December 4, 2012

TO: NACHA Rulebook Subscribers

FROM: Danita Tyrrell, AAP
Director, Network Rules

RE: 2012 *NACHA Operating Rules* Supplement #2-2012

FOR YOUR INFORMATION

On October 31, 2012, NACHA's Voting Membership approved two amendments to the *NACHA Operating Rules (Rules):*

- ACH Security Framework; and
- Healthcare Payments via ACH.

The effective date of these changes is September 20, 2013.

This supplement provides ACH Network participants with a summary of the key components of each change, along with details regarding the technical changes to the *Rules* language.

This supplement also contains a modification to the Formal Rules Interpretation on the Proper Use of SEC Codes. Since the adoption and issuance of the interpretation in November 1997, the NACHA voting membership approved two amendments to the *Rules* concerning the proper use of SEC codes: 1) the rule allowing recurring TEL entries; and 2) the rule encompassing certain mobile-initiated entries within the scope of the WEB SEC code. NACHA's Board of Directors amended the interpretation on November 13, 2012 in order to be fully consistent with these two rules.

The amendments to the interpretation: 1) remove references that describe TEL as limited to Single Entries, and insert appropriate references to recurring TEL entries; and 2) insert references in relation to mobile-initiated ACH entries describing when it is appropriate to use either the WEB SEC Code (as consistent with the mobile rule regarding the authorization of a debit entry via a Wireless Network) or the POS SEC code (as consistent with the original Board interpretation regarding the initiation of an entry at a POS terminal). No changes were made to the guidance regarding transaction aggregation.

To ensure compliance with the most current rules, use this supplement in conjunction with your 2012 *Rules*. This information will also be available under the Supplement tab in the *ACH Rules Online* at the following link:

http://achrulesonline.org/supplements2012.aspx.

If you have any questions or need additional information regarding this supplement, please contact your regional payments association or NACHA's Network Rules Department. The Network Rules Department can be reached at (703) 561-1100.

Attachment

NACHA
The Electronic Payments Association®

NOTICE OF AMENDMENTS
TO THE
2012 NACHA OPERATING RULES

December 4, 2012

SUPPLEMENT #2-2012

1. ACH Security Framework

Effective Date: September 20, 2013

2. Healthcare Payments via ACH

Effective Date: September 20, 2013

3. Formal Rules Interpretation: Proper Use of SEC Codes

Amended: November 13, 2012

Supplement #2-2012 to the *NACHA Operating Rules*

On October 31, 2012, NACHA's Voting Membership approved two amendments to the *NACHA Operating Rules* ("*Rules*"): ACH Security Framework and Healthcare Payments via ACH. These amendments will become effective September 20, 2013.

This supplement provides ACH Network participants with a summary of the key components of each change, along with details regarding the technical changes to the 2012 *Rules* language. To ensure compliance with the most current rules, this Supplement should be used in conjunction with the 2012 *Rules*.

ACH Security Framework

(Approved October 31, 2012 – Effective September 20, 2013)

SUMMARY

The ACH Security Framework amendment creates a framework within the *NACHA Operating Rules (Rules)* aimed at protecting the security and integrity of certain ACH data throughout its lifecycle. The Security Framework establishes minimum data security obligations for ACH Network participants to protect ACH data within their purview. Specifically, the Framework:

- requires non-consumer Originators, Participating DFIs, Third-Party Service Providers and Third-Party Senders to establish, implement and, as appropriate, update security policies, procedures, and systems related to the initiation, processing and storage of Entries and resulting Protected Information;

- requires each Participating DFI, Third-Party Service Provider, and Third-Party Sender to verify, as part of its annual ACH Rules Compliance Audit, that it has established, implemented, and updated the data security policies, procedures, and systems required by the *Rules*; and

- requires an ODFI to use a commercially reasonable method to establish the identity of each non-consumer Originator or Third-Party Sender with which the ODFI enters into an Origination Agreement.

Background

Currently, the *NACHA Operating Rules* contain a number of data security and authentication requirements for ACH transactions that are generally based on individual Standard Entry Class (SEC) Codes and/or triggering events. The marketplace has changed since these security requirements were included in the *Rules* many years ago. Sound industry practices now reflect the understanding that certain financial data should be protected at all times - whether before, during or after transmission, and regardless of the form of transmission (e.g., by Internet or otherwise). By establishing minimum data security obligations, the ACH Security Framework changes will benefit the ACH Network by reducing the potential for both out-of-pocket losses experienced by ACH participants and their customers, and the damaging effect of data breaches on the reputation of the ACH Network and its participants.

KEY COMPONENTS OF RULE AMENDMENT

The ACH Security Framework amendment consists of three elements: (1) Protection of Sensitive Data and Access Controls; (2) Self-Assessment; and (3) Verification of Third-Party Senders and Originators.

Protection of Sensitive Data and Access Controls

The Security Framework requires all non-consumer Originators, Participating DFIs (as both ODFIs and RDFIs), Third-Party Service Providers, and Third-Party Senders to comply with specific security requirements with respect to the handling and storage of Protected Information. The security requirements will not apply directly to consumers, who can be Originators of CIE entries; however, such security requirements will apply to parties originating CIE Entries on behalf of consumers (i.e., the consumer's financial institution or a Third-Party Sender).

Under this rule, non-consumer Originators, Participating DFIs, Third Party Service Providers, and Third-Party Senders will be required to establish, implement, and, as appropriate, update security policies, procedures, and systems related to the initiation, processing, and storage of entries. These policies, procedures, and systems must:

(1) protect the confidentiality and integrity of Protected Information;

(2) protect against anticipated threats or hazards to the security or integrity of Protected Information; and

(3) protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

The amendment defines Protected Information 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.

The definition of Protected Information not only covers financial information, but also includes sensitive non-financial information (such as non-financial account information contained in Addenda Records for bill payments) that may be incorporated into the Entry or any related Addenda Record.

By covering natural persons, the rule on the protection of sensitive data applies to consumer information only, which is consistent with the approach of aligning the Security Framework with existing industry regulations and guidance. Impacted ACH participants, however, may apply the rule more broadly so that it covers all customers.

The security policies, procedures, and systems of ACH participants covered by the Security Framework must include controls on system access that comply with applicable regulatory guidelines. The impacted systems include all of those used by the ACH participant to initiate, process, and store entries. Although it is expected that security policies will be reviewed and approved at a level of responsibility within an organization that is commensurate with the importance of the subject matter, this amendment does not include specific requirements regarding the level of approval of such policies and procedures, thus providing institutions flexibility to accommodate their respective corporate governance structures.

Self-Assessment

The amendment requires each Participating DFI, Third-Party Service Provider, and Third-Party Sender to verify, as part of the requirements for an annual ACH Rules Compliance Audit, that it has established, implemented, and updated the data security policies, procedures, and systems required by the ACH Security Framework.

As with all provisions of the *Rules*, the annual Rules Compliance Audit applies directly to DFIs and third-parties, but not directly to Originators. Originators are bound to the *NACHA Operating Rules* through their Origination Agreements with their ODFIs. As such, Originators must ensure that they have existing policies, procedures, and systems in place that will enable compliance with the Security Framework

Verification of Third-Party Senders and Originators

The amendment establishes a requirement that an ODFI use a commercially reasonable method to determine the identity of each non-consumer Originator or Third-Party Sender with which the ODFI enters into an Origination Agreement, at the time the agreement is created. The *NACHA Operating Rules* currently require an ODFI to warrant that the ODFI has used a commercially reasonable method to establish the identity of the Originator or Third-Party Sender that entered into an Origination Agreement via an Unsecured Electronic Network. The Security Framework replaces this warranty with a new prerequisite to origination that more broadly requires the ODFI to verify the identity of all Originators/Third-Party Senders, regardless of the manner in which the Origination Agreement was executed. The amendment makes the requirement an obligation rather than a "warranty" as previously used for transmissions over Unsecured Electronic Networks.

IMPACT TO PARTICIPANTS

Originators: Each non-consumer Originator will incur costs related to an initial effort to determine whether it has existing policies, procedures, and systems in place that would enable it to comply with the Security Framework. A non-consumer Originator that is in compliance with existing data security regulations should also be in compliance with the amendment and will have no to low implementation costs. Non-consumer Originators that do not have such policies, procedures, and systems will incur costs in establishing and/or updating such policies, procedures, and systems to ensure compliance with the Security Framework.

ODFIs: Each ODFI will incur costs related to an initial effort to determine whether it has existing policies, procedures, and systems in place that would enable it to comply with the amendment. An ODFI that is in compliance with existing data security regulations should also be in compliance with the amendment and will have no to low implementation costs. An ODFI that does not have such policies, procedures, and systems will incur costs in establishing and/or updating such policies, procedures, and systems to ensure compliance with the Security Framework. Each ODFI also will incur ongoing costs to make commercially reasonable efforts to verify the identity of its Originators and Third-Party Senders. However, such costs will only be incremental over the ODFI's existing costs to the extent that it does not currently conduct such assessments and verification. Finally, ODFIs would incur minimal incremental costs to add a verification item to their annual Rules Compliance Audit.

Third-Party Service Providers and Third-Party Senders: Each Third-Party Service Provider and each Third-Party Sender will incur costs related to an initial effort to determine whether it has existing policies, procedures, and systems in place that will enable it to comply with the amendment. A Third-Party Service Provider or Third-Party Sender that is in compliance with existing data security regulations should also be in compliance with the Security Framework and will have no to low implementation costs. Each Third-Party Service Provider or Third-Party Sender that does not have such policies, procedures, and systems will incur costs in establishing and/or updating such policies, procedures, and systems to ensure compliance with the Security Framework. Third-parties will incur minimal incremental costs to add a verification item to their annual Rules Compliance Audit.

RDFIs: Each RDFI will incur initial costs to determine whether it has existing policies, procedures, and systems in place that will allow it to comply with the amendment, to the extent the RDFI receives Protected Information. An RDFI that is in compliance with existing data security regulations should also be in compliance with the Rule and will have no to low implementation costs. An RDFI that does not have such policies, procedures, and systems will incur costs in establishing and/or updating such policies, procedures, and systems to ensure compliance with the Security Framework. Finally, RDFIs will incur minimal incremental costs to add a verification item to their annual Rules Compliance Audit.

TECHNICAL SUMMARY

The changes to the *Rules* language, as noted below, represents modifications to the *NACHA Operating Rules* that will become effective on September 20, 2013.

- *Article One, Subsection 1.2.2 (Audits of Rules Compliance)* - modified to correct language related to Third-Party Senders for consistency throughout the *Rules*.

- *Article One, Subsection 1.6 (Security Requirements)* - new subsection incorporates general ACH Security Requirements into the *NACHA Operating Rules*.

- *Article Two, Subsection 2.2.1 (ODFI Verification of Originator or Third-Party Sender Identity)* - new subsection creates an obligation for the ODFI to use a commercially reasonable method to establish the identity of each Originator or Third-Party Sender.

- *Article Two, Subsection 2.4.1.8 (ODFI has Verified the Identity of Originator or Third-Party Sender That Uses an Unsecured Electronic Network Dishonor of Return by ODFI)* - this subsection is removed from the *Rules.*

- *Article Eight, Section 8.67 (Protected Information)* - adds a definition for the new term "Protected Information."

- *Appendix Eight, Part 8.2 (Audit Requirements for All Participating DFIs)* - adds a new item "f" that requires annual ACH Rules Compliance Audits to include a verification that the covered ACH participants (i.e., Participating DFIs, Third-Party Service Providers, and Third-Party Senders) have established, implemented, and updated (as appropriate) the security policies, procedures, and systems as required by the Security Requirements provisions.

- *Appendix Eight, Part 8.4 (Audit Requirements for ODFIs)* - modifies item "i" for consistency with the new subsection 2.2.1.

Implementation Date: September 20, 2013

• • • •

As approved October 31, 2012, effective September 20, 2013, the Rules are modified as follows for the rule change related to the ACH Security Framework:

ARTICLE ONE

General Rules

SUBSECTION 1.2.2 Audits of Rules Compliance

A Participating DFI must annually conduct, or have conducted, an audit of its compliance with these Rules in accordance with Appendix Eight (Rule Compliance Audit Requirements). A Third-Party Service Provider, including a Third Party Sender, that has agreed with a Participating DFI to process Entries must annually conduct, or have conducted, an audit of its compliance with these Rules in accordance with Appendix Eight (Rule Compliance Audit Requirements).

▶*A Participating DFI must annually conduct, or have conducted, an audit of its compliance with these Rules in accordance with Appendix Eight (Rule Compliance Audit Requirements). A Third-Party Service Provider or a Third Party Sender that has agreed with a Participating DFI to process Entries must annually conduct, or have conducted, an audit of its compliance with these Rules in accordance with Appendix Eight (Rule Compliance Audit Requirements).*

▶SECTION 1.6 Security Requirements (new section)

Each non-consumer Originator, Participating DFI, and Third-Party Service Provider must establish, implement, and update, as appropriate, policies, procedures, and systems with respect to the initiation, processing, and storage of Entries that are designed to:

(a) protect the confidentiality and integrity of Protected Information until its destruction;

(b) protect against anticipated threats or hazards to the security or integrity of Protected Information until its destruction; and

(c) protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

Such policies, procedures, and systems must include controls that comply with applicable regulatory guidelines on access to all systems used by such non-consumer Originator, Participating DFI, or Third-Party Service Provider to initiate, process, and store Entries.

An ODFI may dishonor a Return Entry, with the exception of an IAT Return Entry, if:

ARTICLE TWO

Rights and Responsibilities of ODFIs, Their Originators and Third-Party Senders

▶*SUBSECTION 2.2.1 ODFI Verification of Originator or Third-Party Sender Identity (new subsection)*

The ODFI must utilize a commercially reasonable method to verify the identity of an Originator or Third-Party Sender at the time the ODFI enters into an Origination Agreement with the Originator or Third-Party Sender.

SUBSECTION 2.4.1.8 The ODFI has Verified the Identity of Originator or Third-Party Sender That Uses an ▶*Unsecured Electronic Network (this subsection will be removed from the Rules)*

The ODFI has utilized a commercially reasonable method to establish the identity of an Originator or Third-Party Sender that entered into an Origination Agreement via an Unsecured Electronic Network.

ARTICLE EIGHT

Definitions of Terms Used in These Rules

▶*SECTION 8.67 "Protected Information"*

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.

APPENDIX EIGHT

Rule Compliance Audit Requirements

PART 8.2 Audit Requirements for All Participating DFIs

Each Participating DFI, Third-Party Service Provider, and Third-Party Sender must conduct the following audit of ACH operations. These audit specifications apply generally to all Participating DFIs, regardless of a Participating DFI's status as an ODFI or RDFI.

a. Verify that a Record of each Entry is retained for six years from the date the Entry was Transmitted, except as otherwise expressly provided in these Rules. Verify that a printout or reproduction of the information relating to the Entry can be provided, if requested by the Participating DFI's customer or any other Participating DFI or ACH Operator that originated, Transmitted, or received the Entry. (Article One, subsections 1.4.1 and 1.4.2)

b. When a Record required by these Rules is created or retained in an Electronic form, verify that the Electronic form (a) accurately reflects the information in the Record, and (b) is capable of being accurately reproduced for later reference, whether by Transmission, printing, or otherwise. (Article One, subsection 1.4.3)

c. Verify that the Participating DFI conducted an audit of its compliance with the rules in accordance with Appendix Eight (Rule Compliance Audit Requirements) for the previous year. (Article One, subsection 1.2.2)

d. Verify that required encryption or a secure session is used for banking information transmitted via an Unsecured Electronic Network. (Article One, subsection 1.6)

e. Verify that the Participating DFI has reported and paid to the National Association (a) all annual fees, and (b) a per-Entry fee for each Entry that is Transmitted or received by the Participating DFI, including those Entries that are not processed through an ACH Operator but are exchanged with another non-affiliated Participating DFI. (Article One, subsection 1.10)

f. Verify that the Participating DFI has conducted an assessment of the risks of its ACH activities and has implemented a risk management program on the basis of such an assessment. (Article One, subsection 1.2.4)

▶ *g. Verify that the Participating DFI has established, implemented and updated, as appropriate, security policies, procedures and systems as required by Article One, Section 1.6. (Article One, Section 1.6).*

