ACH Quality and Risk Management Topics

NACHA Request for Comment
May 11, 2018

NACHA
The Electronic Payments Association®

Executive Summary

- NACHA revisits rules on ACH Network quality and risk management topics as warranted from time to time
- Recent amendments to the *NACHA Operating Rules* regarding quality and risk management include:
  - September 2017 - to establish Third-Party Sender Registration
  - October 2016 - to implement the Unauthorized Entry Fee
  - September 2015 – to reduce the unauthorized return rate threshold, and establish the administrative and overall return rate levels

Executive Summary

- NACHA is issuing this Request for Comment to obtain industry feedback on several new topics to help manage risk and improve quality
  1. Limiting the length of time an RDFI can make a claim against an ODFI's authorization warranty
  2. Differentiating among types of unauthorized returns
  3. Supplementing the fraud detection standard for Internet-initiated (WEB) debits
  4. Allowing RDFIs to indicate within a return that the original transaction was questionable or part of anomalous activity
  5. Supplementing the existing account information security requirements for large Originators and Third-Parties
- Responses from the industry are requested by Friday, June 29, 2018
  - Please visit NACHA's web site at https://www.nacha.org/rules/proposed to submit comments

Overview

- NACHA views risk management on the ACH Network as a process of continuous improvement
  - Rules, guidance, best practices, and other tools related to ACH Network quality and risk management topics are proposed and developed from time to time as warranted
- At the same time, NACHA is also focused on reducing friction experienced by ACH participants
  - Friction can be reduced by reducing complexity, lowering costs, or improving the user experience and access to the ACH Network
- An overall objective of this set of proposals is to achieve and maintain a fair and reasonable balance between requirements and controls for risk management, and fully enabling the use of ACH
  - This set of proposals is intended to provide benefits for both the origination and receipt sides of ACH transactions

Overview

- This set of rule proposals is intended to benefit ODFIs and their ACH Originators by:
  - Setting a maximum limit on the length of time under which an RDFI can make a claim for breach of the ODFI's authorization warranty
  - Providing more granular and precise reasons when an ACH debit is returned as unauthorized
  - Providing an indicator in a return of an ACH transaction to flag anomalous or questionable activity

Overview

- This set of rule proposals is intended to benefit RDFIs and their customers by:
  - Improving ACH origination practices to screen the origination of WEB debit entries
  - Enabling a return reason that will serve as an indicator to the ODFI/Originator that the original transaction was questionable or part of anomalous activity
  - Better protecting RDFIs' account numbers used in ACH entries

Overview

- It is important to view the individual parts of this Request for Comment as integral parts of a whole, intended to create a better quality and stronger risk management environment for all participants

Goal	Proposal
Address significant friction point for ACH Originators	Define length of authorization warranty
Allow for better data for all participants	Differentiate unauthorized return reasons
Balance risk and easy origination	Supplement commercially reasonable fraud detection systems
Enable a tool for use in risk events	Return reason for “questionable”
Tailor where appropriate to apply to largest users of the ACH to avoid over-burdening smaller participants	Account information security requirement for large Originators/TPSPs/TPSs

- The components together provide benefits for all participants while not over-burdening any one segment of ACH Network participants

Rule Proposals

NACHA
The Electronic Payments Association®

1. Limiting the Length of Time that an RDFI Can Make a Claim Against an ODFI's Authorization Warranty – Current Rules and Environment

- Under existing NACHA Rules, an ODFI warrants that an ACH entry has been properly authorized by the Receiver
  - While extended returns for unauthorized entries are allowed by the Rules for 60 days from the Settlement Date, the ODFI authorization warranty currently does not have a time limit defined in the Rules
  - Time limits are determined by statutes of limitation, which vary from state to state, and can be as long as 10 years
- A major point of friction for ACH Originators, especially consumer billers, is receiving "unauthorized" returns long after the expiration of the 60-day extended return deadline
  - For example, an account holder disputes the past 4 years of recurring bill payments as unauthorized
  - Because the authorization warranty is not time-limited, the RDFI can bring a claim against the warranty; the ODFI therefore agrees to accept late returns of all the entries, and charges them back to the Originator
- The ACH Network is one of the few payment systems without a time limit for these warranty claims

