Biometric Authentication in Financial Services

Regulatory Validation Report | FFIEC · OCC · Federal Reserve · CFPB · FTC

Issued by	Clavira Standards Program
Document Type	Regulatory Validation Report
Version	1.0 · March 2026
Applies	Biometric Evidence Standard (BES-1)
Document ID	BES-FIN-VAL-1.0

Document Scope

This report surveys federal regulatory guidance and enforcement posture relevant to the use of biometric authentication in financial services. It identifies evidentiary and control themes that may emerge from that guidance and maps them to the evidence architecture defined in the Biometric Evidence Standard (BES-1). It does not interpret state statutory obligations, which are addressed in jurisdiction-specific companion guides, and it does not state that any federal regulator has adopted BES-1 or any equivalent biometric evidence framework. This report does not determine whether any specific biometric authentication program is lawful, does not replace legal counsel, and does not convert inferred evidentiary expectations into binding regulatory requirements.

FFIEC and Banking Regulator Guidance on Authentication

Risk-Based Frameworks & MFA. U.S. banking regulators (OCC, Federal Reserve, FDIC) through the FFIEC endorse a risk-based, layered approach to digital authentication. The FFIEC's 2021 Authentication and Access to Financial Institution Services and Systems guidance emphasizes that banks should conduct periodic risk assessments to determine appropriate authentication controls. If those assessments show single-factor login is inadequate for a given risk, institutions are generally expected to implement multi-factor authentication (MFA) or comparably strong layered controls to mitigate unauthorized access, consistent with the institution's risk assessment and control environment.The guidance highlights the weaknesses in single-factor authentication and how MFA (or equivalent controls) can effectively reduce the risk of account compromise.

Biometrics as an Authentication Factor. The FFIEC guidance recognizes biometrics as a "something-you-are" factor that may be used within a multi-factor authentication program. It notes that multi-factor authenticators may include biometric identifiers alongside other factor types like passwords, tokens, or one-time codes. In practice, this means fingerprints, facial or voice recognition, and behavioral biometrics are acceptable elements of a bank's authentication program. The guidance describes behavioral biometrics software that analyzes how a user swipes or types as a way to continuously authenticate and detect anomalies. Biometric factors are supported as part of a layered security scheme, provided they are implemented securely.

Privacy & Security Expectations. The regulators stress stringent safeguards around authentication systems. The FFIEC guidance calls for controls like encryption, access limits, and audit logging to protect sensitive authentication data and systems. It advises deploying validated cryptographic tools and secure channels to prevent theft or replay of credentials. Cryptographic keys used in MFA devices should be stored in secure modules to prevent compromise. Audit trails and monitoring are similarly emphasized — banks should log authentication activities and review those logs to detect unauthorized access or fraud attempts. The guidance specifically notes that transaction and audit logs help identify intrusions, reconstruct events, and promote accountability. Banking regulators expect financial institutions to apply robust technical and governance controls — including authentication safeguards, secure storage, access restriction, monitoring, and audit practices — to authentication systems and the sensitive data those systems rely on. Where biometrics are used, those expectations apply to the authentication environment as part of the institution's broader control framework, rather than as a separate biometric-specific mandate.

Vendor Oversight. When banks rely on third-party providers for authentication solutions (including biometrics), regulatory guidance makes clear that risk management and oversight are required. The FFIEC urges institutions to include all users and access points — customers, employees, third parties, and service accounts — in their authentication risk assessments. This extends to cloud or vendor-hosted systems: banks must ensure vendors meet security expectations and report any unauthorized access incidents. The guidance explicitly calls for processes to monitor third-party access and to have providers notify the bank of security breaches in outsourced systems. Regulators expect financial institutions to apply their third-party risk management programs to biometric technology vendors — including due diligence, contractual security and privacy requirements, and ongoing oversight — just as they would for any critical service provider.