PART 8.4 Audit Requirements for ODFIs

In addition to the audit procedures outlined in Parts 8.1 (General Audit Requirements) and 8.2 (Audit Requirements for All Participating DFIs) of this Appendix Eight, ODFIs, Third-Party Service Providers, and Third-Party Senders must conduct an audit of the following relating to the origination of ACH entries:

a. Verify that the ODFI has entered into Origination Agreements with all Originators or Third-Party Senders that bind the Originator or Third-Party Sender to these Rules; that authorize the ODFI to originate entries on behalf of the Originator or Third-Party Sender; that, within such agreements, the Originator or Third-Party Sender acknowledges that Entries may not be initiated that violate the laws of the United States; that includes any restrictions on types of Entries that may be originated; that includes that the Third-Party has entered into an agreement with each Originator/ and that such agreements include the right of the ODFI to terminate or suspend the agreement for breach of the Rules, and the right of the ODFI to audit the Originator's, the Third-Party Sender's and the Third-Party Sender's Originators' compliance with the Origination Agreement and the Rules. With respect to IAT Entries, verify that agreements contain all necessary provisions. (Article Two, subsections 2.2.1.1, 2.2.1.2 and 2.5.8.3)[1]

[1] *Article Two, Subsections 2.2.1.1(d), (e) and (f) and 2.2.1.2(d), (e), (f) and (g) are applicable to Origination Agreements that were entered into on or after June 18, 2010.*

b. Verify that, if applicable, the ODFI has entered into agreements with all Sending Points that Transmit Entries on the ODFI's behalf to an ACH Operator. (Article Two, subsection 2.2.1.3)

c. Verify that the ODFI has assessed the risks of the Originator's or Third-Party Sender's ACH activity, and has established and implemented an exposure limit for each Originator or Third-Party Sender. Verify that the ODFI has established, implemented, and periodically reviewed procedures to monitor the Originator's or Third-Party Sender's origination and return activity across multiple Settlement Dates; enforce restrictions on the types of Entries that may be originated; and enforce the exposure limit. (Article Two, subsection 2.2.2)

d. Verify that the ODFI accepts Return Entries and Extended Return Entries that comply with these Rules and that are Transmitted by the RDFI within the time limits established by these Rules. Verify that dishonored Return Entries are Transmitted within five banking days after the Settlement Date of the Return Entry and that contested dishonored Return Entries are accepted, as required by these rules. Verify that the ODFI is using return reason codes in an appropriate manner. (Article Two, subsections 2.12.1, 2.12.5.1, and 2.12.5.2; Appendix Four)

e. Verify that information relating to NOCs and Corrected NOCs is provided to each Originator or Third-Party Sender within two Banking Days of the Settlement Date of the NOC or Corrected NOC in accordance with Appendix Five (Notification of Change). Verify that refused NOCs are Transmitted within fifteen (15) days of receipt of an NOC or corrected NOC. (Article Two, subsections 2.11.1 and 2.11.2)

f. With the exception of XCK entries, verify that the ODFI provides to the RDFI, upon receipt of the RDFI's written request, the original, a copy, or other accurate Record of the Receiver's authorization with respect to a Consumer Account within ten banking days without charge. (Article Two, subsections 2.3.2.5 and 2.5.18.6)

g. Verify that, when agreed to by the ODFI, late Return Entries are accepted in accordance with these rules. (Article Two, subsection 2.12.6)

h. Verify that the ODFI has provided the Originator with proper notice to ensure compliance with UCC Article 4A with respect to ACH transactions. (Article Two, subsection 2.3.3.2)

i. Verify that the ODFI has utilized a commercially reasonable method to establish the identity of each Originator or Third-Party Sender that uses an Unsecured Electronic Network to enter into an Origination Agreement with the ODFI. When an ODFI has a relationship with a Third-Party Sender rather than with an Originator directly, also verify that the Third-Party Sender has utilized a commercially reasonable method to establish the identity of each Originator that uses an Unsecured Electronic Network to enter into an Origination Agreement with the Third-Party Sender. (Article Two, subsections 2.4.1.8 and 2.15.2)

▶ *i. Verify that the ODFI has utilized a commercially reasonable method to verify the identity of each Originator or Third-Party Sender that enters into an Origination Agreement with the ODFI. When an ODFI has a relationship with a Third-Party Sender rather than with an Originator directly, also verify that the Third-Party Sender has utilized a commercially reasonable method to establish the identity of each Originator that enters into an Origination Agreement with the Third-Party Sender. (Article Two, subsection 2.2.1)*

j. Verify that Reversing Entries and Reversing Files are initiated in accordance with the requirements of these Rules. (Article Two, sections 2.8 and 2.9)

k. For BOC Entries, verify that the ODFI has (1) established and implemented commercially reasonable procedures to verify the identity of each Originator or Third-Party Sender of such entries; and (2) established and implemented procedures to document specific information with respect to each Originator, as required by these rules, and that, upon request, such information is provided to the RDFI within the required time frame. (Article Two, subsection 2.5.2.5)

l. Verify that the ODFI has reported Return Rate information on each Originator or Third-Party Sender, as requested by the National Association. (Article Two, subsection 2.17.2)

m. Verify that the ODFI has (1) registered its Direct Access status with the National Association; (2) obtained the approval of its board of directors, committee of the board of directors, or its designee for each Direct Access Debit Participant; (3) provided required statistical reporting for each Direct Access Debit Participant; and (4) notified the National Association of any change to the information previously provided with respect to any Direct Access Debit Participant. (Article Two, subsection 2.17.1)

n. Verify that the ODFI has kept Originators and Third-Party Senders informed of their responsibilities under these rules. (Article Two, section 2.1)

Healthcare Payments via ACH

(Approved October 31, 2012 – Effective September 20, 2013)

SUMMARY

The Healthcare Payments via ACH changes amend the *NACHA Operating Rules ("Rules")* to support health plans' and healthcare providers' use of the ACH Network for healthcare claims payments and payment related information. This amendment includes processing enhancements and transaction identification and formatting requirements specific to healthcare claim payments.

Background

The Patient Protection and Affordable Care Act (ACA) requires the Department of Health and Human Services (HHS) to adopt a standard for Health Care Electronic Funds Transactions, as well as industry-vetted operating rules regarding the use of the standard transaction. On January 10, 2012, HHS issued an Interim Final Rule with Comment[2] that:

1) adopted the NACHA Corporate Credit or Debit Entry with Addenda Record (CCD+) as the standard for Healthcare EFT (electronic funds transfers);

2) adopted the ASC X12 835 TRN Segment ("reassociation number")[3] as the standard for the data content of the Addenda Record of the CCD+; and

3) discussed NACHA's role in the development and maintenance of the CCD+ standard through the *Rules*.

On August 10, 2012, HHS issued another Interim Final Rule with Comment[4] that adopted the Council on Affordable Quality Healthcare Committee on Operating Rules for Information Exchange (CORE) Phase III CORE EFT & ERA Operating Rule Set as the industry-vetted operating rules for EFT and ERA (electronic remittance advice). The CORE rule set includes five Operating Rules, of which the most critical for financial institutions is the Phase III CORE EFT & ERA Reassociation (CCD+/835) Rule. The EFT & ERA Reassociation Rule

- requires that the "provider must proactively contact its financial institution to arrange for the delivery of the CORE-required Minimum CCD+ Data Elements" and obligates health plans to proactively inform health care providers of this requirement during EFT enrollment; and

- describes the CORE-required Minimum CCD+ Data Elements as three fields in the ACH CCD record that are used for reassociation of the ACH Entry and the Electronic Remittance Advice (ERA): 1) the Effective Entry Date field (CCD Record 5, Field 9); 2) the Amount field (CCD Record 6, Field 6); and 3) the Payment Related Information field (CCD Record 7, Field 3).

[2] Administrative Simplification: Adoption of Standards for Health Care Electronic Funds Transfers (EFTs) and Remittance Advice, *http://www.gpo.gov/fdsys/pkg/FR-2012-01-10/pdf/2012-132.pdf*

[3] *The reassociation number does not constitute Protected Health Information as defined by HIPAA.*

[4] Administrative Simplification: Adoption of Operating Rules for Health Care Electronic Funds Transfers (EFT) and Remittance Advice Transactions, *http://www.gpo.gov/fdsys/pkg/FR-2012-08-10/pdf/2012-19557.pdf*

KEY COMPONENTS OF RULE AMENDMENT

The Healthcare Payments via ACH amendment consists of five components.

Unique Identification of Health Care EFTs

This amendment requires Originators to clearly identify CCD Entries that are Health Care EFT Transactions through the use of a specific identifier. The presence or absence of this healthcare-specific indicator provides RDFIs with certainty in distinguishing Health Care EFT Transactions from non-health care CCD Entries, allowing RDFIs the ability to comply with the *Rules* and specific processing requests from health care customers.

