

Last Modified on 10/29/2026 1:57 pm MDT

Using payment law and contract evidence to support loss allocation

A treasury agreement can improve the bank's position in a payment dispute only if it describes a process the bank follows. Clear authority records, an identifiable security procedure, and service-specific loss allocation usually matter more than an expansive disclaimer. Draft the agreement around the payment law, then test it against onboarding and operations.

Identify the payment law before allocating the loss

For funds transfers within its scope, Article 4A distinguishes an actually authorized payment order from an unauthorized order that may nevertheless be effective against the customer under an agreed security procedure. Valid credentials are evidence, not an automatic bank victory. The applicable analysis includes commercial reasonableness, good faith, compliance with the agreed procedure and applicable written restrictions, and the protections in section 4A-203. [1, 2]

Consumer electronic transfers require a separate coverage analysis. Regulation E applies to covered consumer accounts and transfers, with exclusions for certain services. A consumer account does not make every transfer subject to Regulation E, and a business banking interface does not eliminate consumer protections that otherwise apply. Route the service and dispute to the correct rules before applying a contractual deadline or customer liability clause. [3]

Make the security procedure provable

The customer file should identify the selected procedure, alternatives offered, authorized election, and configuration in effect. Where the bank relies on a customer's rejection of a stronger procedure, preserve the record required for that argument. Commercial reasonableness depends on the statutory factors and governing law; the

agreement cannot make every offered procedure reasonable merely by declaring it so. [1]

State the customer's duties to protect credentials, devices, administrator accounts, machine credentials, and contact channels. Define how compromise is reported and when revocation becomes effective. Preserve the bank's right to suspend or require additional verification where lawful. Then test whether callbacks, dual approval, and limits in the accepted procedure operate as written.

Distinguish account takeover from an authorized scam payment

A fraudster using stolen credentials and an employee intentionally sending a payment after receiving a fraudulent vendor email raise different questions. The agreement should address independent verification of changed payment details and the customer's responsibility for its vendor records. It should not assume that every fraud loss fits the unauthorized order provisions. Beneficiary identification and number reliance can also require separate analysis under the governing payment law.

Reserve discretion to investigate unusual instructions without promising to detect every scam. If the bank agrees to perform a particular verification step, implement and retain evidence of that step. Excluding internal analytics from the agreed security procedure does not remove statutory duties, good faith requirements, or a separate contractual undertaking.

Use service-specific reporting periods

Distinguish a prompt operational reporting duty from a deadline that changes legal remedies. Article 4A-204 addresses the effect of delayed notice on interest in an unauthorized order refund, while section 4A-505 contains a separate one year preclusion rule tied to notification of the order. Check the law, consumer protection laws, and payment network rules, which use different frameworks. Assess any proposed shorter contractual period under governing law rather than copying one universal 30 day forfeiture clause. [4, 5]

Identify the report the customer must review, when it becomes available, how the bank delivers it, and where the customer reports a problem. Confirm that the operations team can receive and escalate those reports. A deadline tied to information the bank cannot show it supplied creates an avoidable evidence problem.

Test a liability clause against a real loss

Separate reimbursement of the payment principal, interest, service damages, consequential loss, and indemnity claims before setting a cap. Article 4A restricts variation of certain refund obligations and separately regulates damages for execution errors. A generic cap cannot be assumed to displace those rules. For liabilities that may be limited, assess the service, enforceability, insurance, and exposure. [4, 6]

As a drafting exercise, place a \$10,000 fee-based cap beside a service permitting \$5 million wires. Identify exactly which claims the cap would reach and which remain outside it. That mismatch requires a deliberate decision, but there is no universal rule requiring every cap to equal the largest authorized wire. A fee multiple may suit some information services; payment services may require separate treatment. State the cap's scope, aggregation period, and exceptions. Coordinate exclusions and indemnities with nonwaivable duties and applicable state requirements for allocating negligence risk.

Build the evidence before a fraud report arrives

Sample executed agreements against live settings. Confirm the administrator trail, selected procedure, limits, amendments, and records of any declined alternatives. Preserve relevant system logs and communications when an incident is reported, including changes immediately preceding the disputed payment. Retention periods should reflect law, contract, litigation risk, and the bank's records policy.

A useful exercise is to reconstruct a recent high-value payment without relying on the relationship manager's memory. Can the bank establish who had authority, what procedure applied, how the order was verified, and which terms governed? Resolve missing links before the next incident. If the signed agreement promises dual approval while the system permits one user to release a payment, correct the mismatch through an authorized process and retain the historical record.

The management deliverable

- Maintain an Article 4A evidence package for commercial payment services and a separate process for covered consumer disputes.
- Review each fraud-related promise against the control the bank actually performs and can prove.
- Test notice provisions, caps, and indemnities by service and claim type, including a loss involving the largest permitted transaction.

Sources and application

[1] **UCC 4A-202**. Authorized and verified payment orders and commercial

reasonableness.

[2] **UCC 4A-203**. Unenforceability of certain verified payment orders.

[3] **Regulation E coverage**. 12 CFR 1005.3 and official interpretations; account and transfer coverage and exclusions.

[4] **UCC 4A-204**. Refunds for unauthorized payment orders and the effect of delayed reporting.

[5] **UCC 4A-505**. Preclusion of objections to account debits.

[6] **UCC 4A-305**. Damages for late or improper execution or failure to execute.

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.