Use of Biometrics in Fraud Detection. The use of biometrics is also acknowledged in anti-fraud and identity verification contexts. The FFIEC guidance gives examples like voice biometrics in call-center authentication and out-of-band identity checks to thwart social engineering. A bank's call center may employ biometric voice recognition or secure video chat to confirm a caller's identity before resetting credentials. Behavioral biometric analysis (monitoring how a user behaves on an account) is cited as a tool to detect suspicious deviations that could indicate fraud. These examples illustrate that regulators recognize biometrics as one possible component in fraud prevention and anomaly detection when implemented within a sound, risk-based control framework.

CFPB Posture Relevant to Biometrics and Consumer Protection

Circular 2024-06 (Employment & FCRA). The Consumer Financial Protection Bureau (CFPB) has not issued rules specifically on customer-facing biometric authentication, but it has weighed in on biometric data in other contexts. In October 2024, the CFPB released Consumer Financial Protection Circular 2024-06, which addresses the use of biometrics and other data in employment-related background reports under the Fair Credit Reporting Act (FCRA). This guidance makes clear that compiling extensive dossiers on workers — including surveillance data and biometric information — can bring those reports under FCRA coverage. The CFPB emphasized that when employers use third-party services to track things like workers' keystrokes, facial images, or other biometric traits, those services are often acting as consumer reporting agencies subject to FCRA obligations. Biometric data used for eligibility decisions (like hiring or promotions) triggers the same consent, accuracy, and adverse action notice requirements as any consumer report. While this circular addressed employment-related background reports rather than customer-facing banking authentication, it indicates that the CFPB may treat biometric and surveillance-related data as materially sensitive when used in decision-making contexts governed by federal consumer-finance law.

No CFPB Biometrics Rule — UDAAP Still Applies. The CFPB has not promulgated any biometric-specific regulation for customer authentication in financial services. There is no CFPB rule mandating or prohibiting banks' use of fingerprints or face scans for login — those decisions are left to the institutions, guided by safety-and-soundness and privacy standards. However, the CFPB can still police biometric practices through its broad authority over Unfair, Deceptive, or Abusive Acts or Practices (UDAAP). CFPB guidance and enforcement actions indicate that poor data security or opaque data practices may be viewed as unfair to consumers. In 2022 the CFPB issued Circular 2022-04 explicitly stating that inadequate data protection (e.g., failing to secure sensitive consumer information) can constitute an unfair practice under the Consumer Financial Protection Act. This stance implicitly covers biometric data — if a bank misrepresents the security of its biometric login system or fails to protect biometric identifiers from breach, the CFPB could deem that an unfair or deceptive practice. The CFPB has highlighted stronger security controls, including multi-factor authentication in some contexts, as relevant to consumer-data protection. That does not create a biometric-specific authentication rule, but it does reinforce that weak security or misleading representations about authentication safeguards may create UDAAP risk. While no CFPB regulation specifically targets biometric authentication, general consumer-protection law still applies. Financial institutions should therefore assess whether biometric-authentication disclosures, security representations, and data-handling practices could create unfairness or deception risk under broader CFPB authority. These interpretations reflect general consumer-protection principles and should not be read as biometric-specific regulatory requirements. Applicability to a given implementation requires verification against primary-source guidance.

FTC Policy and Enforcement on Biometric Information

May 2023 Biometric Policy Statement. The Federal Trade Commission (FTC) has been increasingly vocal about risks posed by biometric technologies. In May 2023, the FTC issued a formal Policy Statement on Biometric Information Technologies, warning that the surge in biometric data use raises serious privacy, security, and bias concerns. The Commission made clear it is committed to combating unfair or deceptive acts or practices related to the collection and use of consumers' biometric information. This policy statement put companies on notice that false or unsubstantiated claims about biometric technologies (for example, claiming a facial recognition system is 100% accurate or bias-free without evidence) may violate the FTC Act's deception prohibitions. It also outlined factors the FTC will consider in determining if a company's use of biometric data is unfair, such as: failing to assess foreseeable harms from the technology, using biometrics for secret surveillance, or not vetting third-party vendors and downstream users for their handling of the data. The FTC has indicated through policy statements and enforcement actions that misuse of biometrics — including misrepresentation, poor security, or invasive implementation — can present unfairness or deception risk under Section 5 and may attract enforcement scrutiny.

