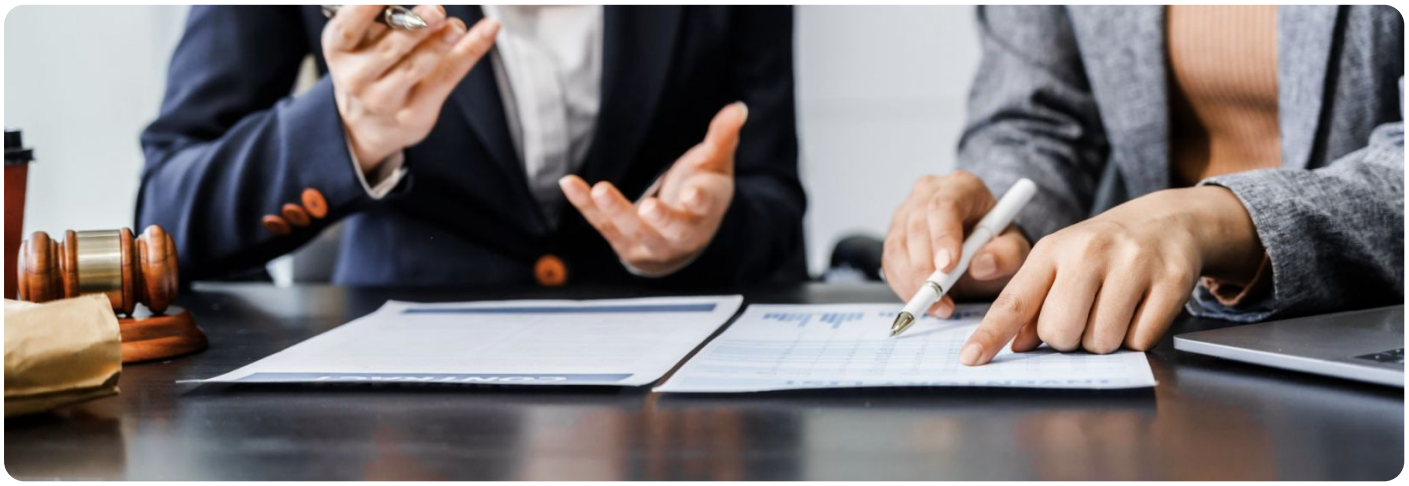
Proof

NACHA Certification Pathway Guide

From readiness assessment through ongoing compliance

Contents

A new compliance posture



June 22, 2026 is not the end of a process. It is the beginning of a compliance posture your firm will be measured against from that point forward.

NACHA Phase 2's False Pretenses mandate changes how identity verification works at the transaction layer for every mid-market recordkeeper in the country.

By June 22, firms that process disbursement transactions need documented procedures, deployed IAL2-compliant controls, and machine-readable audit evidence they can hand to an ODFI auditor on demand. Firms that cannot do all three are exposed from Day 1.

This guide is for the firms getting compliant before that deadline, and for the compliance, operations, and banking relationship teams building the posture that holds after it.

It covers five stages along the pathway to compliance, from the exposure assessment that tells you where you stand all the way to the ongoing maintenance that keeps the compliance posture current.

Each stage has a defined owner, a clear output, and a gate that marks completion. Work through them in order, and your firm arrives at June 22 with a compliance posture that is documented, deployed, and defensible.

What "NACHA Phase 2 Compliant" actually means

NACHA Phase 2 compliance is a documented, defensible posture that your ODFI can examine, verify, and confirm. Your firm builds it by deploying identity verification controls that meet the IAL2 standard, writing the procedures that describe how those controls work, generating machine-readable audit evidence at the transaction layer, and maintaining a record that survives scrutiny at any point going forward.

In practice, compliance means you can answer yes to three questions your ODFI will ask:

1. Do you have written, documented Risk-Based Procedures describing how you verify the identity of transaction initiators?
2. Are those procedures applied consistently across all relevant ACH entries?
3. Can you produce machine-readable evidence confirming that IAL2 verification executed at the transaction layer for each high-risk transaction?

This guide maps the pathway to yes on all three, and what it takes to hold that position.

The five stages of the certification pathway

Stage 1: Exposure assessment

The pathway begins with an honest accounting of where your firm stands against the False Pretenses mandate.

The assessment covers your current identity verification stack across every transaction type that triggers IAL2 requirements, and produces a written gap analysis that becomes the foundation of your ODFI evidence file.

What the assessment must cover:

- Every transaction type subject to NACHA Phase 2's "money-out" definition
- The identity verification controls currently applied to each
- Whether those controls meet NIST 800-63 IAL2 requirements: government ID verification, live biometric binding, liveness detection
- Whether your current controls generate machine-readable audit evidence
- Whether your written procedures, if they exist, accurately describe what your controls actually do

The output is your gap matrix.

Owner

Chief Compliance Officer, with COO input

Gate

Documented gap analysis showing current posture vs. IAL2 requirements

End result

A written gap analysis exists, has been reviewed by your CCO, and the scope of IAL2 deployment required has been confirmed.