Specifically, the new rules require Originators of Health Care EFT Transactions to populate the Company Entry Description field of the CCD Entry with the value "HCCLAIMPMT". RDFIs will be able to identify a CCD Entry with this standard description as a Health Care EFT Transaction. This descriptive statement is readable, providing healthcare providers with additional information about the payment. Finally, this standard description enables various ACH participants (including NACHA in cooperation with the ACH Operators) to have greater data available on the volume of Health Care EFT Transactions.

Additional Formatting Requirements for Health Care EFT Transactions

For each CCD Entry that contains the healthcare indicator, as described above, the Originator is required to ensure that the CCD Entry complies with the following formatting requirements, which are necessary to provide Receivers (healthcare providers) with clear identification of the source and purpose of the payment.

- *Company Name*

As is required for all ACH transactions, the Company Name field must be populated with information that is readily recognized by the Receiver, in this case a healthcare provider. The amendment requires an Originator of a Health Care EFT Transaction to populate the Company Name field of the CCD Entry with the name of the health plan. In situations where an organization is self-insured, this field could contain the name of the organization's third-party administrator that is recognized by the healthcare provider and to which the healthcare provider submits its claims. Recognizing that there are other potential variations in health claims processing models, the overarching intent of NACHA's existing Company Name Rule applies – that the Company Name field contain the name of the payor that is known and readily recognized by the Receiver (healthcare provider).

- *Addenda Record and Payment Related Information Requirements for Health Care EFT Transactions*

The new rule requires Originators to include an addenda record with each CCD Entry used for a Health Care EFT Transaction. The rule also requires Originators to populate the Payment Related Information field of the addenda record with the ANSI ASC X12 Version 5010 835 TRN (Reassociation Trace Number) data segment. The TRN data segment, along with additional information contained within the Entry, is needed by healthcare providers to reassociate the Health Care EFT Transaction with the electronic remittance advice (ERA) that is transmitted separately.

Delivery of Payment Related Information (Reassociation Number)

The Healthcare Payments via ACH amendment aligns with the existing rules regarding the delivery of payment related information.[5] The rule requires an RDFI to provide or make available, either automatically

[5] *Among ACH participants, the Payment Related Information is commonly referred to as the "remittance information." For a CCD Entry that is a Health Care EFT, the Payment Related Information will always contain the "reassociation number" (i.e., the ASC X12 835 TRN Segment), and not detailed remittance information that contains Protected Health Information. Readers should not confuse the common ACH usage of "remittance information" with the terms "remittance advice" or "electronic remittance advice (ERA)" as used in the health care industry to mean the detailed explanation of benefits.*

(if such a service is established by the RDFI) or upon the request of a Receiver that is a healthcare provider, all information contained within the Payment Related Information field of an Addenda Record transmitted with a CCD Entry that is a Health Care EFT Transaction. The RDFI is required to provide or make available the Payment Related Information no later than the opening of business on the RDFI's second Banking Day following the Settlement Date of the Entry. The rule also requires the RDFI to offer or make available to the healthcare provider an option to receive or access the Payment Related Information via a secure, electronic means that provides a level of security that, at a minimum, is equivalent to 128-bit RC4 encryption technology.

Under this rule, an RDFI's obligation to provide healthcare EFT payment related information upon the Receiver's request is very similar to current requirements for other business-to-business payments. The rule, however, explicitly incorporates language regarding the "automatic" provision or delivery of payment related information transmitted with a Health Care EFT Transaction as an option for RDFIs. Any RDFI that decides to automatically provide this information to Health Care Provider customers, without waiting for it to be requested, would be in compliance with the rule. The inclusion of the term "automatically" as an option does not require the RDFI to proactively deliver the information, but recognizes that there are RDFIs that, either now or in the future, automatically provide the payment related information to their customers through online access to their account information or other methods. While automatic delivery of payment related information has always been acceptable for CCD Entries, the addition of the term "automatically" at this time recognizes this capability, especially as relates to health care, and acknowledges that the automatic delivery of the data is in compliance with the new rule.

The requirement that an RDFI must offer, or make available, to Health Care Providers an option to receive the healthcare payment related information electronically via a secure electronic delivery channel adopts an encryption standard that is consistent with other data security requirements under the *NACHA Operating Rules* (see Article One, Section 1.6) regarding the secure transmission of banking information over unsecured electronic networks. It is consistent with CAQH CORE rules regarding "connectivity" via the public Internet using SSL/HTTPS-level security. Examples of a secure, electronic delivery channel can include SSL or HTTPS secure e-mail, online account access, online reports, or file transmissions that meet the 128-bit RC4 encryption technology minimum standard. Mail, unsecured fax or unsecured e-mail of payment related information is not considered a secure, electronic delivery method.

Finally, the rule clarifies that the new reassociation information delivery requirements apply to Health Care EFT Transactions that are sent to Non-Consumer Accounts of Receivers. While the existing rules have always been based on the presumption that SEC Codes are used correctly (in this case, that CCDs are business-to-business transactions and directed to business accounts), the rule clarifies that RDFIs will not incur new obligations if Receivers do not use appropriately designated Non-Consumer Accounts to receive Health Care EFT Transactions.

Addition of New EDI Data Segment Terminator

The Healthcare Payments via ACH changes provide for the use of a second data segment terminator, the tilde ("~"), to any data segments carried in the Addenda Record of the CCD Entry.[6] As the tilde is a valid character for ACH Entries, it should already be recognized as such by ACH processing software. EDI translation software, however, might need to be modified to recognize the tilde as a valid data segment terminator for the CCD Addenda Record and NACHA-approved banking conventions.

[6] *Appendix Three of the NACHA Operating Rules currently defines the asterisk ("*") as the delimiter between data segments, and the backslash ("\") as the terminator indicating the end of a data segment included within the addenda records of ACK, ATX, CCD, CIE, ENR, IAT, PPD, and WEB Entries. The proposed addition of the tilde as a valid data segment terminator for health care CCD Entries would also apply to all of these SEC Codes to ensure consistent processing of remittance information.*

Healthcare Terminology within the NACHA Operating Rules

This rule expands the defined terms within the *NACHA Operating Rules* to 1) incorporate four health care-specific concepts within their scope, and 2) define a Non-Consumer Account to ensure appropriate application of health care-specific rules by ACH participants.

Health Care EFT Transaction: a CCD Entry originated by a Health Plan to a Health Care Provider with respect to a health care claim. Under this definition, a Health Care EFT Transaction must include one addenda record that contains an ASC X12 Version 5010 835 TRN (Reassociation Trace Number) data segment within the Payment Related Information field.

Health Plan: an individual or group plan that provides, or pays the cost of, medical care.

Health Care Provider: a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

CORE-required Minimum CCD+ Reassociation Data Elements: information transmitted by a Health Plan to a Health Care Provider for the purpose of re-associating a Health Care EFT Transaction with an electronic remittance advice. The CORE-required Minimum CCD+ Reassociation Data Elements include the information contained within the Effective Entry Date field, the Amount field, and the Payment Related Information field of the CCD Entry.

In addition, this adds a definition for Non-Consumer Account to assist ACH Participants in properly applying rules governing Health Care EFT Transactions. The term Non-Consumer Account is used to clarify the types of accounts for which the requirements to provide or make available payment related information apply.

Non-Consumer Account: an account held by a Participating DFI and established by an Organization primarily for commercial purposes. A Non-Consumer Account may be established by a natural person if the Participating DFI's records indicate that the account is primarily for commercial and not for personal, family, or household purposes (i.e., it is not a Consumer Account).

IMPACT TO PARTICIPANTS

Receivers: Receivers (Health Care Providers) should not incur any direct costs as a result of the adoption of these changes. Existing bank accounts can readily accept the receipt of ACH credit payments. Health Care Providers that elect to upgrade systems to automatically use the TRN Reassociation Data Segment to reassociate the ACH payment with the electronic remittance advice transmitted separately may incur some transition costs.

RDFIs: RDFIs that do not currently offer a secure, electronic means of delivering payment related information to their business customers will need to establish a means of doing so and make such access available to Health Care Providers receiving Health Care EFT Transactions. RDFIs with EDI translation software also may incur programming costs to ensure that the tilde is recognized as a valid data segment terminator for ACH entries.

ODFIs and Originators of Health Care EFT Transactions: These participants may incur one-time programming costs if they choose to automate the formatting of Health Care EFT Transactions to include the required Company Entry Description and the required addenda record.

