Third-Party Sender Roles and Responsibilities

Issue date: May 21, 2021

Close date: July 1, 2021

Request For Comment

Nacha®

Third-Party Sender Roles and Responsibilities Request for Comment

- **Nacha is seeking comment and feedback from industry stakeholders on two related Rules proposals collectively referred to as "Third-Party Sender Roles and Responsibilities"**
- **The overarching purpose of these proposals is to further clarify the roles and responsibilities of Third-Party Senders in the ACH Network by**
    1. Addressing the commercially existing practice of Nested Third-Party Sender relationships, and
    2. Making explicit and clarifying the requirement that a TPS conduct a Risk Assessment

Nacha®

Third-Party Sender Roles and Responsibilities Request for Comment Summary

- **This Request for Comment includes the following specific proposals to amend the Nacha Operating Rules**
  - Address the commercially existing practice of Nested Third-Party Sender relationships:
    - Define a Nested Third-Party Sender
    - Establish the "chain of agreements" and responsibilities in a Nested TPS arrangement
    - Update the requirements of an Origination Agreement for a Nested TPS relationship
    - Update existing TPS registration to denote whether a TPS has Nested TPS relationships
  - Third-Party Sender performance of a Risk Assessment
    - Make explicit that a Third-Party Sender, whether nested or not, must complete a Risk Assessment of its ACH activities
    - Clarify that a Third-Party Sender cannot rely on a Rules Compliance Audit or a Risk Assessment completed by another TPS in the chain; it must conduct its own
- **Responses on these proposed changes are requested by July 1, 2021.**

Nacha®

Third-Party Sender Roles and Responsibilities
Why Are Changes Being Proposed?

- **“Nested” Third-Party Senders play an active role in a variety of ACH processing models, but are not currently addressed in the Rules**
    - The lack of formal definition for a Nested TPS that is a step removed from the ODFI occasionally results in confusion over responsibilities
- **The existing Rules are not clear and explicit regarding Third-Party Senders and Risk Assessments**
    - ODFIs are obligated to perform a Risk Assessment, and a TPS takes on this requirement when it takes on the responsibilities of the ODFI; but this obligation is not explicitly stated and is a source of confusion.
    - In addition, Nacha has seen some instances in which a TPS advertises, “We do our ACH Audit, so you don’t have to”
- **A fraud event in August 2019 involving a Nested TPS payroll provider caused significant disruption to other ACH Network participants**
    - Better-defined responsibilities, and a thorough assessment of risks and Rules compliance, may have added controls that would have prevented or lessened the severity of this incident

Third-Party Sender Roles and Responsibilities Request for Comment

Nacha invites comments on these Rules proposals. In addition to comments on each specific proposal (as further described in this RFC), industry feedback and perspectives are requested on the following aspects of the overarching purposes:

- Would these proposed changes improve ACH Network risk management and ACH payments integrity for both financial institutions, third-party senders, and business and consumer users?
- Would these proposed changes have an overall positive effect on the ACH Network, and on your organization?
- How would these proposed changes impact your organization?

Proposal #1 – Nested Third-Party Senders

This proposal would define a Nested Third-Party Sender, and would provide for the "chain of agreements" and responsibilities

- A "Nested Third-Party Sender" would be defined as a Third-Party Sender that has an agreement with another Third-Party Sender to act on behalf of an Originator, and does not have a direct agreement with the ODFI
- Nested TPSs must be addressed in ACH Origination Agreements
    - An ODFI Origination Agreement with a TPS must address whether the TPS can have Nested TPSs, and if so, "push down" the requirement for an Origination Agreement to exist between a TPS and a Nested TPS
    - An Origination Agreement must exist between a TPS and a Nested TPS
    - Changes to ACH Origination Agreements would be applicable on a going-forward basis from the effective date
- Other TPS obligations and warranties would be updated to identify and cover Nested TPS relationships
- An ODFI must identify in Nacha's Risk Management Portal all Third-Party Senders that allow Nested Third-Party Sender customers
    - E.g., "Does TPS "XYZ" have Nested TPS customers? Check Yes or No."
    - Upon request, an ODFI must provide Nacha with the Nested TPS relationships for any TPS

Proposal #1 – Expected Benefits

- **The proposal is intended to provide clarify and remove confusion about roles and responsibilities of parties involved in a Nested Third-Party Sender relationship**
  - Defines a Nested Third-Party Sender, and provides clarity on agreements and obligations of defined parties
  - Further encourages a culture of compliance and risk management in ACH, especially regarding TPS relationships
  - Reasonably expands ODFIs' due diligence to know whether TPS customer have Nested Third-Party Sender relationships
- **Ultimately, better clarity and knowledge by ACH participants about the roles and responsibilities of parties should help improve ACH quality**

Proposal #1 – Potential Impacts

- **To the extent that ODFIs and Third-Party Senders do not already address Nested TPSs, they might need to:**
    - Modify Origination Agreements for future use (i.e., going-forward after the effective date)
    - Expand due diligence on TPS customers regarding Nested TPS relationships
- **ODFIs with Third-Party Sender relationships will need to update their registrations in the Risk Management Portal to denote which TPSs have Nested TPS relationships**
    - ODFIs that have TPS-Nested TPS relationships must be able to provide Nacha with such information, upon request

Proposal #1 – Request for Comment

Nacha requests comment on all aspects of this proposal, including:

- Should a Nested TPS be defined within the Nacha Rules?
- Do you agree with the proposed definition?
- Should an ODFI with TPS customers know whether their TPS customers allow Nested TPS relationships?
- Should an ODFI with TPS customers address Nested TPS relationships within their ACH Origination Agreements?
- Should a Nested TPS have an ACH Origination Agreement between the TPS and Nested TPS?
- Should a TPS disclose Nested Relationships prior to originating entries for a Nested TPS?
- Should ODFIs be required to identify TPSs that allow Nested TPSs in the Risk Management Portal?
- Should the Rules address how many levels can exist in a chain of Nested Third-Parties Senders?

