Proof

The ODFI Audit

What Your Bank Will Ask Before June 22

Your bank is currently evaluating its own exposure to the NACHA Phase 2 mandate. Because the ODFI carries the ultimate liability for fraudulent ACH originations, their risk committees are moving beyond simple policy reviews. They are now looking for proof of technical execution.

When your relationship manager calls to discuss your "Risk-Based Procedures," they will likely lead with these five questions to determine if your firm remains a defensible risk.

01 Can you provide a machine-readable audit trail for every high-value transaction?

The bank needs more than a policy manual. They require a specific record of the identity verification event that occurred at the moment of the transaction. If your audit trail consists of a timestamped manual review, it likely fails the new standard for "commercially reasonable" fraud detection.

02 Does your process include hardware-backed liveness detection?

Standard MFA and Knowledge-Based Authentication (KBA) are now vulnerable to generative AI and automated injection attacks. Your bank will ask if you have a technical control in place to confirm a live human is present during the disbursement request.

03 Is your identity execution layer aligned with the NIST 800-63 IAL2 standard?

IAL2 is the benchmark for high-confidence identity proofing. The bank will check if you have bridged the gap between the digital request and the physical person through government ID verification and biometric binding.

04 What percentage of your high-value volume still relies on manual signature matching?

Every "analog hole" in your process represents a liability for the ODFI. Banks are increasingly flagging manual reviews and physical mail-in forms as high-risk vulnerabilities that must be closed to maintain your current origination limits.

05 Can you demonstrate a real-time block on impersonation attempts?

The False Pretenses rule requires procedures that prevent fraud, rather than just identifying it after the money has moved. Your bank will ask if your system can programmatically halt a transaction based on a failed identity check.

An ODFI audit is a defensive move by the bank to protect its own balance sheet. If you cannot answer these questions with technical certainty, the bank may choose to lower your origination limits or increase your reserve requirements to hedge their risk.

Proof provides the IAL2-compliant execution layer you need to answer these questions confidently. We help you move from a policy of "assuming risk" to a state of "executing identity," providing the machine-readable evidence your bank requires to keep your money moving.

Calculate your exposure

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.