TECHNICAL SUMMARY

Below is a summary of the impact of this rule change on the *NACHA Operating Rules.* Sections of the *Rules* that are affected by this amendment are also included below and reflect rule language as it will read upon implementation.

- *Article Two, Subsection 2.5.3 (General Rule for CCD Entries – Corporate Credit or Debit Entry)* - identifies Health Care EFT Transactions as CCD Entries having a mandatory addenda record in which required health care payment related information must be included.

- *Article Three, Subsection 3.1.5.3 (RDFI Must Provide Payment-Related Information to Receivers of CCD, CTX, CIE and IAT Entries to Non-Consumer Accounts)* -

  – requires RDFIs to provide or make available, either automatically or upon the request of a Receiver that is a Health Care Provider, all information contained within the Payment Related Information field of an Addenda Record transmitted with a Health Care EFT Transaction.

  – requires RDFIs to offer Health Care Provider Receivers a secure, electronic delivery channel for the receipt of health care payment related information.

  – adds language recognizing that some RDFIs automatically provide their business customers with payment related information.

- *Article Eight, Subsections 8.19, 8.44, 8.45, 8.46, and 8.57* - new subsections to define the following terms within the *Rules*:

  – CORE-required Minimum CCD+ Reassociation Data Elements
  – Health Plan
  – Health Care EFT Transaction
  – Health Care Provider
  – Non-Consumer Account

- *Appendix One, Part 1.2 (Data Specifications for ACH Records)* - requires the Company Entry Description specific to Health Care EFT Transactions to be presented in upper case characters.

- *Appendix Three, Subpart 3.1.8 (Sequence of Records for CCD Entries)* - adds footnotes specific to Health Care EFT Transactions to the CCD record layouts.

- *Appendix Three, Subpart 3.2.2 (Glossary of Data Elements)* - expands the descriptions of the following fields to accommodate formatting requirements specific to Health Care EFT Transactions:

  – Addenda Record Indicator
  – Company Entry Description
  – Company Name
  – Payment Related Information

Implementation Date: September 20, 2013

• • • •

As approved October 31, 2012, effective September 20, 2013, the Rules are modified as follows for the rule changes related to Healthcare Payments via ACH:

ARTICLE TWO

Rights and Responsibilities of ODFIs, Their Originators and Third-Party Senders

SUBSECTION 2.5.3 General Rule for CCD Entries (Corporate Credit or Debit Entry)

A CCD Entry is originated by an Organization to or from the account of that Organization or another Organization. A CCD Entry may be a credit Entry or a debit Entry, and may provide payment related information in one Addenda Record. A CCD Entry may also be a Non-Monetary Entry that carries payment related information in one Addenda Record.

▶ *A CCD Entry that is a Health Care EFT Transaction must include one Addenda Record that contains the ASC X12 835 TRN (Reassociation Trace Number) data segment in the Payment Related Information field.*

ARTICLE THREE

Rights and Responsibilities of RDFIs and Their Receivers

SUBSECTION 3.1.5.3 RDFI Must Provide Payment-Related Information to Receivers of CCD, CTX, CIE and IAT Entries to Non-Consumer Accounts

Upon the request of a Receiver, an RDFI must provide to the Receiver all information contained within the Payment Related Information field of an Addenda Record(s) Transmitted with a CCD or CTX Entry, or a CIE or IAT Entry to a non-Consumer Account. The RDFI must provide this information by the opening of business on the RDFI's second Banking Day following the Settlement Date of the Entry.

▶ *Upon the request of a Receiver, an RDFI must provide to the Receiver all information contained within the Payment Related Information field of an Addenda Record(s) Transmitted with a CCD Entry that is not a Health Care EFT Transaction, a CTX Entry, or a CIE or IAT Entry to a Non-Consumer Account. The RDFI must provide this information by the opening of business on the RDFI's second Banking Day following the Settlement Date of the Entry.*

For a Health Care EFT Transaction to a Non-Consumer Account, an RDFI must, either automatically or upon the request of a Receiver that is a Health Care Provider, provide or make available all information contained within the Payment Related Information field of the Addenda Record Transmitted with the Health Care EFT Transaction. The RDFI must provide or make available the Payment Related Information by the opening of business on the RDFI's second Banking Day following the Settlement Date of the Entry. The RDFI must offer or make available to the Health Care Provider an option to receive or access the Payment Related Information via a secure, electronic means that provides a level of security that, at a minimum, is equivalent to 128-bit RC4 encryption technology.

ARTICLE EIGHT

Definitions of Terms Used in These Rules

▶*SECTION 8.19 "CORE-required Minimum CCD+ Reassociation Data Elements" (new section)*

information transmitted by a Health Plan to a Health Care Provider in a Health Care EFT Transaction for the purpose of reassociating the Health Care EFT Transaction with an electronic remittance advice. The CORE-required Minimum CCD+ Reassociation Data Elements include the information contained within the Effective Entry Date field, the Amount field, and the Payment Related Information field of the CCD Entry.

▸*SECTION 8.44 "Health Plan" (new section)*

an individual or group plan (including a self-insurance plan) that provides, or pays the cost of, medical care (i.e., the meaning of "Health Plan" assigned at 45 CFR 160.103, as modified from time to time).

▸*SECTION 8.45 "Health Care EFT Transaction" (new section)*

a CCD Entry originated by a Health Plan to a Health Care Provider with respect to a health care claim. A Health Care EFT Transaction must be accompanied by one Addenda Record that contains the ASC X12 835 TRN (Reassociation Trace Number) data segment in the Payment Related Information field.

▸*SECTION 8.46 "Health Care Provider" (new section)*

a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business (i.e., the meaning of "Health Care Provider" assigned at 45 CFR 160.103, including a provider of certain services specified in the regulation, as modified from time to time).

▸*SECTION 8.57 "Non-Consumer Account" (new section)*

an account held by a Participating DFI and established by an Organization primarily for commercial purposes. A Non-Consumer Account may be established by a natural person if the Participating DFI's records indicate that the account is primarily for commercial and not for personal, family, or household purposes (i.e., it is not a Consumer Account).

APPENDIX ONE

ACH File Exchange Specifications

PART 1.2 Data Specifications for ACH Records

The following table shows the data specifications for ACH Records.

TYPE OF FIELD	ALPHABETIC/ ALPHAMERIC	NUMERIC
Valid Characters	0-9, A-Z, a-z, space, EBCDIC values greater than hexadecimal "3F", ASCII values greater than hexadecimal "1F"	0-9

TYPE OF FIELD	ALPHABETIC/ ALPHAMERIC	NUMERIC
Justification	Left	Right
Empty Field Handling	Space filled	Zero filled
Special Notes	Certain fields require the use of UPPER CASE characters – see below.	Must be unsigned (Neither positive (+) or negative (–) signage.)

UPPER CASE characters must be used for all of the following:

- all alphabetic characters within the Standard Entry Class Code field;
- all alphabetic characters within the File ID Modifier field;
- all alphabetic characters within the Change Code and Refused COR Code fields;
- all alphabetic characters within the Return Reason Code, Dishonored Return Reason Code, and Contested Dishonored Return Reason Code fields;
- Company Entry Description fields containing the words "REVERSAL," "RETURN FEE," "RECLAIM," "NONSETTLED," "AUTOENROLL" (for ENR entries), "REDEPCHECK" (for RCK entries), and "NO CHECK" (for XCK entries); and
- ▶ *Company Entry Description fields containing the words "REVERSAL," "RETURN FEE," "RECLAIM," "NONSETTLED," "AUTOENROLL" (for ENR entries), "REDEPCHECK" (for RCK entries), "NO CHECK" (for XCK entries), and "HCCLAIMPMT" (for Health Care EFT Transactions); and*
- Company Name fields containing the words "CHECK DESTROYED" (for XCK entries).

APPENDIX THREE

ACH Record Format Specifications

SUBPART 3.2.2 Glossary of Data Elements

Addenda Record Indicator: 1 Position - Entry Detail Record and Corporate Entry Detail Record – Mandatory (ACK, ADV, ARC, ATX, BOC, CCD, CIE, CTX, DNE, ENR, IAT, MTE, POP, POS, PPD, RCK, SHR, TEL, TRC, TRX, WEB, XCK, refused ACK, refused ATX, Returns, dishonored Returns, contested dishonored Returns, COR, refused COR)

This field indicates the existence of an Addenda Record.