Enforcement Actions and Deletion of Models. The FTC has taken enforcement actions in the biometrics arena, including cases requiring companies to delete algorithms or models derived from biometric data. In certain enforcement matters, the FTC has required not only deletion of the biometric data itself, but also destruction of models or algorithms developed using that data — a remedy sometimes referred to as "algorithmic disgorgement." A notable example is the FTC's action against Everalbum, Inc. (2021), in which the FTC alleged the company deceived users by applying facial recognition to photos without proper consent and retaining data indefinitely. The settlement required Everalbum to obtain express consent for any future use of facial recognition and to delete the facial images and all models or algorithms developed using those images. In its 2019 settlement with Facebook, the FTC imposed significant remedial obligations tied to facial recognition and biometric templates. Together with the Everalbum matter, these actions show that the FTC is willing to pursue aggressive remediation where biometric use is found deceptive or unfair. These enforcement actions underscore that the FTC will insist on full remediation of biometric data misuse where it determines a violation has occurred. The FTC views certain biometric practices (e.g., secretive face-scanning of consumers or retention of voiceprints without consent) as inherently risky, and it will use its authority under Section 5 of the FTC Act to police both deceptive statements and unfair data handling in the biometrics space.

Note: Algorithmic disgorgement has been applied in specific enforcement matters and represents an available remedy rather than a general regulatory requirement. Financial institutions should be aware of this enforcement precedent when assessing the downstream risks of biometric data collected without valid consent.

GLBA Interaction with State Biometric Privacy Laws

No Blanket Exemption via GLBA. It is sometimes assumed that being a financial institution under the federal Gramm-Leach-Bliley Act (GLBA) automatically immunizes a company from state biometric privacy laws. In practice, GLBA status does not automatically eliminate all exposure under state biometric privacy laws. Whether a given entity, activity, or data flow falls within an applicable state-law exemption remains a fact-specific and jurisdiction-specific question. BIPA itself contains an exemption for any financial institution subject to Title V of GLBA, and many banks have invoked that clause to avoid BIPA claims. However, recent case law shows that this exemption is not absolute in practice. Courts have required a company to truly qualify as a GLBA-regulated financial institution before BIPA is waived, and some entities have failed to meet that bar. In one case, a university's GLBA defense was rejected because the school could not prove it was significantly engaged in lending funds — a key criterion for being a financial institution under GLBA. This illustrates that merely citing GLBA is insufficient; an entity must fit GLBA's definitions, and courts are willing to limit the scope of the exemption.

Vendors and Partial Coverage. Even where a financial institution believes it falls within a GLBA-related exemption under a state biometric law, third-party vendors may not automatically share that position. Exemption analysis can differ by entity, activity, role in processing, and the statutory structure of the state law at issue. Financial institutions should therefore avoid assuming that vendor-side biometric processing inherits the institution's own exemption analysis without separate legal review.

Colorado HB 24-1130. Colorado's House Bill 24-1130 (effective July 2025) amends the Colorado Privacy Act to add biometric data protections. Similar to BIPA, it requires consent, disclosures, and retention policies for biometric identifiers. The Colorado law carries forward the CPA's existing exemptions (e.g., GLBA-regulated entities and data), meaning traditional banks may not be directly subject to the biometric provisions when handling customer data. However, that exemption is limited. A fintech or merchant outside GLBA's scope must comply with Colorado's rules, and even GLBA-covered banks could be subject to the law's requirements if they handle biometric data outside of consumer finance activities (for instance, employee biometrics or partner data that are not covered by GLBA). GLBA does not wholly preempt state biometric protections — financial institutions should carefully verify the applicability of each state law. Where no explicit exemption exists, or where exemption scope is uncertain, institutions should assess state biometric obligations alongside their existing GLBA and Regulation P responsibilities rather than assuming federal financial-privacy rules wholly displace state biometric requirements. Applicability of GLBA exemptions and their interaction with state biometric laws should be evaluated on a fact-specific basis and verified against current statutory and case law.