Proposal #2 – TPS Risk Assessments

- **Risk Assessments are already defined and required in the Nacha Rules for Financial Institutions and, by extension, for Third-Party Senders under their obligations to perform and warrant ODFI obligations**
  - However, the Risk Assessment obligation for TPS is not expressly stated
- **The proposed rule would expressly state that a Third-Party Sender, whether or not it is Nested, is required to conduct a Risk Assessment**
  - As with other parties that conduct Risk Assessments, a Third-Party Sender must implement, or have implemented, a risk management program based on their Risk Assessment
  - The obligation to perform a Risk Assessment, as well as the required Rules Compliance audit, cannot be passed onto another party; i.e., each participant must conduct its own

Proposal #2 – TPS Risk Assessments

- **Risk assessments are common practice in the payments industry**
  - The card networks' Payment Card Industry (PCI) Data Security Standards (DSS) requires annual risk assessments
  - The Payments Associations and TPPP industry groups offer risk assessment services and products
  - Nacha Publications, including the "ACH Risk Management Handbook" and "Third-Party Senders and the ACH Network," promote the benefits of risk assessments and provide techniques and suggestions for assessing and mitigating risk
- **FFIEC Guidance requires FIs to assess the risk posed by Third-Party Payment Providers (TPPP) to their financial institution**
  - While risk assessments by the TPPP are not addressed in the FFIEC guidance, third-parties can still understand what is expected when they take on the role and responsibilities of an ODFI (see https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum11/sisummer11-article1.pdf)

Proposal #2 – Risk Assessment Guidance for TPSs

- **Each TPS operates in a different space, with challenges, risks, and controls that may be different than the challenges, risk and controls faced by another TPS**
- **Attempting to prescribe the exact topics and methods for a TPS risk assessment would likely over-prescribe risk and controls for some TPSs, and fail to identify risk and controls for others**
    - For the same reason, Rules Compliance Audit requirements were recently removed from the Rules (Appendix 8)
- **Assistance in understanding and performing Risk Assessments is widely available in the marketplace, through Payment Associations, Nacha publications, and many other organizations**

Proposal #2 – Risk Assessment Guidance for TPSs

- **Nevertheless, a TPS risk assessment should likely cover many of the same types of risk as do assessments performed by other parties in the ACH Network, or by the TPS as required for other payment systems when the TPS acts as a TPPP**
  - Broad risk categories include Operational Risk, Return Risk, Credit Risk, Fraud Risk, Compliance Risk, and Reputational Risk
  - TPSs can look to the ODFI Risk Management Requirements and other requirements of Articles One and Two of the Rules; for example: 1) performing customer due diligence; 2) setting and enforcing customer exposure limits; 3) auditing and testing Originator authorization processes and quality; 4) monitoring forward and return transactions volumes, dollars, and rates; 5) establishing data security policies, procedures, and systems with access controls, authentication, authorization, and encryption; and 6) SEC Code-specific risk management requirements and warranties
  - TPSs can also look to requirements and guidance issued by banking regulators (such as the OCC and the FDIC) on risk management expectations for ODFIs

Nacha®

Proposal #2 – Expected Benefits

- **Risk Assessments are vital to managing risk for any party in the ACH Network; clarifying this requirement will promote active risk management by Third-Party Senders**
    - Encourages a culture of risk management and compliance in ACH processing
    - Aligns the ACH Network with the wider payments industry
    - Improves the quality of ACH payments by elevating the prominence of risk assessment among additional ACH Network participants

Proposal #2 – Potential Impacts

- Third-Party Senders that have not previously conducted an ACH risk assessment would have to do so
- Third-Party Senders that have relied on other TPSs' Risk Assessments or Rules Compliance Audits would need to conduct their own

Proposal #2 – Request for Comment

Nacha requests comment on all aspects of this proposal, including:

- Are the Rules currently clear about whether TPSs are required to conduct ACH risk assessments?
- Should the Rules be explicit that TPSs must conduct ACH risk assessments?
- Similar to Rules Compliance Audits, should the Rules avoid prescribing specific topic or methods for TPS risk assessments?

Third-Party Sender Roles and Responsibilities Proposed Effective Date and Implementation Periods

- **Both proposals would become effective on a single effective date, June 30, 2022**
- **Changes to ACH Origination Agreements would be effective on a going-forward basis – i.e., applicable to agreements entered into on or after the effective date**
- **A six-month grace period – to December 31, 2022 – would be provided for:**
  - ODFIs - to update TPS registrations to denote whether or not a TPS has Nested TPSs
  - TPSs that have not conducted a Risk Assessment would have a 6-month period to do so
    - A TPS need not wait for passage of this rule, or its effective date, to conduct a Risk Assessment