Code Values:

0	No Addenda Record follows the Entry
1	One or more Addenda Records follow the Entry

▶ *CCD: When used for a Health Care EFT Transaction, the value of this field must be "1."*

IAT: The value of this field for all IAT Entries, including IAT Prenotification Entries, will always be "1."

Zero dollar CCD, CTX, and IAT Entries, Notification of Change, Refused Notification of Change, Return, Dishonored Return, Contested Dishonored Return, DNE, ENR, MTE, POS, SHR, and TRX Entries: The value of this field will always be "1". This is not applicable to MTE, POS, SHR, or TRX Prenotifications.

Company Entry Description: 10 Positions – Company/Batch Header Record – Mandatory (all batches)

The Originator establishes the value of this field to provide the Receiver with a description of the purpose of the Entry. For example, "Gas bill," "Reg. Salary," "ins. prem.," "Soc. Sec.," "DTC," "Trade Pay," "PURCHASE," etc.

This field must contain the word "NONSETTLED" when the batch contains Entries that could not settle.

This field must contain the word "RECLAIM" when the batch contains Reclamation Entries.

This field must contain the words "RETURN FEE" when the batch contains Return Fee Entries

This field must contain the word "REVERSAL" when the batch contains Reversing Entries.

ADV: The Originator, i.e., the Originating ACH Operator, uses this field to describe to the institution receiving the ADV File the type of activity to which the accounting information relates.

▶ *CCD: This field must contain the word "HCCLAIMPMT" when the batch contains Health Care EFT Transactions.*

ENR: This field must contain the word "AUTOENROLL" when the batch contains Automated Enrollment Entries.

RCK: This field must contain the word "REDEPCHECK".

TRX: This field contains the routing number of the keeper.

XCK: This field must contain the words "NO CHECK".

Company Name: 16 Positions – Company/Batch Header Record – Mandatory (all batches except IAT)

This field identifies the source of the Entry and is used for descriptive purposes for the Receiver. Except as otherwise noted below, this field must contain the name by which the Originator is known to and readily recognized by the Receiver of the Entry.

In a transaction in which the Originator of a debit Entry is not the payee of the transaction (the party to which payment is ultimately being directed), the Company Name field of the debit Entry must contain the name by which the payee is known to and readily recognized by the Receiver of the Entry. In a transaction in which the Originator of a credit Entry is not the payor of the transaction (the party from which payment is ultimately being directed), the Company Name field of the credit Entry must contain the name by which the payor is known to and readily recognized by the Receiver of the Entry.

For Return Fee Entries, this field must contain the same name of the Originator as identified in the Company Name field of the underlying Entry. For a Return Fee Entry based on the return of a Check, the Company Name field must contain the name of the payee of the Check.

ADV: The ACH Operator is both the Originator and the ODFI. The ACH Operator originating the ADV File identifies itself by name in this field.

ARC, BOC: This field identifies the payee of the Eligible Source Document or the payee name indicated on the bill or invoice.

▶ *CCD: For a Health Care EFT Transaction, this field must contain the name of the Health Plan originating the Entry, or, where an organization is self-insured, the name of the organization's third-party administrator that is recognized by the Health Care Provider and to which the Health Care Provider submits its claims.*

CIE: This field contains the bill payment service provider's name.

MTE: This field identifies the owner of the terminal where the transaction was initiated.

POP, POS, SHR: This field identifies the merchant with whom the Receiver initiated the transaction.

RCK: This field identifies the Originator of the RCK Entry, which is the original payee on the face of the Check.

TRC: This field identifies the name of the keeper.

XCK: This field must contain the words "CHECK DESTROYED" (left justified).

Payment Related Information: 80 Positions – Addenda Record – Optional (ACK, ATX, CCD, CIE, CTX, DNE, ENR, IAT, PPD, TRX, WEB)

In the Addenda Records of ACK, ATX, CCD, CIE, ENR, IAT, PPD, and WEB Entries, an asterisk ("*") must be used as the delimiter between the data elements, and the backslash ("\") must be used as the terminator between the data segments.

▶ _In the Addenda Records of ACK, ATX, CCD, CIE, ENR, IAT, PPD, and WEB Entries, an asterisk ("*") must be used as the delimiter between the data elements, and the backslash ("\") or tilde ("~") must be used as the terminator at the end of a data segment._

ACK, ATX: This field contains the ANSI ASC X12 REF (Reference) data segment. This REF segment is used to convey the Identification Number contained within the original CCD or CTX Entry, and/or other information of significance to the Originator.

CCD, PPD, WEB: Addenda Records contain payment related ANSI ASC X12 data segments or NACHA endorsed banking conventions (i.e., Tax Payment, Third-Party Tax Payments, Child Support, or Electronic Dealer Drafting).

▶ *CCD, PPD, WEB: Addenda Records contain payment related ANSI ASC X12 data segments or NACHA endorsed banking conventions (i.e., Tax Payment, Third-Party Tax Payments, Child Support, or Electronic Dealer Drafting). For CCD Entries that are Health Care EFT Transactions, this field must contain the ASC X12 835 TRN (Reassociation Trace Number) data segment, which conveys the Reassociation Trace Number used by the Health Care Provider to match the payment to remittance data.*

Example: _TRN*1*12345*1512345678*999999999_

Example: _TRN*1*12345*1512345678*999999999~_

CIE: This field contains payment related ANSI ASC X12 data segments to further identify the payment or Transmit additional remittance information.

For Example:

N1*BT*JohnDoe\N3*12MainStreet\N4*21070\

CTX: This field contains information formatted in accordance with the syntax of ANSI ASC X12.5 and X12.6, an ASC X12 transaction set containing a BPR or BPS data segment, or payment related UN/EDIFACT syntax.

ANSI ASC X12.5 ("Interchange Control Structure") means the standard to define the control structures for the electronic interchange of business transactions encoded in ASC X12-based syntax. This standard provides the interchange envelope of a header and trailer for the electronic interchange through a data transmission, a structure to acknowledge the receipt and processing of this envelope, and optional, interchange-level service request structures.

ANSI ASC X12.6 ("Application Control Structure") means the standard used to define the structure of business transactions for computer-to-computer interchange. This structure is expressed using a symbolic representation of X12 data in terms of both the design and use of X12 structures, independent of the physical representation (e.g., character set encoding).

BPR or BPS Data Segment ("Beginning Segment for Payment Order/Remittance Advice") means the beginning segment for the payment order/remittance advice used in ASC X12-based syntax to indicate the beginning of a payment-related transaction set that contains the necessary banking information to process the transaction.

DNE: Addenda Records contains the following NACHA endorsed banking convention starting in position 04:

DATE OF DEATH*MMDDYY*CUSTOMERSSN*

#########*AMOUNT*$$$$.cc\

The date of death always appears in positions 18-23. If the Social Security Number (SSN) is not available, positions 38-46 contain zeros. The amount of the expected beneficiary payment always begins in position 55.

ENR: This field contains the following NACHA endorsed banking convention:

All information in this field pertains to the account holder on whose behalf the Automated Enrollment Entry is initiated.

Transaction Code – This field contains the Transaction Code of the account holder's account. This field contains "22" (Demand Credit), "27" (Demand Debit), "32" (Savings Credit), or "37" (Savings Debit). (2 positions)

Receiving DFI Identification Number -- This field contains the routing number used to identify the DFI at which the account holder maintains its account. (8 positions)

Check Digit – This field contains the check digit pertaining to the routing number for the DFI at which the account holder maintains its account. (1 position)

DFI Account Number – This field contains the account holder's account number. (1 - 17 positions)

Individual Identification Number/Identification Number – For automated enrollments initiated on behalf of consumers, this field contains the consumer's Social Security Number. For automated enrollments initiated on behalf of companies, this field contains the company's Taxpayer Identification Number. (9 positions)

Individual Name (Surname)/Company Name – This field contains the consumer's surname or the first fifteen characters of the Company Name. (1 - 15 positions)

Individual Name (First Name)/Company Name – This field contains the consumer's first name or the next seven characters of the Company Name. (1 - 7 positions).

Representative Payee Indicator/Enrollee Classification Code – For enrollments for Federal Government benefit payments, this field contains "0" (zero) meaning "no" or "1" (one) meaning "yes" to denote whether the authorization is being initiated by someone other than the named beneficiary.

For all other enrollments, this field contains "A" to indicate that the enrollee is a consumer, or "B" to indicate that the enrollee is a company. (1 position)

For Example:

22*12200004*3*123987654321*777777777*DOE*JOHN*0\

22*12200004*3*987654321123*876543210*ABCCOMPANY**B\

27*12200004*3*987654321123*876543210*ABCELECTRONICIN*DUSTRIE*B\

IAT: This field contains 80 characters of payment related information. (Note: A maximum of two optional Addenda Records may be used for IAT remittance information.)

When the Transaction Type Code Field within the First IAT Addenda Record contains ARC, BOC, or RCK, this field must contain the Check Serial Number starting in position 04:

CHECK SERIAL NUMBER\

For example: 3349809002\

When the Transaction Type Code Field within the First IAT Addenda Record contains POP, this field must contain the following NACHA-endorsed banking convention starting in position 04:

CHECK SERIAL NUMBER (MAXIMUM OF 9 CHARACTERS)*TERMINAL CITY (MAXIMUM OF 4 CHARACTERS)*TERMINAL STATE/FOREIGN COUNTRY (2 CHARACTERS)\

For example: 123456789*PARI*FR\

When the Transaction Type Code Field within the First IAT Addenda Record contains MTE, POS, or SHR, this field must contain the following NACHA-endorsed banking convention starting in position 04:

TERMINAL IDENTIFICATION CODE(MAXIMUM OF 6 CHARACTERS)*TERMINAL LOCATION (MAXIMUM OF 27 CHARACTERS)*TERMINAL CITY)MAXIMUM OF 15 CHARACTERS)

*TERMINAL STATE/FOREIGN COUNTRY
(2 CHARACTERS)\

For example:

200509*321 EAST MARKET STREET*ANYTOWN*VA\

367802*10TH & VINE STREETS*LONDON*UK\

TRX: This field contains information formatted in accordance with National Association for Check Safekeeping syntax.

APPENDIX THREE

▶ACH Record Format Specifications

Please refer to the following Sequence of Records for CCD Entries for changes related to Health Care EFT Transactions.

SUBPART 3.1.8 Sequence of Records for CCD Entries

CCD ENTRY DETAIL RECORD

FIELD	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
DATA ELEMENT NAME	**RECORD TYPE CODE**	**TRANSACTION CODE**	**RECEIVING DFI IDENTIFICATION**	**CHECK DIGIT**	**DFI ACCOUNT NUMBER**	**AMOUNT**	**IDENTIFICATION NUMBER**	**RECEIVING COMPANY NAME**	**DISCRETIONARY DATA**	**ADDENDA RECORD INDICATOR**	**TRACE NUMBER**
Field Inclusion Requirement	M	M	M	M	R	M	O	R	O	M	M
Contents	‘6’	Numeric	TTTTAAAA	Numeric	Alphameric	$$$$$$$$¢¢	Alphameric	Alphameric	Alphameric	Numeric[1]	Numeric
Length	1	2	8	1	17	10	15	22	2	1	15
Position	01-01	02-03	04-11	12-12	13-29	30-39	40-54	55-76	77-78	79-79	80-94

CCD ADDENDA RECORD

FIELD	**1**	**2**	**3**	**4**	**5**
DATA ELEMENT NAME	**RECORD TYPE CODE**	**ADDENDA TYPE CODE**	**PAYMENT RELATED INFORMATION**	**ADDENDA SEQUENCE NUMBER**	**ENTRY DETAIL SEQUENCE NUMBER**
Field Inclusion Requirement	M	M	O	M	M
Contents	‘7’	‘05’	Alphameric[2]	Numeric	Numeric
Length	1	2	80	4	7
Position	01-01	02-03	04-83	84-87	88-94

[1] *For Health Care EFT Transactions, the Addenda Record Indicator of the CCD Entry must always contain a value of "1."*

[2] *For Health Care EFT Transactions, the Payment Related Information Field of the CCD Entry Addenda Record must always contain the ASC X12 Version 5010 835 TRN Segment.*

Formal Rules Interpretation – Proper Use of SEC Codes; Aggregation of Transactions

SUMMARY

This formal interpretation of the NACHA *Rules* addresses (i) when it is appropriate to aggregate transactions into a single ACH entry, (ii) what is the most appropriate SEC code to use for specific transaction types given the method used to obtain consumer authorization, the manner in which an ACH product is used by the consumer and the information needed by RDFIs and NACHA to manage risk and, in the case of RDFIs, to manage customer relationships, and (iii) what party should be identified in the "Company Name" field of the ACH entry. The NACHA Board has determined that (i) transactions may not be aggregated under the POS or MTE codes, but may be aggregated under the WEB or PPD codes if the transactions are accumulated for more than fourteen (14) days, (ii) if either the POS or MTE code may apply to a transaction that otherwise could be characterized as WEB or PPD (including when a Receiver uses his or her mobile device to initiate a transaction at the point-of-sale), the POS or MTE code, respectively, must be used, and (iii) the payee of the underlying transaction being settled through the ACH should be identified in the "Company Name" field. This interpretation does not address the accumulation by a single merchant of multiple purchases at that merchant (e.g., weekly billing of music purchases at an internet music site). That is a separate issue that will be separately considered by NACHA.

ISSUE

Some providers of ACH services seek to aggregate transactions that occur during a single day, or over multiple days, into a single ACH entry. This aggregation may be attempted across multiple merchants and multiple transactions types (e.g., transactions at retail locations might be combined with ATM withdrawals). Accordingly, the issue has arisen whether such aggregation is permissible under the Rules, and if so, how such transactions should be handled within the existing Rules. As a corollary, if more than one of the POS, MTE, WEB or PPD codes arguably might apply on their face, which code should be used in which circumstances? Moreover, since the payee of such transactions may be different from the Originator who obtains the Recipient's authorization, which name should be included in the "Company Name" field of the ACH message?

INTERPRETATION

The NACHA Rules do not permit aggregation of transactions under the POS or MTE codes. Each time an ACH-linked card or other similar ACH service that can be used at multiple payees is used by a consumer at an electronic terminal in a retail location in the case of the POS code, or at an ATM in the case of the MTE code, the ODFI must submit a separate ACH entry that is properly formatted using the POS or MTE SEC codes, respectively. Multiple transactions at one or more electronic terminals may not be aggregated in a single POS or MTE entry.

Transactions may be aggregated under the WEB or PPD codes only in the following circumstances. The PPD code may be used for a properly authorized ACH transaction that represents a single payment on a separate account regardless of whether there have been multiple charges by the consumer to that account (i.e., for a bill payment), provided that each such payment on account covers at least fourteen (14) days of transactions. If the original enrollment for an ACH service was performed on the internet, the WEB code may be used for a properly authorized ACH transaction that represents a single payment on a separate account regardless of whether there have been multiple charges by the consumer to that account (i.e., for a bill payment), provided that each such payment on account covers at least fourteen (14) days of transactions. This fourteen (14) day window provides a clear dividing line between payments on an account, such as monthly bill payments (e.g., the monthly payment of a charge card bill), and transactions that are effectively pass-through debits to a deposit account at an RDFI.

If a consumer has an account that ordinarily is billed in periods of more than fourteen (14) days, and the consumer separately authorizes an individual payment on account for a period of less than fourteen days (for example, by logging on to the biller's website to make an individual interim payment prior to the close of a monthly billing cycle), the ODFI may process such transaction as a single PPD or WEB transaction, depending on whether the original enrollment for the ACH service was obtained on the internet. A separate authorization of payment in this context must be a specific authorization of the specific total amount to be debited at that time, and a separate specific authorization must be obtained from the consumer each time another payment of fourteen (14) days or less is made. For clarity, the use of a debit card at the point-of-sale does not constitute a separate specific authorization for this purpose.

Furthermore, the SEC Code Allocation Chart attached hereto provides guidance on the appropriate SEC Code to use in connection with transactions based on how an ACH service is being used and how the original authorization for that service was obtained. For example, if an Originator provides a debit card to consumers that can be used for a variety of transactions pursuant to a written, standing authorization to debit the amount of those transactions to a deposit account at an RDFI, the transactions should be handled as follows: Each use of the debit card at a point-of-sale terminal should be treated as a separate POS transaction; each use of the debit card at an ATM should be treated as an MTE transaction; and each use of the debit card to make purchases on the internet should be treated as a PPD transaction. By contrast, if the Originator obtains the consumer's original standing authorization for the same product via the internet, the transactions should be handled as follows: Each use of the debit card at a point-of-sale terminal still should be treated as a separate POS transaction; each use of the debit card at an ATM still should be treated as an MTE transaction; but each use of the debit card to make purchases on the internet should be treated as a WEB transaction. As indicated above, the Originator may not aggregate multiple transactions across multiple payees. However, if the "account" offered by Originator is only billed to the consumer for periods of more than fourteen (14) days, then those transactions may be processed as a single bill payment transaction under the PPD or WEB code, respectively, for the total amount owing at the end of such period.