RDFI Warranty Claims – Rule Proposal

- The proposed rule change would limit the length of time in which an RDFI would be permitted to make a claim against the ODFI's authorization warranty
  - For an entry to a non-consumer account, the time limit would be one year from the settlement date
    - This is analogous to the one-year rule in UCC §4-406 that applies to checks and items charged to bank accounts
  - For an entry to a consumer account, the time limit would be 18 months from the settlement date
    - This is intended to exceed the one-year Statute of Limitations in the Electronic Funds Transfer Act (covering Regulation E claims), which runs from the date of the occurrence of the violation, which may be later than the settlement date of the transaction
    - This also allows for "extenuating circumstances" in which a consumer is delayed from reporting an error to his or her financial institution
    - RDFIs generally would still be enabled to recover amounts they must pay consumers under Regulation E
    - There may be a small increase to the risk that an RDFI could be liable to its customer without the ability to collect from the ODFI

RDFI Warranty Claims – Potential Benefits and Impacts

- Potential benefits
  - Addresses a friction point for many ACH participants
    - For ACH Originators, by limiting the length of time in which an ACH payment can be charged back
    - For ODFIs, by providing much greater certainty regarding long-term return of transactions and associated credit risk
  - Lowers a barrier to ACH origination for potential ODFIs and Originators, as it creates more certainty for transaction liability
  - A more equitable allocation of liability – receivers have a responsibility to review statements and report unauthorized activity in a timely manner
  - Lessens the impact of “friendly fraud”
  - Provides an incentive to RDFIs to assert their contractual defenses to claims by account holders
- Potential impacts
  - Shifts liability for older transactions from ODFIs and Originators to RDFIs and Receivers
  - Potential for small increase in risk that there will be some circumstances in which an RDFI could be liable to its customer without the ability to collect from the ODFI; associated RDFI courtesy write-offs
  - Could be viewed as less consumer friendly

RDFI Warranty Claims – Alternatives

- NACHA is requesting comments on alternatives to the proposed rule, which include
  - Setting the same time limit for entries to both consumer accounts and non-consumer accounts – i.e., 18 months for all
  - Setting different limits than those proposed, such as
    - 1 year
    - 13 months (i.e., 1 year + a 30-day statementing period)
    - 2 years

RDFI Warranty Claims – Request for Comment

- NACHA requests comment on all aspects of the proposal to establish a time limit for an ODFI's authorization warranty
  - For ACH Originators, is this a real source of friction in using ACH? If so, how frequently does it occur?
  - As an RDFI, how often do you make such claims after the return time period has expired (or ask for permission to send returns late)?
  - Does the proposal establish the right allocation of liability between ACH origination and receipt when an account holder dispute a payment(s) as unauthorized?
  - Do you agree with the timeframes proposed, or do you prefer any of the alternatives?

2. Differentiating Unauthorized Return Reasons – Current Rules and Environment

- Currently, return reason code R10 is a catch-all for various types of underlying return reasons
  - Wrong date
  - Wrong amount
  - Incomplete transaction
  - Improperly reinitiated transaction
  - Originator not known/recognized
  - Authorization never given
- For several of these underlying reasons, there is an actual relationship and a payment authorization between the Originator and the Receiver, but the Originator has made an error regarding the payment

Differentiating Unauthorized Return Reasons – Rule Proposal

- A different return code (R11) would be re-purposed to be used for a transaction in which there is an error, but for which there is an authorization
  - R11 volume is currently very low – only 345 total returns in 2017, none of which are related to its original purpose to return check truncation entries
  - The re-purposed reason would be “Customer Advises Entry Not In Accordance with the Terms of the Authorization”
  - The new R11 would have the same 60-day extended return time frame and requirement for a Written Statement as currently with R10
  - These returns would continue to be covered by the Unauthorized Entry Return Rate and Unauthorized Entry Fee definitions as currently with R10
- Return reason code R10 would continue to be used when a consumer claims he or she does not know the Originator, does not have a relationship with the Originator, or did not give authorization for the account to be debited
  - “Customer Advises Originator is Not Known to Receiver and/or Is Not Authorized by Receiver to Debit Receiver's Account”

