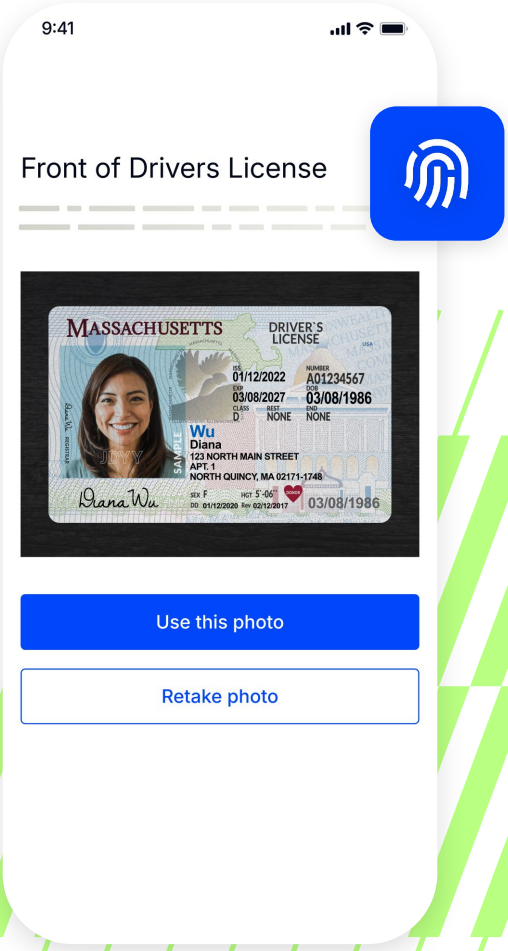
Proof

NACHA Phase 2 Compliance Guide

Everything you need to know for implementation and ODFI audits



Contents

NACHA Phase 2 Compliance

June 22 is fixed. NACHA Phase 2's False Pretenses mandate arrives whether your firm is ready or whether it is scrambling.

Every mid-market recordkeeper will be subject to it.
Every ODFI will enforce it. A
nd the standard it sets - NIST 800-63 IAL2, with government ID verification, biometric binding, and machine-readable audit evidence - rules out most of what firms currently rely on.

This playbook covers two things: how to implement IAL2-compliant real-time identity verification before the deadline, and how to organize your audit evidence so your ODFI review goes the way it should.

What the false pretenses mandate actually requires

The compliance floor

NACHA Phase 2's False Pretenses mandate requires firms to maintain documented "Risk-Based Procedures" specifically designed to identify and prevent impersonation fraud. The compliance floor is NIST 800-63 IAL2.

In plain terms:

- **Document verification:** Remote identity proofing with a government-issued ID
- **Biometric binding:** A live facial biometric match at the moment of the transaction
- **Liveness detection:** Technical controls that defeat deepfakes and replay attacks

These requirements define the standard against which your ODFI will evaluate your fraud controls.

What fails the audit

The following approaches are explicitly insufficient under the False Pretenses mandate:

- **Knowledge-based authentication (KBA):** Confirms that someone knows certain information about an account holder, without verifying the person actually initiating the transaction.
- **SMS OTP:** Confirms device access, without verifying identity.
- **eSign and generic RON platforms:** Verify a signature without generating IAL2-compliant audit evidence.
- **Manual review with paper logs:** Cannot produce machine-readable evidence for ODFI auditors. "Best efforts" language is explicitly rejected under Phase 2.

The penalty structure

Under Phase 2, your Originating Depository Financial Institution bears direct legal liability for your fraud controls. Any NACHA violation triggers mandatory review of your entire fraud control stack. Banks will exit relationships with non-compliant originators rather than absorb the regulatory liability. Loss of your ODFI relationship means loss of ACH access.

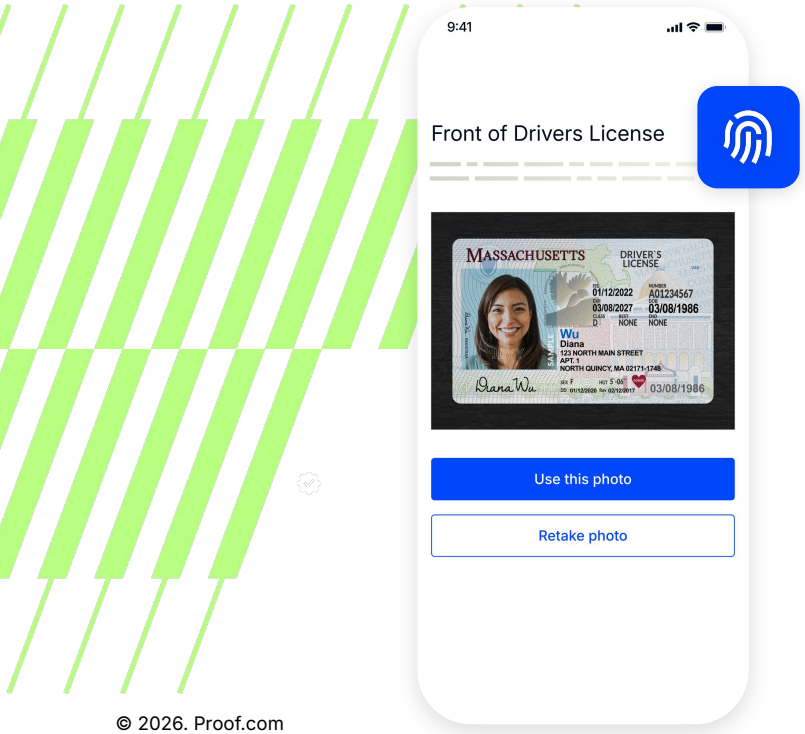
The penalty structure escalates quickly:

Class 1 **Warning/Minor**	Up to **$1,000** for initial failure to document a process
Class 2 **Repeat/Major**	Up to **$5,000** per occurrence
Class 1 **Egregious/Willful**	Up to **$500,000** per month for systemic failures

Where most firms stand today

Most mid-market recordkeepers enter June 22 with one of three compliance postures. Knowing which one applies to your firm determines how much of the implementation path below you need.