Finally, in order to provide appropriate information to the RDFI and NACHA, the party identified in the "Company Name" field of the ACH Entry in each of these cases should be the party to which the funds ultimately will be transferred. For example, in the card product above, the ultimate payee is the merchant or owner of the ATM where the card is used, not the Originator that issues the card. Similarly, in a bill payment service, the ultimate payee is the biller, not the provider of the bill payment service.

EXPLANATION OF SEC CODE ALLOCATIONS

The following articulates the basis for the allocations set forth in the SEC Code Allocation Chart ("Chart") that accompanies the Proper Use of SEC Codes; Aggregation of Transactions Rules Interpretation ("Interpretation"). As noted, the Chart addresses only products that can be used on a recurring basis rather than individual entry transactions, which are not at issue in this Interpretation.

The first row of the Chart addresses products that are physically used at the point-of-sale for retail purchases. Box A addresses products for which both enrollment and use occurs at the point-of-sale. This is the quintessential transaction for which the POS code was originally developed.

Box B addresses products for which the original enrollment occurred on the internet, but which are then used at the physical point-of-sale. The Interpretation requires that such transactions be treated as POS because this more specific SEC code is more closely related to the nature of the transaction being initiated by the consumer at the time of use of the card. As noted above, use of this code results in the delivery of appropriate information to RDFIs to enable risk management and customer service, and also enables NACHA to more effectively conduct its risk management services for the ACH Network. Accordingly, the POS code should be used when a Receiver uses his or her mobile device enabled with near-field communication or similar technologies to authorize Entries at the point-of-sale, even if the WEB code also could technically apply.

Box C addresses products for which enrollment occurred over the telephone, e.g., via the entry of a code through a VRU, but which are then used at the physical point-of-sale. As with the other boxes in this row, the POS code is the most directly relevant code, enabling the communication of the individual transaction data to the RDFI.

Boxes D, E and F address ACH products that are used on the internet. When an ODFI (or Originator) has a pre-existing standing authorization obtained through another channel (e.g., a physically signed authorization for insurance payments), the fact that the customer later uses the ODFI's or Originator's internet service to confirm an individual payment does not require conversion of the transaction to a WEB code. Many of the risks associated with internet-based transmission of the original account information are not present in such circumstances.

Boxes G, H and I address the use of ACH products at the ATM, and raise issues very similar to the boxes in the first row of the chart. In short, in order to manage risks associated with access to their accounts at ATMs, RDFIs need to have the information communicated through the MTE transaction code, regardless of how the consumer originally enrolled in the service.

Boxes J, K and L address the authorization of ACH transactions over the phone pursuant to a previously obtained standing ACH authorization or a one-time confirmation of a previously provided written authorization form.

Similarly, the final row of the chart addresses recurring debits for which enrollment occurred via hard copy, via the internet or via the telephone. As with the preceding row, the appropriate codes for transactions relying on hard copy or internet enrollment (including VRU-based acceptance of a hard copy authorization form) are the general codes that apply based on the form of enrollment for the service — WEB for internet-based enrollment, and PPD for all others. If the Originator complies with the Rules for origination of recurring TEL transactions in connection to a telephone-based authorization (including recorded phone line and written confirmation), the TEL code applies.

NACHA SEC CODE GUIDANCE FOR RECURRING OR MULTIPLE DEBITS

TRANSACTION INITIATION METHOD	ENROLLMENT/AUTHORIZATION METHOD		
	PHYSICAL ENROLLMENT	INTERNET ENROLLMENT	TELEPHONE ENROLLMENT
Use at Point-of-Sale	Example: Customer enrolls at a merchant store, a bank branch or in response to a mail solicitation for an ACH-based debit card, and uses the card at a POS terminal Proper SEC Code: **POS** *Box A*	Example: Customer enrolls at a merchant or bank web site for an ACH-based debit card, and uses the card at a POS terminal Customer enrolls via a mobile device for an ACH-based near-field communication debit service on the device, and uses the mobile device at a POS terminal Proper SEC Code: **POS** *Box B*	Example: Customer enrolls through a merchant or bank telephone system for an ACH-based debit card, and uses the card at a POS terminal Proper SEC Code: **POS** *Box C*
Use on the Internet	Example: Customer opens account at a bank branch and authorizes debits to transfer funds into the account, and initiates such debits via the bank's web site Customer enrolls in biller's or service provider's bill payment service via mail, and initiates individual bill payments at the biller's or service provider's web site Customer enrolls at a merchant store, a bank branch or in response to a mail solicitation for an ACH-based debit card, and uses the card to make a purchase at a web site Proper SEC Code: **PPD** *Box D*	Example: Customer executes at a bank's web site an authorization to transfer funds into a savings account, and initiates each transfer via the bank's web site Customer enrolls at a biller's or service provider's web site to pay bills, and initiates individual bill payments at the web site Customer enrolls at a merchant or bank website for an ACH-based debit card, and uses the card to make a purchase at a web site Customer enrolls via a mobile device in his/her biller's mobile bill presentment and payment service, and initiates individual bill payments via the mobile device Proper SEC Code: **WEB** *Box E*	Example: Customer enrolls through a biller's or service provider's telephone system to pay bills, and initiates individual bill payments at the biller's or service provider's web site Customer enrolls through a merchant or bank telephone system for an ACH-based debit card, and uses the card to make a purchase at a web site Proper SEC Code: **PPD** *Box F*
Use at ATM	Example: Customer enrolls at a merchant store, a bank branch or in response to a mail solicitation for an ACH-based debit card, and uses the card at an ATM to withdraw cash Proper SEC Code: **MTE** *Box G*	Example: Customer enrolls at a merchant or bank web site for an ACH-based debit card, and uses the card at an ATM to withdraw cash Proper SEC Code: **MTE** *Box H*	Example: Customer enrolls through a merchant or bank telephone system for an ACH-based debit card, and uses the card at an ATM to withdraw cash Proper SEC Code: **MTE** *Box I*

TRANSACTION INITIATION METHOD	**ENROLLMENT/AUTHORIZATION METHOD**		
	PHYSICAL ENROLLMENT	**INTERNET ENROLLMENT**	**TELEPHONE ENROLLMENT**
Use via Telephone	Example: Customer opens account at a bank branch and authorizes debits to transfer funds into the account, and initiates such debits via the bank's telephone system Customer enrolls in biller's or service provider's bill payment service via mail, and initiates individual bill payments through the biller's or service provider's telephone system Customer enrolls at a merchant store or a bank branch for an ACH-based debit card, and uses the card to make a purchase over the phone Proper SEC Code: **PPD** *Box J*	Example: Customer executes at a bank's web site an authorization to transfer funds into a savings account, and initiates each transfer via the bank's telephone system Customer enrolls on a biller's or service provider's web site to pay bills, and initiates individual bill payments via the biller's or service provider's telephone system Customer enrolls on a merchant or bank website for an ACH-based debit card, and uses the card to make a purchase over the phone Proper SEC Code: **WEB** *Box K*	Example: Customer receives a written ACH authorization with a billing statement and "signs" the authorization to pay the bill by entering a code into the biller's VRU Proper SEC Code: **PPD** *Box L*
Use via Pre-Authorization (i.e., no other direct action)	Example: Customer executes in person or via mail a written authorization for a monthly ACH debit to pay a bill Customer executes in person or via mail a written authorization for a monthly ACH debit to transfer funds into another account Proper SEC Code: **PPD** *Box M*	Example: Customer executes at a biller's web site an authorization for a monthly ACH debit to pay a bill Customer executes at a bank's web site an authorization for a monthly transfer into a savings account Proper SEC Code: **WEB** *Box N*	Example: Customer receives a written ACH authorization with a billing statement and "signs" the authorization to pay the bill and future recurring bills by entering a code into the biller's VRU Proper SEC Code: **PPD** Customer calls into a recorded biller customer service line and orally authorizes monthly debits; the biller complies with the Rules for recurring TEL transactions and timely mails a written copy of the authorization Proper SEC Code: **TEL** *Box O*