Proof℠

Nacha 2026 checklist

Nacha's fraud monitoring rules now cover every business that sends ACH payments. Use this list to check your controls.

WHAT THE RULES ASK

- Risk-based processes to catch payments that are unauthorized or made under false pretenses
- A review of those processes at least once a year
- False pretenses includes business email compromise, vendor impersonation and payroll impersonation
- In effect for all non-consumer originators since June 19, 2026, and for the largest since March 20

Source: Nacha Operating Rules, fraud monitoring

THE CHECKLIST

Assess risk

- [ ] Your risk assessment separates higher-risk payments, like new payees, changed bank details and large amounts, from routine ones
- [ ] Monitoring covers the credit payments you send, as well as the returns you receive

Bank-detail changes

- [ ] Every change to payee bank details goes through a documented change control
- [ ] The control confirms who requested the change, and that they can act for the payee
- [ ] Confirmation never relies only on the email or phone number in the request

Approval and release

- [ ] Payments above your threshold need an approver whose identity is checked at release
- [ ] New and changed payees get dual control before the first payment

Evidence and review

- [ ] Each check leaves a record of who requested, approved and released the payment
- [ ] You can produce those records for your bank, your auditors and your annual review
- [ ] Procedures are reviewed at least once a year for new attacks, like deepfaked voices

WHERE PROOF FITS

Proof verifies the person behind each bank-detail change and high-value approval with a face scan, and keeps a signed record of who acted and for which company. Your team can use that record in its monitoring and annual review.

Book time with our team to walk through your controls. proof.com/treasury