Posture A and B require a full implementation path. Posture C requires a targeted gap assessment and workflow expansion.



Posture A: Manual review dependent

The firm uses KBA, SMS OTP, or manual review for high-risk transactions. Fraud is flagged, but transactions proceed. There is no machine-readable audit trail. This posture fails the False Pretenses audit on Day 1.

Posture B: eSign or generic RON deployed

The firm has digitized document workflows but relies on signature verification rather than identity verification. Biometric binding is absent and ODFI-defensible evidence is not generated. This posture partially satisfies Phase 2 but fails the biometric binding requirement.

Posture C: IAL2 partially deployed

The firm has identity verification in some workflows but has not applied it consistently across all disbursement types. Inconsistent application fails the "documented and consistent procedures" requirement.

Proof

Audit evidence: What your ODFI will require

What Proof generates per session

Every Proof IAL2 session produces the following automatically:

Immutable session recording
Full video record of the identity verification session, tamper proof and timestamped

Government ID verification record
Document match result with full audit metadata

Biometric match record
Live facial biometric confirmation tied to the government ID

Liveness detection result
Technical confirmation that deepfake and replay attack controls executed

Cryptographic signature
Session record cryptographically signed to the verified identity, AI-proof and digitally verifiable

Machine-readable compliance evidence
ODFI-formatted audit artifacts generated for every session

What your ODFI will assess

When your ODFI conducts a Phase 2 review, their assessment covers three areas:

01

Documented procedures
Can you produce written Risk-Based Procedures describing your identity verification process for each disbursement workflow type?

02

Consistent application
Can you demonstrate that these procedures apply consistently across all relevant ACH entries, rather than selectively?

03

Auditable evidence
Can you produce machine-readable records confirming that IAL2 verification executed at the transaction layer?

Proof generates the evidence for item three automatically. Items one and two require your compliance team to produce written documentation. The elements below cover what those written procedures must include.

Risk-based procedures

Your written procedures should address the following:

- The transaction types subject to IAL2 verification
- The identity verification standard applied: NIST 800-63 IAL2
- The platform used to execute verification: Proof
- How verification results are recorded and retained
- The escalation procedure for failed or incomplete verification attempts
- How procedures are reviewed and updated on an ongoing basis

What passing looks like

A passing ODFI audit under Phase 2 means one thing: you can demonstrate that you know who initiated every high-risk transaction, and you can prove it with evidence that survives scrutiny.

Every Proof session generates a cryptographically signed, tamper-proof record tied to a government-verified, biometrically confirmed identity.

The evidence chain is machine-readable and ODFI-formatted from the moment the session closes.

Your June 22 readiness checklist

Pre-Implementation

- ❑ IAL2 Readiness Gap Assessment completed
- ❑ All transaction types requiring IAL2 at the disbursement layer identified
- ❑ Current identity verification procedures documented
- ❑ Technical scoping call with Proof scheduled
- ❑ ODFI Relationship Manager briefed on upcoming compliance posture change

Implementation

- ❑ Proof IAL2 sessions activated across all target transaction types
- ❑ API integration or EasyLink deployment confirmed live
- ❑ Session recording, audit metadata, and Certify cryptographic signing confirmed active
- ❑ Financial advisor and operations team training completed
- ❑ Test sessions run and audit artifacts verified

Audit-Readiness

- ❑ Written Risk-Based Procedures documented and filed
- ❑ Consistent application confirmed across all relevant ACH entry types
- ❑ Machine-readable evidence accessible and ODFI-formatted
- ❑ Audit file assembled: written procedures, session evidence, and gap assessment results
- ❑ Escalation procedure documented for failed verification attempts
- ❑ ODFI Relationship Manager briefed and relationship confirmed

Day 1 Confirmation (June 22)

- ❑ All high-risk transactions routing through Proof IAL2
- ❑ Audit evidence generating automatically for every session
- ❑ Board and risk committee notified of compliance posture
- ❑ ODFI confirmation of Phase 2 readiness on file

The June 22 deadline is fixed.
The implementation pathway exists.
The only variable is when you start.

Calculate your ODFI exposure risk

Talk to Proof

About Proof

Proof provides the high-assurance digital identity infrastructure for the internet's most important transactions. As a digital identity issuer, Proof verifies who is behind a critical action and ensures every interaction is continuously secured through our Identity Authorization Network. Our platform empowers organizations to authorize high-stakes actions and preserve verifiable records that are both defensible and authentic. To date, Proof has secured over $640B in transactions across critical workflows including account recovery, financial approvals, and the Notarize Network, the world's largest on-demand notary platform. Learn more at proof.com.