PAYMENTS NEWS

FOR TREASURY CUSTOMERS

1ST QUARTER 2022

UNDERSTANDING THE DIFFERENCE BETWEEN AN ACH ORIGINATOR, THIRD-PARTY SENDER AND NESTED THIRD-PARTY

The Nacha Rules require participants to comply with network Rules based on the type of participant they represent. It is important for participants to understand the difference in types of entities for the purpose of complying with network Rules. It is first important to understand the type of entity you are based on the relationship with your financial institution and the customers you serve.

ORIGINATOR	THIRD-PARTY SENDER	NESTED THIRD-PARTY SENDER
An Originator is an organization or person that initiates an ACH transaction to an account either as a debit or credit.	A third-party sender is a type of third-party service provider that acts on behalf of the originator only. In other words, it is a layered relationship that is intermediary between the originator and the ODFI. In this type of relationship, there is generally no contractual agreement between the ODFI and the originator making this relationship a higher risk relationship based on network Rules and regulatory guidance.	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.

The risks associated with Third-Party Senders and Nested Third-Party Senders has to do with the downstream relationships of the Originating Depository Financial Institution. While the network does allow Third-Party Sender and Nested Third-Party Senders, organizations need to understand their requirement to comply based on the type of relationship. Network rules have evolved over recent years to place an emphasis on organizations to ensure compliance with Nacha Rules and to build out their programs commensurate with the risks associated with the type of relationship. In September 2022, the network Rules will be expanded to include specific requirements of layered relationships including Third-Party Senders and Nested Third-Party Senders. Effective September 30, 2022, there are requirements that an Originating Financial Institution must:

- Address in their agreement with the Third-Party Sender to ensure that Nested Third-Party Sender relationships are addressed. NOTE: Originating Financial Institutions can prohibit Nested Third-Party Sender relationship in their agreement with Third-Party Senders.
- Updates existing TPS registration to denote whether a TPS has Nested TPS relationships
- Requires that a Third-Party Sender, whether Nested or not, complete a Risk Assessment of its ACH activities.
- 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 will conduct or have conducted its own.

If you are an Originator and have a change in processing relationships, this may impact you as there are specific compliance requirements when a change in processing results in a layered relationship.

If you are a Third-Party Sender, it is important that you prepare for this change, train all applicable areas and implement an ACH program that aligns with these upcoming network changes.

If you are a Nested Third-Party Sender regardless of the size of your company, it is important to understand this type of relationship presents additional risks and should be addressed in preparation with upcoming network changes.

For information on these types of relationships, the risks presented and current and newly passed network requirements, contact your originating depository financial institution.

Your Responsibility for Receiving Notifications of Change (NOCs)

A Notification of Change (NOC) is a **non-dollar entry** transmitted by a Receiving Depository Financial Institution (RDFI) to notify you that information contained within an entry is erroneous and/or has become outdated and must be changed. The ACH Rules require your company to make the requested changes **within 3 banking days of the receipt of the NOC or prior to the initiation of another ACH entry.**

Although the NOC is unlike a return that normally has a dollar amount attached, Originators are still required to handle the NOC in accordance with the NACHA Rules.

Cash Management Users: Update Your Contact Information

It is important that we have your updated contact information to ensure you receive timely updates on cash management services. Remember that if employees leave or you add key team members that should receive updates to cash management updates or educational tools, contact your account officer or treasury service representative.

RANSOMWARE AWARENESS: YOUR GUIDE TO UNDERSTANDING THIS CYBER-THREAT

Ransomware is a form of malware (malicious software) designed to encrypt files on a device, resulting in any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. Over the years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations and hit smaller organizations and consumers.

Malicious actors continue to advance and adjust their tactics over time, and the U.S. Government, state and local governments, as well as the private sector remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures across the country and around the world.

This guide describes what actions organizations should take to understand the technological and regulatory limitations, responsibilities, and resources available to them, and how to implement controls to their operations. **This guide does not constitute legal advice and is only for reference purposes.** For additional information on ransomware awareness, visit https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident.