

Last Modified on 10/28/2026 1:18 pm MDT

Preventing authority and configuration gaps before payment services go live

A payroll deadline arrives before the authority package is complete. An implementation team copies an existing administrator profile. Payments begin, and the temporary arrangement becomes permanent. If fraud follows, the bank must explain who authorized access and why the system allowed the transaction. Treasury onboarding should produce that explanation before the service is activated.

Verify who can bind the customer

The person coordinating implementation may be a controller, bookkeeper, accountant, consultant, or platform employee. That role alone does not establish authority to bind the customer entity. Confirm the legal customer, account ownership, authorized signers, and the organizational basis for their authority. Then obtain a separate administrator designation identifying the powers delegated through the treasury service.

If the authority record is incomplete, restrict activation to capabilities that the completed documentation supports. A bank may permit reporting access while withholding payment origination if its own risk review supports that approach. Record the restriction and the remaining conditions. Relationship familiarity and a pressing payroll deadline do not resolve an authority gap.

Verify changes that can transfer control of the account

An administrator may be able to add users, reset credentials, create beneficiaries, issue API credentials, or raise transaction limits. Document which powers the customer delegates and which changes remain subject to bank approval. The bank should be able to show how the initial administrator was appointed and how each successor obtained authority.

Require independent verification for a new administrator, a security downgrade, a new external account, and limit increases above the bank's stated threshold. Contact a customer representative authorized to approve that change through a preverified channel, independent of the request and any newly supplied contact details. An email from the existing administrator's address is not independent verification. Log the requested change, approver, verifier, time, method, and outcome. These are recommended controls; the bank should define their precise scope in policy and align any contractual promise with the process it can perform.

Apply the same independence to the verification itself. If the request changes both an administrator and the telephone number used for callbacks, verify against the prior trusted record rather than calling the new number. A documented emergency process should identify who may approve an exception, what access is restricted, and when the exception expires.

Make the security election an affirmative record

Use a service election that lists available authentication methods, selected controls, declined alternatives, transaction limits, and any agreed callbacks. Identify the specific procedure version and obtain acceptance from a person with authority. Distinguish authentication factors from transaction controls: two passwords do not create two different factors, and an after-the-fact review cannot prevent an already settled payment. [1, 2]

If a customer declines dual approval, first decide whether the bank will offer the requested service at all. If it will, document the stronger procedure offered, the customer's election, the residual risk approval, and any lower limit or preventive control required. Article 4A gives particular significance to a suitable procedure offered and declined, together with the required written agreement. A signed rejection form alone does not establish every statutory condition or excuse the bank's failure to follow the selected procedure. [2]

Configure permissions for the actual workflow

Confirm who prepares, approves, and releases payments; who adds beneficiaries; and who can change those permissions. If one person can reset a second user's credential and then approve that user's payment, nominal dual control may provide little protection. Test the route by which the control could be bypassed, including support-assisted resets and API access. The FFIEC guidance provides a risk-based foundation for this access review. [3]

Document permitted exceptions and their expiration. A temporary limit increase should

return to its approved level automatically where the system supports it; otherwise assign the reset to a named person and verify completion. Do not copy another customer's profile without reviewing each capability and limit.

Reconcile the signed package to the activation record

Before payments go live, an independent reviewer should compare the signed documents with the configuration export. The reviewer should verify the customer and accounts, enabled services, administrators, users or machine identities, security procedure, limits, and approved exceptions. Any unexplained mismatch should block the affected capability until it is resolved.

Retain an activation certificate that identifies the documents and versions reviewed, configuration evidence, tester, reviewer, activation date, and unresolved items for restricted services. It can be an internal record. Its purpose is to connect the customer's authority to the permissions actually released.

The evidence an onboarding file should contain

Use the control matrix below as an implementation checklist. Assign one owner to each record and link it to the customer file. If a processor retains the authoritative logs, establish the bank's access and retrieval rights before relying on that arrangement.

Control question	Required record	Verification before activation
Who binds the entity	Organizational authority and signer record	Entity and signer match the customer and agreement
Who controls access	Administrator designation and change history	Appointment and sensitive changes independently verified
Who releases payments	User and machine entitlement export	No unintended bypass of approval rules
How orders are verified	Accepted security election	Selected procedure matches the active configuration
What exposure is allowed	Limits and exception approvals	System limits tested and exceptions time-limited
Who approved activation	Activation certificate and evidence links	Reviewer resolved material discrepancies

Repeat the relevant checks when administrators, platforms, payment capabilities, or material limits change. Onboarding is the first configuration decision, not the last. A bank should be able to reconstruct the authority and settings in effect on the date of a disputed payment, even after personnel and vendors have changed.

The management deliverable

- Require verified entity and signer authority before activating services that depend on it.
- Maintain an independently verified change record for administrator succession and other specified high-risk changes.
- Release payment capability only after a reviewer reconciles the accepted documents to the system configuration.

Sources and application

[1] [**UCC 4A-201**](#). Definition of security procedure.

[2] [**UCC 4A-202**](#). Authorized and verified payment orders and commercial reasonableness.

[3] [**FFIEC authentication guidance**](#). Authentication and Access to Financial Institution Services and Systems, August 2021. Risk-based guidance covering customers, staff, third parties, and system access.

Reviewed through October 24, 2026. General information; apply governing law and institution-specific facts. Recommended controls and examples are not universal legal requirements. Article 4A links illustrate the D.C. enactment; check governing state law and applicable federal and system rules.