Control Themes Relevant to Biometric Authentication Programs

Across federal and state guidance, can lead to regulatory findings of deception or unfairness a set of recurring control themes can be identified for biometric authentication programs.

Informed Consent. Entities should not collect or use a person's biometric identifiers without prior notice and affirmative consent. Illinois BIPA requires that a private entity inform the individual in writing about the purpose and duration of biometric use, and obtain a written release before capturing biometric data. Colorado law similarly mandates specific disclosures and opt-in consent from consumers before collecting a biometric identifier. Even where no biometric-specific statute directly applies, transparency and consent-related controls may still be important from a fairness, disclosure, and defensibility perspective, particularly for customer-facing systems. Lack of proper notice or secret biometric tracking may contribute to findings of deception or unfairness depending on context.

Retention & Deletion Policies. Regulations consistently call for defining how long biometric data will be kept and when it will be destroyed. BIPA requires companies to develop a publicly available retention schedule and destruction guidelines, generally capping retention at three years after the data's last use. Colorado HB 24-1130 likewise obligates controllers to adopt a written policy establishing a retention schedule for biometric identifiers and including guidelines that require deletion by certain deadlines. The underlying principle is data minimization — biometric information should not be stored indefinitely. It must be purged once it is no longer necessary for the purpose collected (or once a statutory time limit is reached). Regulators and examiners increasingly focus on whether retention and deletion practices are documented, operationalized, and reviewable.

Secure Storage and Transmission. Because of its sensitivity, biometric data should be protected with strong security controls at rest and in transit. The GLBA Safeguards Rule (administered by the FTC for non-banks and mirrored by bank regulators) compels financial institutions to protect the security and confidentiality of customer information, which includes using encryption and access controls for sensitive data. Any biometric database should be encrypted, and access strictly limited to authorized personnel and systems. Secure enrollment channels are critical — for example, if customers provide face images or voiceprints via a mobile app, the connection should be encrypted to prevent eavesdropping. The FFIEC guidance further advises that cryptographic keys or reference data used in authentication be securely stored (e.g., in hardware security modules) to prevent tampering. Financial institutions should apply safeguards commensurate with the sensitivity of biometric-related systems and data.

Audit Trails & Monitoring. Whether required by statute or not, maintaining logs of biometric system use and monitoring for anomalies is a widely recommended control. The FFIEC guidance highlights monitoring, logging, and reporting of authentication activities as an important risk management practice. Each biometric login attempt, enrollment, or override should be logged, and those logs reviewed for signs of unauthorized access or fraud. Many biometric laws (like BIPA) do not explicitly mandate audit logs, but keeping evidence of when consent was obtained, when data was accessed or deleted, and how events were sequenced is important for demonstrating compliance. If an incident occurs, audit trails help forensic analysis and legal defense by showing what occurred. Regulators implicitly expect robust logging as part of sound internal controls, and the logs themselves must be protected from alteration. Where institutions need to demonstrate sequencing, scope, and retention execution, operational logs alone may be insufficient without an independent evidence architecture. Where institutions need to demonstrate

sequencing, scope, and lifecycle enforcement, operational logs alone may be insufficient without an independent evidence architecture.

Breach Response and Notification. Both federal guidance and state laws impose obligations around incident response for biometric data. The banking agencies' 2005 Interagency Guidance (still in effect) requires regulated institutions to have a response program for data breaches, including notifying customers and regulators in the event sensitive personal information (which would include biometric data) is compromised. In 2021 the OCC, Fed, and FDIC finalized rules obligating banks to notify their primary regulator within 36 hours of certain significant cyber incidents. On the state side, Colorado's new law specifically instructs that a biometric privacy policy must include a protocol for responding to a data security incident that may compromise biometric identifiers. All 50 states have general data breach notification statutes, many of which now treat biometric data as personal information that triggers individual notice if breached. In Illinois, the Personal Information Protection Act was amended to include fingerprints, retina and iris images, and facial scans in the definition of data that, if breached, requires consumer notification. Financial institutions using biometric-authentication systems should maintain incident-response procedures capable of addressing containment, investigation, internal escalation, and any regulator or consumer notification obligations that may arise under applicable banking, privacy, or breach-notification rules.

