

Last Modified on 10/26/2026 12:33 pm MDT

Coordinating agreements with authority records and security elections

A treasury document suite should let the bank answer a fraud claim without assembling the parties' agreement from old forms and scattered emails. It needs a defined hierarchy, separate records for authority and access, service-specific payment terms, and evidence of the version and security procedure in effect when the disputed instruction arrived.

Give every document a defined job

Start with an inventory of the deposit agreement, digital banking terms, treasury master, service schedules, elections, implementation forms, fee schedules, and negotiated amendments. Identify duplicate definitions and conflicting standards. The most consequential conflicts usually concern authority, payment security, liability, notice, and amendment rights.

The master agreement should establish common terms. A schedule should address the service's payment law, cutoffs, processing rules, finality, fees, and service commitments. Implementation records should identify the accounts, people, limits, and selected controls. Use the document inventory below to assign an owner and required evidence to each layer.

Document	Primary purpose	Evidence to retain
Master agreement	Common terms and the contractual hierarchy	Accepted version and any negotiated amendments
Service schedule	Rail-specific processing rules and commitments	Enabled service and effective schedule

Document	Primary purpose	Evidence to retain
Authority records	Who can bind the customer and appoint administrators	Signer authority and effective delegations
Security election	Agreed payment verification procedure	Options offered, selected procedure, and authorized acceptance
Implementation record	Actual accounts, permissions, and limits	Configuration export, testing, and activation approval

Separate legal authority from system permissions

Corporate authority to sign the agreement, delegated authority to administer services, and permission to submit a transaction are different questions. Obtain the authority record appropriate to the customer entity. Document administrator appointments and their limits separately. Then configure individual and machine access within that delegation. A user list alone does not establish that the customer authorized the contract or the administrator.

When a customer disputes an instruction, the bank should be able to trace the user or credential back to an effective delegation. Actual authority and an agreed Article 4A security procedure offer different legal routes for analyzing an order. The suite should support both without declaring that possession of credentials conclusively establishes authority in every case. [1, 2]

Record the actual payment security procedure

Use a short election form for each payment channel, with an attachment where the procedure needs more detail. Identify the customer and service, the procedure version, authentication methods offered and selected, maker and approver rules, transaction and aggregate limits, and the exact circumstances for any agreed callback. Record who may change those settings and how a change becomes effective. A general reference to commercially reasonable security is not the procedure itself. [1]

Keep customer-elected controls distinguishable from internal monitoring. If the bank commits to a callback for every order above a threshold, the system and staffing must support that promise. Calling a control discretionary will not erase an actual agreement, statutory duty, or good faith obligation. Review marketing and operating practices alongside the written terms. [2]

If dual approval is declined, record whether the bank accepts the residual risk and what preventive limit or verification is required. A next-day review may help detect loss, but

it cannot stop an immediate payment. Document the customer's authority to make the election and any written agreement required for the bank's Article 4A position. A checkbox form is evidence of an agreement, not a statutory safe harbor. [2]

State which terms prevail

Define precedence by subject. A negotiated amendment should identify the provisions it changes. A service schedule can control service-specific matters, and the security election can control the agreed procedure. An implementation form should configure the service without changing risk allocation unless it expressly does so and is accepted through the bank's amendment process. Explain how deposit terms continue to govern account matters.

Incorporate payment system rules with attention to the roles they govern. Customer compliance with applicable Nacha obligations should not be confused with a promise that the customer assumes the bank's own network duties. Nor can a private hierarchy override mandatory law or a binding funds transfer system rule. [3]

Preserve the agreement that applied to the transaction

Retain the executed or electronically accepted master, schedules, election, authority records, and amendments as a customer-specific package. For electronic amendments, preserve the notice, delivery method, effective date, and contractual basis for acceptance. Keeping only the current blank form leaves the bank unable to establish what governed an earlier transaction.

Maintain an inventory showing the form owner, version, approval date, covered services, superseded forms, and required activation documents. Link the inventory to customer adoption status. A revised form is not implemented merely because the template repository contains it.

Migrate legacy customers through a recorded process

Prioritize customers whose signed terms contradict the live security configuration, whose high-value services lack an identifiable election, or whose administrator authority is unclear. Compare the actual documents before deciding whether amendment notice is enough. A bank should not assume that a platform conversion or service addition silently replaces every legacy term.

For each migration group, record the old agreement, proposed change, required assent, notice date, effective date, and implementation checks. Require affirmative acceptance where the existing contract or applicable law requires it. Before closing the migration,

sample completed customer files and compare them with the system. FFIEC authentication guidance supports a risk-based review of access controls, including access by third parties. [4]

The management deliverable

- Adopt a document map showing the job, precedence, and owner of each form.
- Require a completed security election and authority trail before activating payment capability.
- Maintain customer adoption records and test whether executed terms match the live 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] **UCC 4A-501**. Variation by agreement and effect of funds transfer system rules.

[4] **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.
