

SPOTLIGHT ON NACHA

Third-Party Senders Obligations under the Nacha Operating Rules

A Spotlight on Third-Part Senders
Obligation to Implement Risk-based
Controls in ACH Operations



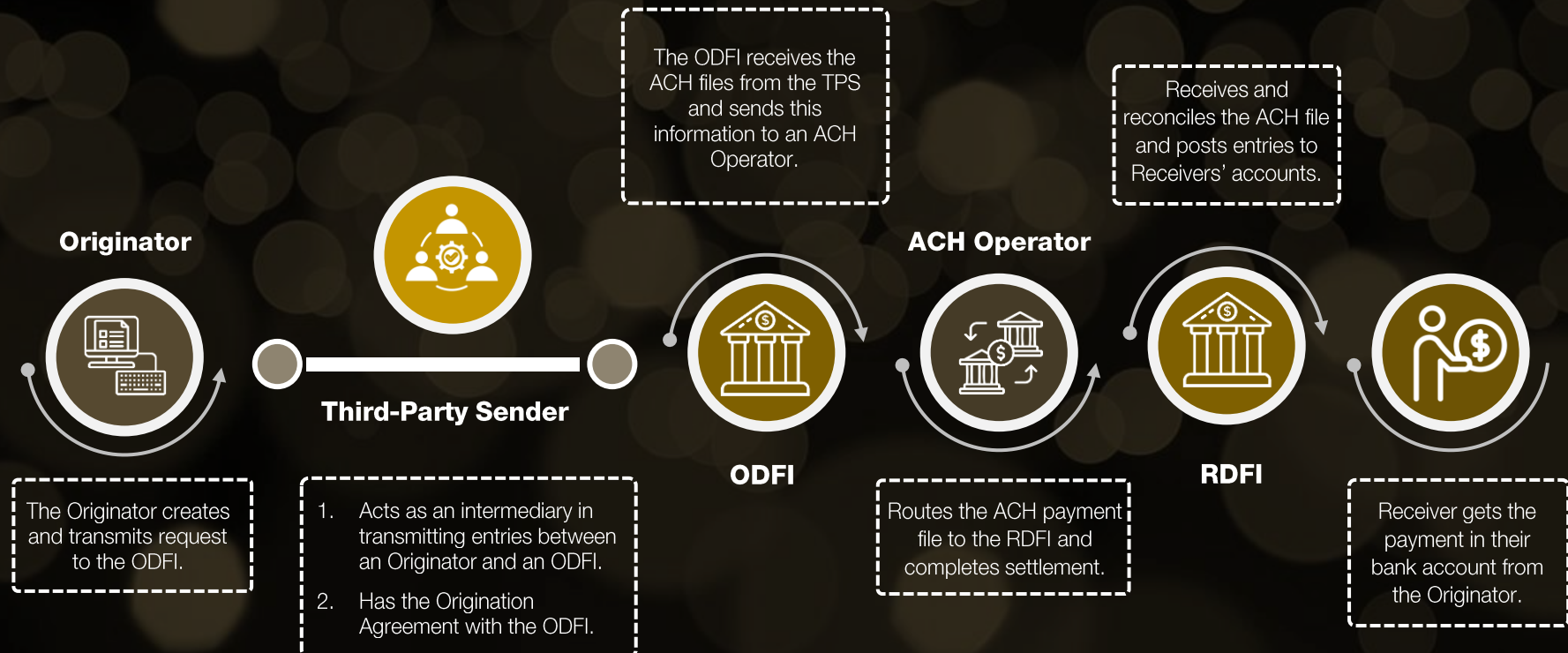
RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT



Understanding Third-Party Sender and ACH Payment

A Third-Party Sender (TPS) initiates Automated Clearing House (ACH) payments on behalf of Originators through an Originating Depository Financial Institution (ODFI), creating an indirect link to the ACH Network. Nacha Rules govern this flow by requiring TPSs to maintain origination agreements, register promptly, and conduct independent risk assessments and annual audits. TPSs are also accountable for ensuring compliance with applicable Nacha requirements affecting both ODFIs and Receiving Depository Financial Institutions (RDFIs) across all ACH transactions.