Quality and Accuracy Controls

Although not always mandated by statute, regulators and enforcement agencies are increasingly attentive to the accuracy, reliability, and potential bias of biometric technologies— particularly facial and voice recognition — because errors can lead to account lockouts, denied access, or adverse employment outcomes.

The FTC has warned that false or unsubstantiated claims about biometric accuracy or bias mitigation may constitute deceptive practices, and that failure to assess foreseeable harms may be considered unfair. As a practical governance matter, financial institutions should evaluate biometric technologies for accuracy, reliability, and known limitations; avoid overstating system performance in customer or employee disclosures; monitor for error rates and anomalous outcomes over time; and provide fallback authentication methods when biometric systems fail.

However, accuracy testing alone is not proof of lawful or compliant use. Even a highly accurate biometric system can expose an institution to regulatory or litigation risk if it cannot demonstrate that biometric data was collected after valid consent, that use was limited to the disclosed purpose, that retention and deletion followed documented policy, and that errors were handled in accordance with established procedures.

Quality controls address how well a biometric system performs. Regulators, auditors, and courts increasingly ask for evidence of how the system was governed. For this reason, financial institutions should distinguish between model quality controls and program integrity evidence. While biometric vendors may provide accuracy metrics, bias testing results, or model validation reports, institutions remain responsible for maintaining verifiable records showing when biometric systems were enabled, under what

authority, and how biometric data was governed throughout its lifecycle. This evidentiary gap is where an independent integrity layer becomes operationally relevant.

Turning Authentication Activity Into Exportable Evidence

Federal banking regulators and consumer protection agencies consistently emphasize monitoring, auditability, and documentation when biometric authentication is deployed. In practice, however, many financial institutions rely on operational logs — SIEM outputs, vendor dashboards, IAM reports — that were designed for security operations, not for regulatory examinations, audits, or litigation.

Logs show activity. Evidence demonstrates sequence, scope, and authorization.

Regulators, auditors, and courts increasingly ask for reviewable evidence rather than system activity alone.

Why Operational Logs Are Frequently Insufficient

Operational logs are typically:

- **Fragmented** across biometric vendors, identity systems, and security tooling
- **Mutable**, retained for limited periods, or difficult to version under typical administrative controls
- **Decoupled** from consent scope, declared purpose, and jurisdiction
- **Not structured** for export as time-ordered, reviewable evidence

As a result, institutions often struggle to demonstrate — after the fact — that consent was obtained before biometric enrollment, that biometric use matched the disclosed purpose, that retention and deletion occurred according to written policy, and that third-party vendors handled biometric data within contractual limits.

This gap is not a technology failure. It is an evidence architecture gap.

The Integrity-Layer Architecture

The evidentiary and control expectations that emerge from federal guidance and applicable state biometric obligations — including sequencing, purpose limitation, retention enforcement, vendor accountability, and exportable audit records — point toward a structural need that operational logs alone frequently cannot satisfy.

An integrity-layer architecture addresses this gap by operating parallel to existing biometric systems as a metadata-only evidence engine. The integrity layer does not capture biometric data, store biometric identifiers, or make authentication or identity decisions. Instead, it records compliance-relevant metadata — subject and provider identifiers, declared purpose and consent scope, jurisdiction and policy version, and timestamped lifecycle events (e.g., consent capture, enrollment, use, deletion) — and produces structured, exportable evidence artifacts.