Most mid-market firms enter this assessment relying on manual review, knowledge-based authentication, or eSign workflows. These controls fall short of the IAL2 standard and cannot produce the machine-readable audit evidence Phase 2 requires. Firms with partial IAL2 deployment face a narrower scope, but inconsistent application still fails the "documented and consistent procedures" requirement.

Stage 2: Procedure documentation

The False Pretenses mandate requires documented procedures, which means documentation must exist before your controls go live.

Your written Risk-Based Procedures are a formal compliance document, and your ODFI will request them during any Phase 2 review.

Required documentation elements:

- The transaction types subject to IAL2 verification, defined specifically
- The identity verification standard applied (NIST 800-63 IAL2) and the platform used to execute it (Proof)
- How verification results are recorded, retained, and made accessible for audit
- The escalation procedure when verification attempts fail or are incomplete
- The review cycle for the procedures themselves: who reviews them, how often, and what triggers an off-cycle review

Owner

Chief Compliance Officer

Gate

Written Risk-Based Procedures reviewed, approved, and filed

End result

Written procedures have been reviewed by your compliance team, approved by the CCO, and filed in your compliance management system.

Stage 3: Technical deployment and validation

This stage converts your gap analysis and written procedures into a live, running system.

Proof IAL2 sessions are activated across all transaction types identified in Stage 1, and validation confirms that evidence is generating correctly before June 22.

Deployment validation must confirm:

- Proof IAL2 sessions are routing for every transaction type identified in your gap analysis
- Session recording, government ID verification, biometric match, liveness detection, and Certify cryptographic signing are all active and generating correctly
- Audit metadata is machine-readable and formatted for ODFI review
- The participant experience has been tested end-to-end with a representative transaction
- Financial advisor and operations staff have been trained on the new workflow

Owner

COO or Head of Operations, with IT

Gate

Live IAL2 sessions confirmed across all in-scope transaction types, with test evidence reviewed

End result

Test sessions have been run across all in-scope transaction types, audit artifacts have been reviewed for correct formatting, and your operations team has confirmed live deployment.

Proof

Stage 4: ODFI communication and relationship validation

Your ODFI bears direct legal liability for your fraud controls under Phase 2.

Proactive communication before June 22 is a relationship-preservation strategy: banks will exit originator relationships rather than absorb regulatory liability, and the firms that arrive at the deadline with documented compliance already on file with their ODFI are the ones that keep their ACH access intact.

What to communicate to your ODFI:

- Your written Risk-Based Procedures (the document from Stage 2)
- Your deployment confirmation: IAL2 sessions are live across all in-scope transaction types
- A sample Proof session audit artifact, demonstrating what evidence your ODFI will receive on any session they request
- Your escalation procedures for failed verification attempts
- Your procedure review cycle and who owns ongoing compliance

The goal is written acknowledgment that your ODFI has reviewed your compliance posture and confirmed readiness. This confirmation belongs in your compliance file and should be in place before June 22.

Owner

ODFI Relationship Manager, with CCO and COO

Gate

Written acknowledgment from your ODFI of your Phase 2 compliance posture

End result

Your ODFI has received your compliance documentation, reviewed a sample audit artifact, and provided written confirmation of your Phase 2 readiness posture.

Stage 5: Ongoing compliance maintenance

June 22 is a deadline, and compliance is a posture that must be maintained. The False Pretenses mandate carries no expiration date, and ODFI reviews can be triggered at any time by a NACHA violation anywhere in your originator relationship. Firms that achieve compliance by June 22 must also demonstrate consistent application going forward.

Ongoing compliance requires:

Annual procedure review
Written Risk-Based Procedures should be reviewed at least annually, updated to reflect any changes in transaction types, platforms, or regulatory guidance, and re-filed with your compliance management system. The reviewer and date of review should be documented.

Trigger-based re-assessment: Certain events require an immediate review of your compliance posture. These include adding new transaction types to your ACH program, changing your identity verification platform, changes to NACHA's operating rules, and any ODFI audit inquiry.

Evidence retention
Proof session records are immutable and tamper-proof, but your firm is responsible for confirming that evidence remains accessible at the retention horizon your ODFI requires.

Consistent application monitoring
Compliance requires consistent application across all relevant ACH entries. Firms should maintain a process for confirming that every in-scope transaction type routes through IAL2 verification, with documented justification for any exceptions.

Owner

Chief Compliance Officer

Gate

Annual procedure review completed; evidence accessible; change triggers documented

End result

The compliance posture is maintained through regular review cycles, year over year.

Summary

Stage	Owner	Gate	End Result
1: Exposure Assessment	CCO, COO	Gap matrix reviewed and scope confirmed	Written gap analysis
2: Procedure Documentation	CCO	Procedures filed in compliance management system	Written Risk-Based Procedures
3: Technical Deployment	COO, IT	Test artifacts validated across all transaction types	Live Proof IAL2 sessions
4: ODFI Communication	ODFI RM, CCO, COO	Written ODFI confirmation on file	ODFI briefing package
5: Ongoing Maintenance	CCO	Review cycle documented and active	Annual review, change log

The two-week implementation window assumes Stage 1 begins immediately. Firms that complete Stage 1 today have a viable path through Stages 2, 3, and 4 before June 22. Every day of delay compresses the time available for each subsequent stage.

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.