The following illustrates an TPS ACH payment flow:



Shift from “Commercially Reasonable” to “Risk-Based”

Fraud risk management has long been a core operational and financial responsibility for TPS. Recent Nacha Operating Rules (Rules) amendments between 2025 and 2026 have increased the need for proactive monitoring and swift response, positioning fraud oversight a critical priority in maintaining compliance and safeguarding integrity of ACH activities.



Risk Management Compliance Practices

Relevant risk management and compliance practices under Nacha focus on ensuring that ACH participants actively identify, monitor, and mitigate fraud and operational risks. Effective risk management and compliance practices safeguard ACH operations, ensuring regulatory adherence while protecting institutions from fraud and operational disruptions.



Regulatory Adherence

- Follow Nacha/OFAC rules
- Maintain clear procedures
- Document all actions



Fraud Prevention and Security

- Monitor for anomalies
- Enforce strong access controls
- Protect sensitive data



Customer and Third-Party Management

- Perform due diligence
- Monitor return rates
- Flag high-risk activity



Training and Continuous Improvement

- Provide staff training
- Perform quality control
- Update practices regularly

Nacha Rules Audit



ACH Rules Compliance Audit Requirements

The annual ACH Rules Compliance Audit is a Nacha requirement designed to verify that each participant's ACH activities align with the Operating Rules. The ACH Rules Compliance Audit is critical in enforcing accountability, strengthens risk management, and ensures the integrity of the ACH Network.

Who Must Conduct an Audit?

- All TPS and Nested TPS.
- Applies whether TPS sends entries on behalf of one client or multiple clients.



Schedule

The audit must be completed by **December 31** every year.

Scope of the Audit

- All applicable Nacha Operating Rules relevant to the TPS ACH activities.
- Process Controls:
 - Authorization Requirements
 - Origination Practices
 - Security and Data Protection
 - Returns and Reversals
 - Record Retention
 - TPS Agreements
- Governance and Risk Management



Audit Method

- Audits must be performed under the direction of the audit committee, audit manager, senior level officer, or independent (external) examiner or auditor.
- Nacha does not otherwise specify the method but does provide an ACH Audit Workbook for guidance.



Audit Report

- Proof of completion of the audit must be retained for six (6) years from the date of the audit.
- Nacha does not require submission unless requested by the following:
 - ODFI sponsoring the TPS; or
 - Nacha or its Regional Payment Associations during a rule's enforcement review.



Enforcement

- Class 1: Minor Issues (Operational/Technical errors with minimal impact)

Warning/Corrective Action

- Class 2: Significant Issues (Repeat violations affecting other ACH participants)

Fines starting at \$1,000 per month

- Class 3: Severe Issues (High risk violations that threaten the ACH network)

Up to \$500,000 per month + risk of losing ACH access



Discover
what
Stratis
Advisory
can do
for you



Annual Nacha ACH Rules Compliance Audit

Understanding your role in an ACH transaction is critical to determining whether you may be subject to performing an annual audit under Nacha's Operating Rules (Rules). In Banking as a Service (BaaS) and For Benefit Of (FBO) operating models, you may be acting as a third-party sender (TPS) under the Rules. Stratis can help you comply with your BaaS or FBO agreement requirements as a TPS to perform your annual Nacha Operating Rules audit by December 31 of the calendar year.



ACH Risk Assessment

Participating in the ACH network requires numerous operational requirements. For companies operating as a TPS, an ACH risk assessment should be conducted to assess various risks such as operational risk, return risk, credit risk, fraud risk, compliance risk, cybersecurity risk, and reputational risk. Moreover, an ACH risk assessment is a factor in determining annual compliance with Nacha's Operating Rules. Stratis can help you evaluate your ACH operations, understand your risks in the ACH network, inclusive of return rates and codes, and document your annual ACH risk assessment to comply with the Rules, but also your BaaS or FBO master's services agreement.



BaaS, FBO, ACH Contract Compliance

Operating under a BaaS, FBO, ACH master's services agreement (MSA) with a banking or payment partner usually passes down statutory, industry, and best practice requirements during the agreement term. Namely, compliance with annual anti-money laundering, sanctions, and Nacha Operating Rules audits, executing ongoing vendor management, customer monitoring, and complaints processing, among others. Stratis can help you with developing your core compliance frameworks to implement these programs or execute the annual audits to comply with your BaaS, FBO, ACH MSA.