The following table illustrates how evidentiary and control themes map to BES-1 primitives and corresponding evidence artifacts. It is illustrative and does not represent a regulatory standard. The BES-1 standard defines the structural properties of such an architecture through four integrity primitives:

Regulatory Expectation	Evidence Typically Requested	BES-1 Primitive	Output Artifact
Consent obtained before biometric capture	Timestamped consent record tied to enrollment	Event Attestation	Consent receipt / manifest
Purpose limitation	Evidence of declared purpose at time of use	Event Attestation	Purpose-bound event log
Retention & Deletion	Purpose-bound lifecycle log	SIEM Reconciliation	Deletion certificate
Auditability	Tamper-evident lifecycle history	Anchor to Ledger	Verifiable event timeline
Examinations & Discovery	Structured, exportable records	Proof Bundle	CSV / JSON / PDF Export

The integrity-layer model represents a conceptual architecture for producing verifiable biometric-governance records. Clavira is a reference implementation of one such architecture as a metadata-only sidecar evidence layer aligned with BES-1.

Logs vs. Evidence

- Policies describe what should happen.
- Logs show what systems recorded.
- Proof Bundles show what can be demonstrated, reviewed, and defended.

An integrity layer does not replace biometric vendors, IAM platforms, or SIEM tools. It provides an independent evidence architecture that binds consent, purpose, and lifecycle events into a form suitable for regulatory review and legal scrutiny.

Algorithmic Disgorgement and Chronology Risk

In certain enforcement matters, regulators have required not only deletion of biometric data collected without valid consent, but also destruction of models or algorithms derived from that data. The FTC's Everalbum matter (2021) required destruction of facial recognition models built from improperly collected images. The FTC's 2019 Facebook settlement imposed significant remedial obligations related to facial recognition systems and associated data.

These enforcement actions show that deletion of downstream models or algorithms can be an available remedy where regulators determine biometric data was collected or used unlawfully or deceptively. This precedent has implications for financial institutions deploying biometric systems: if an institution cannot demonstrate that biometric inputs were collected under valid consent and used within declared scope, downstream models or derived work product may be subject to remediation orders depending on enforcement findings.

An integrity-layer evidence architecture does not inspect or control model training. However, it can help institutions evidence chronology by preserving cryptographically verifiable records showing when consent was obtained, when biometric enrollment occurred, and what purpose and scope were declared at each stage. This event-level chronology may be relevant when institutions must demonstrate that biometric inputs were not used before the required authorization, disclosure, or governance controls were in place.

Third-Party Vendor Oversight

Regulatory guidance emphasizes ongoing monitoring of third-party service providers. In biometric programs, institutions often lack defensible records showing how vendors handled consent, retention, or deletion.

An integrity-layer architecture can support vendor oversight by attesting to vendor-emitted compliance events (metadata only), reconciling vendor logs against institutional records, and producing shared evidence artifacts for audits and contract enforcement. This allows institutions to demonstrate oversight rather than relying on contractual assertions alone.

Limitations

An integrity-layer evidence architecture does not collect or store biometric identifiers, evaluate biometric accuracy or bias, make authentication or identity decisions, or guarantee regulatory compliance. It also does not convert supervisory guidance, enforcement posture, or framework compatibility into a binding regulatory requirement.

Key Takeaway

As biometric authentication expands across financial services, the compliance challenge is no longer limited to how well systems work, but whether institutions can prove how those systems were governed.

Federal regulators and enforcement agencies increasingly focus not only on whether authentication and governance controls exist, but on whether institutions can demonstrate how those controls operated in practice. This creates an evidentiary burden: institutions must be able to reconstruct the sequence of notice, consent, authentication events, retention enforcement, and deletion actions.

An integrity-layer evidence architecture provides a structural mechanism for producing such records without altering underlying biometric systems. Clavira is a reference implementation of this architecture as a metadata-only sidecar evidence layer aligned with BES-1. A proof layer does not replace controls. It can make controls more reviewable and more defensible.

Companion Documents

Biometric Evidence Standard (BES-2026-01)

BIPA Evidence Interpretation Guide (2026)

Colorado HB 24-1130 Evidence Interpretation Guide (2026)

BIPA Evidence Readiness Checklist (2026)

Colorado HB 24-1130 Evidence Readiness Checklist (2026)

Biometric Audit Trail Documentation — Operational Guide (2026)