Differentiating Unauthorized Return Reasons – Potential Benefits and Impacts

- Potential benefits
  - Providing more granular and precise reasons for returns
    - ODFIs and Originators would have clearer information in instances in which customer alleges “error” as opposed to “no authorization”
    - Corrective action easier to take in instances in which the underlying problem is an error – e.g., wrong date, wrong amount
    - More drastic action (i.e., closing an account) can be avoided in instances in which the underlying problem is an error
  - Allows collection of better industry data on unauthorized return activity
- Potential impacts
  - ACH Operator and financial institution changes to repurpose an existing R-code, including modifications to return reporting and tracking capabilities
  - Education on proper usage of codes by RDFIs; education, monitoring and remediation by Originators/ODFIs
  - Inclusion of an additional return code within existing rules on ODFI Return Reporting and Unauthorized Entry Fees

Differentiating Unauthorized Return Reasons – Alternatives

- NACHA is requesting comments on alternatives to the proposed rule, which include
  - Splitting out the underlying reasons among R10/R11 differently
  - Re-purposing a different return reason code than R11
  - Creating a new return reason code

Differentiating Unauthorized Return Reasons – Request for Comment

- NACHA requests comment on all aspects of this proposal to differentiate among types of unauthorized reasons
  - As an ODFI or Originator, what are the benefits of this differentiation?
    - Would different return reasons better enable different corrective actions to be taken?
  - As an RDFI, how much effort is involved in training staff to use R-codes correctly?
  - Do you prefer any of the alternatives?

3. Commercially Reasonable Fraud Detection – Current Rules and Environment

- Currently, ACH Originators of WEB debit entries are required to use a "commercially reasonable fraudulent transaction detection system" to screen WEB debits for fraud
  - The requirement is intended to help prevent the introduction of fraudulent payments into the ACH Network, and to help protect RDFIs from posting fraudulent or otherwise incorrect/unauthorized payments
  - Originators are in the best position to detect and prevent fraud related to payments they are initiating
  - In recent risk events perpetrated via social media channels, it has become apparent that some ACH Originators do not have or use any such system to screen WEB debits

Commercially Reasonable Fraud Detection – Rule Proposal

- The current screening requirement would be supplemented to make it explicit that "account validation" is an inherent part of a "commercially reasonable fraudulent transaction detection system"
  - Existing NACHA guidance already states
    - "An important element of a commercially reasonable fraudulent transaction detection system would be the adoption of risk-based mechanisms designed to confirm the validity of an account to be debited."
  - The supplemental requirement would apply to the first use of an account number, or changes to the account number
  - The proposal is neutral with regard to specific methods or technologies to validate account information. Possibilities include
    - An ACH prenotification
    - ACH micro-transaction verification
    - Commercially available validation service
  - Doing nothing to validate account information on its first use or for changes would be deemed not commercially reasonable

Commercially Reasonable Fraud Detection – Rule Proposal

- Additionally, the current screening requirement would be further supplemented to require the dollar amount of the WEB debit to reasonably relate to the purpose of the payment
  - Such "reasonableness testing" could screen for large overpayments or irregular payment amounts. For example
    - A large overpayment of an amount due on a bill, loan, or other obligation
    - A large, atypical amount of an account-to-account transfer
    - Mis-keying by a customer of an amount to pay or transfer that results in a large overpayment

Commercially Reasonable Fraud Detection – Potential Benefits and Impacts

- Potential benefits
  - Reduce the number of questionable, invalid or fraudulent entries that are submitted into the ACH Network and received by RDFIs
  - Improved fraud detection capabilities on the front-end by ACH Originators of WEB debits
  - Potential improvement in account validation capabilities and services
  - Limit the potential impact of fraud events, such as those spread by social media
- Potential impacts
  - Possible re-tooling of ACH Originators' fraud detection systems
    - Or implementation of a system for Originators who currently do no screening
  - RDFIs could receive a greater volume of ACH prenotifications, micro-transactions, or other account validation requests
    - Some would be in lieu of receiving live-dollar transactions initially

Commercially Reasonable Fraud Detection – Alternatives

- NACHA is requesting comments on alternatives to the proposed rule, which include
  - Requiring a specific account validation method(s) to be used
  - Expanding screening requirements to other SEC codes
  - Providing greater specificity regarding when account validation is required or not

Commercially Reasonable Fraud Detection – Request for Comment

- NACHA requests comment on all aspects of this proposal to include account validation and dollar amount reasonableness testing within the scope of a commercially reasonable fraud detection system
  - As an Originator of WEB debits, do you currently conduct account validation?
    - What account validation methods are effective when originating WEB debits?
  - As an Originator, do you currently limit the dollar amount of a WEB debit to be originated to an amount due or other parameter/benchmark?
  - As an RDFI, what would be the impact of receiving a greater volume of ACH prenotifications and/or micro-transactions prior to or instead of receiving live-dollar transactions?
- ACH Originators of WEB debits and their ODFIs are encouraged to review two white papers on account validation produced by NACHA's Payments Innovation Alliance
  - https://www.nacha.org/content/payments-innovation-alliance-resources

4. Allow a Return for Questionable Activity – Current Rules and Environment

- Currently, an RDFI may return an ACH entry for “any reason”
- The defined return reasons include “unauthorized” and “invalid account number/no account”
- For an ACH transaction that does not have a valid account number, and therefore does not post to any Receiver’s account, there is not a defined return reason code that enables an RDFI to communicate that an ACH transaction is questionable, suspicious, or anomalous in some way
  - In cases in which an RDFI is receiving a large number of questionable transactions, it does not have a method to communicate this via the returns
  - Using a standard administrative return reason (R03 or R04) does not enable an ODFI or its Originator to differentiate such questionable or suspicious transactions from routine account number errors

4. Allow a Return for Questionable Activity – Rule Proposal

- RDFIs would be allowed (but not required) to use return reason code R17 to indicate that the RDFI believes the entry was initiated under questionable circumstances
  - RDFIs electing to use R17 for this purpose would be required to use the description “QUESTIONABLE” in the Addenda Information field of the return
  - An R17 in conjunction with this description would enable these returns to be differentiated from returns for routine account numbers errors
- Currently, return reason code R17 is used in NACHA-coordinated opt-in programs with federal and state tax agencies for RDFIs to return tax refund ACH credits that RDFIs believe are questionable
- Additionally, existing NACHA guidance advises RDFIs that they can use R17 to return questionable transactions that would otherwise be returned via existing invalid/no account return codes (R03/R04)

4. Allow a Return for Questionable Activity – Benefits and Impacts

- Potential benefits
  - Enable an RDFI to communicate that it believes a transaction was questionable
    - Especially useful in scenarios that involve a large number of transactions
  - Enable ODFIs and their Originators to differentiate such questionable transactions from other transactions with routine account number errors
  - Easier implementation by using an existing return reason
- Potential impacts
  - For financial institutions, potentially implementing the capability to use the Addenda Information field if not a existing capability
  - Potential manual processing of additional R17 volume

4. Allow a Return for Questionable Activity – Alternatives

- NACHA is requesting comments on alternatives to the proposed rule, which include
  - Re-purposing a different return reason code than R17
  - Creating a new return reason code
  - Utilizing other risk alert services

4. Allow a Return for Questionable Activity – Request for Comment

- NACHA requests comment on all aspects of the proposal
  - As an RDFI, what are the benefits in being able to denote that a transaction, or a large number of transactions, is questionable?
    - Would you use it?
  - As an ODFI or Originator, what are the benefits in being able to differentiate transactions that are questionable from routine account number errors?
    - Would the capability enable you to prevent additional “questionable” transactions from being originated?
  - Do you prefer any of the alternatives?

5. Account Information Security – Current Rules and Environment

- The existing ACH Security Framework, which became effective in 2013, established the following requirements:
  - Financial institutions, Originators, Third-Parties Service Providers and Third-Party Senders are required to establish, implement and update, as appropriate, security policies, procedures, and systems related to the initiation, processing and storage of ACH transactions
  - These policies, procedures, and systems must:
    - Protect the confidentiality and integrity of Protected Information
      - "Protected Information" is defined as "the non-public personal information, including financial information, of a natural person used to create, or contained within, an Entry and any related Addenda Record"
    - Protect against anticipated threats or hazards to the security or integrity of Protected Information; and
    - Protect against unauthorized use of Protected Information that could result in substantial harm to a natural person
- In the industry at-large there is ongoing concern about the risk of data breaches and the potential use of such data

Account Information Security – Rules Proposal

- The proposal would expand the existing ACH Security Framework rules to explicitly require large, non-FI Originators, Third-Party Service Providers (TPSPs) and Third-Party Senders (TPSs) to protect deposit account information by rendering it unreadable when it is stored electronically
  - Aligns with existing requirement and language contained in PCI; industry participants should be reasonably familiar with manner and intent of requirement
  - Neutral as to methods/technology – encryption, truncation, tokenization, destruction; data stored/hosted/tokenized by ODFI, etc.
  - Would apply only to the deposit account number collected for or used in ACH transactions
    - Would not apply to the storage of paper authorizations
  - Financial institutions as internal Originators are covered by existing FFIEC and similar data security requirements and regulations
- Originators and TPSPs covered by the rule would be required to attest compliance to their ODFI (or for TPSPs and TPS, if applicable, to their counterparty with whom they have their agreement to originate or transmit ACH entries)
  - The proposed rule would be a direct obligation of Originators and TPSPs; ODFIs would not be required to ensure, verify, audit or warrant compliance of their Originators/TPSPs

Account Information Security – Rules Proposal

- Implementation would begin with the largest Originators and TPSPs (including TPSs)
  - The rule would initially apply to ACH Originators/TPSPs/TPSs with ACH volume of 6 million transactions or greater annually
    - Initially, an Originator/Third-Party that originated 6 million or more ACH transactions in calendar year 2018 would need to be compliant and attest by June 30, 2019
  - A second phase would apply to ACH Originators/TPSPs/TPSs with ACH volume of 2 million transactions or greater annually
    - An Originator/Third-Party that originated 2 million or more ACH transactions in calendar year 2019 would need to be compliant and attest by June 30, 2020
  - Many ACH Originators/TPSPs are likely compliant already, particularly those that comply with similar PCI requirements

Account Information Security – Benefits and Impacts

- Potential benefits
  - Enhanced minimum data security standards defined within the Rules
  - Improved security of customers' Protected Information, especially deposit account numbers, held by Originators/Third-Parties
  - Reduction any potential harm from data breach events
    - Associated reduction in unauthorized use of account data and ACH transactions due to stolen data
- Potential impacts
  - Implementation for those Originators and Third-Parties that currently would not be compliant
    - For all covered entities, providing attestation to their ODFI(s)
  - For ODFIs, informing Originators of their direct compliance obligations and collecting attestations

Account Information Security – Alternatives

- NACHA is requesting comments on alternatives to the proposed rule, which include
  - Requiring the use of specific data security methods or technologies (e.g., encryption to a minimum standard)
  - Using different ACH origination volume levels for initial and second-phase implementation
    - For example, 5 million (initial phase) and 1 million (second phase)
    - Eliminate phases
    - Use a different size indicator, such as number of accounts held in storage or revenue
  - Applying the requirement to all ACH Originators/Third-Parties regardless of size/volume
  - Further, the Rules could require destruction of account number data after a period of non-use

Account Information Security – Request for Comment

- NACHA requests comment on all aspect of the proposal
  - Do you agree that the existing ACH Security Framework should be supplemented by requiring that large Originators and Third-Parties that hold deposit account information used in ACH transactions should further protect that information by rendering it unreadable when stored electronically?
  - Do you agree with the volume levels for the two phases?
  - As an Originator or Third-Party, would you already be compliant with the supplemental requirement?
    - What methods or technologies are effective in rendering data unreadable?
  - As an Originator, do you need access to full account numbers in order to conduct customer service functions?
  - As an ODFI, what services do you provide that would help your Originators and Third-Parties comply?

Proposed Effective Dates

NACHA
The Electronic Payments Association®

Proposed Effective Dates

Comments are requested on all proposed effective dates

- September 21, 2018
  - Allow returns for questionable activity using R17
  - RDFIs are currently allowed to use, but without the standard descriptor
- January 1, 2019
  - Account information security, Phase 1
    - Applies to Originators and Third-Parties with volume of 6 million or more in 2018, with compliance and attestation due by June 30, 2019
- March 15, 2019
  - Time limit on RDFI claims against ODFI authorization warranty
    - As of the effective date, an RDFI would not be allowed to make a claim for a transaction that was more than one year old for a non-consumer account; or more than 18 months old for a transaction to a consumer account
- September 20, 2019
  - Commercially reasonable fraud detection – account validation for new or changed account information, and dollar amount reasonableness testing
  - Re-purposing return reason code R11 to differentiate between types of unauthorized reasons
- January 1, 2020
  - Account information security, Phase 2
    - Applies to Originators and Third-Parties with volume of 2 million or more in 2019, with compliance and attestation due by June 30, 2020