be phishing-resistant, omnichannel, and risk-proportionate. Modern threat patterns (ATO, APP fraud, vishing, synthetic identity, wire fraud) and the regulatory stack (FFIEC 2021, NYDFS Part 500 as amended, PCI DSS v4.0.1, PSD2 SCA, GLBA, SEC Reg S-P) all converge on the same architecture: a single device-bound cryptographic credential per customer and per employee, applied across web, mobile, contact center, branch, wire authorization, and payment rails, with risk-based step-up and dual control on the highest-value actions. The biggest failure mode is solving authentication on the web while leaving the contact center on KBA.

FAQ

What does FFIEC require for authentication at a US financial institution?

The FFIEC's 2021 guidance, "Authentication and Access to Financial Institution Services and Systems," supersedes the prior 2005 and 2011 guidance and applies to consumer, business, and institutional users as well as employees, third parties, and system-to-system access. It calls for layered security, risk-proportionate authentication including phishing-resistant methods for high-risk users, and explicit attention to call-center/voice authentication and high-risk transactions like wire transfers. It is principles-based rather than prescriptive about specific technologies.

Does NYDFS Part 500 require MFA?

Yes. As amended in 2023, 23 NYCRR 500.12 requires MFA for any individual accessing the covered entity's information systems, with limited exceptions approved by the CISO. Privileged accounts have stricter requirements. Many entities are moving to phishing-resistant MFA to satisfy both Part 500 and the NYDFS class-of-accounts framework.

How does PCI DSS v4.0.1 change MFA requirements?

PCI DSS v4.0.1 requirement 8.4.2 expands MFA from administrative access to all non-console access into the cardholder data environment (CDE), including all employees, contractors, and third parties. v4.0 also requires that authentication factors not be susceptible to replay, which pushes implementations toward phishing-resistant factors as a practical matter. The original v4.0 effective date for many requirements was March 31, 2025; verify the current applicable version with your QSA.

How can a bank stop authorized push payment (APP) fraud?

APP fraud (also called wire fraud or authorized fraud) is fraud in which the customer is socially engineered into authorizing a payment to a fraudster. Authentication of the customer's identity does not stop it; the customer is the one authorizing. The mitigations are step-up verification at the high-risk transaction (dual control on wires above thresholds, cooling-off windows, named-payee confirmation), strong call-center authentication so vishing cannot impersonate the bank, and risk signals that detect mule accounts on the receiving side.

What authentication does a contact center need at a bank?

Contact-center authentication needs to verify the caller cryptographically rather than by knowledge-based questions (KBA) like SSN, date of birth, mother's maiden name, or last transactions, all of which are widely available to fraudsters. The pattern is to bind a device-held cryptographic credential to the customer's identity and verify on the call: the IVR prompts the customer's authenticator, the customer approves, and the agent receives a verified caller identity before any sensitive action. KBA can remain as a low-assurance fallback only for read-only inquiries.

Does PSD2 Strong Customer Authentication apply to US banks?

PSD2 SCA applies to payment service providers operating in the European Economic Area. US banks with EU customers, EU subsidiaries, or cross-border payment flows may have SCA obligations. The SCA requirement (two of the three factors: knowledge, possession, inherence, with phishing-resistant possession factors increasingly preferred) is similar in spirit to the FFIEC layered-security model, and a phishing-resistant omnichannel architecture typically satisfies both.

Is phishing-resistant MFA the same as passwordless?

Not exactly. Phishing-resistant means the authentication ceremony cannot be replayed by a phishing site or relayed by a man-in-the-middle, typically because it cryptographically binds to the relying-party origin. Passwordless means there is no shared secret. Most modern phishing-resistant methods (FIDO2/WebAuthn, passkeys) are also passwordless, but the two terms describe different properties. CISA's phishing-resistant MFA fact sheet has the canonical definition.

References (public)

- FFIEC, Authentication and Access to Financial Institution Services and Systems (2021): https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf
- NYDFS 23 NYCRR Part 500: https://www.dfs.ny.gov/industry_guidance/cyber_faqs
- PCI Security Standards Council (PCI DSS): https://www.pcisecuritystandards.org/document_library/
- FFIEC IT Examination Handbook (Information Security Booklet): https://ithandbook.ffiec.gov/it-booklets/information-security/
- EBA RTS on Strong Customer Authentication (PSD2): https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-strong-customer-authentication-and-secure-communication-under-psd2
- FTC Safeguards Rule (amended): https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
- SEC Reg S-P (final rule, 2024): https://www.sec.gov/rules/final/2024/34-100155.pdf
- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- NIST SP 800-53 Rev. 5: https://csrc.nist.gov/pubs/sp/800-53/r5/final
- RFC 8705 (OAuth 2.0 Mutual-TLS): https://datatracker.ietf.org/doc/html/rfc8705
- RFC 9449 (OAuth 2.0 DPoP): https://www.rfc-editor.org/rfc/rfc9449.html

---

Related reading

- Phishing-Resistant Web Authentication
- Omnichannel Authentication
- Caller Authentication: Stop Vishing
- Recovery and Fallback Playbook
- Compliance Mapping: NIST and CISA
- M2M Authentication Without Secrets
- Lockstep: Dual Control
- Enterprise Passwordless Vendors Compared