

finovifi



ACH READINESS BRIEFINGS

Questions & Answers

Email Address info@finovifi.com

Social Media <https://finovifi.com/2026-nacha-questions>

Contents

1. Does the Rule apply to all ODFIs for Phase 1?	2
2. Is there a requirement to screen individual ACH entries?	2
3. Are you required to monitor transactions prior to processing?	2
4. What action should an ODFI consider taking if an entry is identified as suspect?	3

1. Does the Rule apply to all ODFIs for Phase 1?

Yes.

Fraud Monitoring by Originators, TPSPs and ODFIs

Effective dates

Phase 1 – March 20, 2026

- The rule will apply to all ODFIs
- The rule will apply to non-Consumer Originators, Third-Party Service Providers (TPSPs), and Third-Party Senders (TPSs) with annual ACH origination volume of 6 million or greater in 2023

Phase 2 – June 19, 2026

- The rule will apply to all other non-Consumer Originators, TPSP, and TPS

RDFI ACH Credit Monitoring

Effective dates

Phase 1 – March 20, 2026

- The rule will apply to RDFIs with annual ACH receipt volume of 10 million or greater in 2023.

Phase 2 – June 19, 2026

- The rule will apply to all other RDFIs.

2. Is there a requirement to screen individual ACH entries?

No, the rule requires a risk-based approach to fraud monitoring. You should apply resources and take extra measures to detect fraud in transactions that are determined to have elevated risks, Allows taking only basic precautions where it has determined that risks are lower. Cannot be used to conclude that no monitoring is necessary In other words, you must do something!

3. Are you required to monitor transactions prior to processing?

No, it is not required; however, this provides the greatest opportunity for preventing potential fraud. Proactive measures could be reserved for Originators deemed high risk. Reactive measures may be acceptable for lower-risk Originators

4. What action should an ODFI consider taking if an entry is identified as suspect?

For transactions that monitoring identifies as suspect, the ODFI can consider a number of actions. Actions may include, but are not limited to:

- stopping further processing of a flagged transaction;
- consulting with the Originator to determine the validity of the transaction;
- consulting with other internal monitoring teams or systems to determine if the transaction raises other flags; and
- contacting the RDFI to determine if characteristics of the Receiver's account raise additional red flags, or requesting the freeze or the return of funds.

With respect to debits, a robust return and return rate monitoring program in with existing Rules (as well as any required compliance with other specific fraud detection Rules for WEB debits and Micro-Entries) is sufficient as a minimum level of fraud monitoring.