NOTICE OF CHANGES TO THE 2021 NACHA OPERATING GUIDELINES

August 6, 2021

SUPPLEMENT #2-2021

Meaningful Modernization Guidelines Updates

Effective Date: September 17, 2021

Supplement #2-2021 – Changes to the Nacha Operating Guidelines

On September 17, 2021, changes to the Nacha Operating Rules resulting from the Meaningful Modernization amendment become effective. This supplement includes updates to areas of the Nacha Operating Guidelines that are impacted by these rule changes.

The Meaningful Modernization rule changes are designed to improve and simplify the ACH user experience by facilitating the adoption of new technologies and channels for the authorization and initiation of ACH payments; reducing barriers to use of the ACH Network; providing clarity and increasing consistency around certain ACH authorization processes; and reducing certain administrative burdens related to ACH authorizations. Specifically, the Meaningful Modernization rules:

- explicitly define the use of standing authorizations for consumer ACH debits;
- define and allow for oral authorization of consumer ACH debits beyond telephone calls;
- clarify and provide greater consistency of ACH authorization standards across all payment initiation channels;
- reduce the administrative burden of providing proof of authorization; and
- better facilitate the use of electronic and oral Written Statements of Unauthorized Debits.

This supplement includes replacement text for various sections of the 2021 Nacha Operating Guidelines that are impacted by the Meaningful Modernization Rule. In most cases, the changes included within this Supplement are shown as excerpts from various chapters and should replace corresponding sections of the Guidelines. In the cases of Chapter 16 (Relationship with Receiver and Authorization Requirements), Chapter 47 (Telephone-Initiated Entries), and Chapter 48 (Internet Initiated/Mobile Entries), broad revisions were necessary. This Supplement contains entire updated chapters for these topics.

For a detailed description of these changes and a listing of the Nacha Operating Rules impacted, see the Revisions section of the 2021 Nacha Operating Rules.

CHAPTER 7

ODFI Risk Management

ADDITIONAL WARRANTIES

In addition to the warranties discussed above, ODFIs also assume a number of other warranties with respect to the origination of specific types of entries. They are as follows:

Accounts Receivable Entries (ARC Entries)

- *Entry information is accurate* – The amount of the entry, the routing number, the account number, and the check serial number accurately represent the source document.

- *Source document will not be presented for payment* – The source document used for an ARC entry must not be presented for payment unless the ARC entry is returned by the RDFI. In addition to the RDFI, ACH Operator, and Association, this warranty runs to any other party that may be liable on the source document.

- *Originator will retain a copy of the source document and related payment data* – The Originator will retain a reproducible and legible copy of the front of the Receiver's source document for two years from the Settlement Date of the ARC entry. The Originator must provide the ODFI with a copy of the source document upon request. In addition, the Originator must use commercially reasonable methods to securely store all ARC source documents until destruction and all banking information relating to ARC transactions.

- *ODFI will provide a copy of the source document to RDFI* – Upon receiving a written request from the RDFI, the ODFI warrants that it will send a copy of the front of the Receiver's source document within ten banking days. The copy must indicate that it is a copy on its face. The RDFI's written request must be received by the ODFI within two years of the Settlement Date of the ARC entry.

Back Office Conversion Entries (BOC Entries)

- *ODFI verification of Originator or Third-Party Sender* – the ODFI employs commercially reasonable procedures to verify the identity of the Originator or Third-Party Sender of a BOC entry.

- *Documentation of Originators* – The ODFI has procedures to maintain the following information with respect to each Originator of BOC entries:

  - company name;
  - address;
  - telephone number;
  - contact person;
  - taxpayer identification number; and
  - a description of the nature of the business of each Originator.

- *Provision of Originator information to RDFI* – The ODFI has procedures to provide the RDFI with the information identifying an Originator of BOC entries to the RDFI within 2 banking days of receipt of the RDFI's written request for such information. The RDFI's written request must be received by the ODFI within 2 years of the Settlement Date of the BOC entry.

- *Verification of Receiver's Identity* – The Originator has employed commercially reasonable procedures to verify the identity of the Receiver.

- *Customer Service Telephone Number* – The Originator maintains a working telephone number that is answered during the Originator's normal business hours for Receiver inquiries regarding BOC transactions. This telephone number must be displayed on the required notice.

- *Entry information is accurate* – The amount of the entry, the routing number, the account number, and the check serial number accurately represent the source document.

- *Source document will not be presented for payment* – The source document used for an BOC entry must not be presented for payment unless the BOC entry is returned by the RDFI. In addition to the RDFI, ACH Operator, and Association, this warranty runs to any other party that may be liable on the source document.

- *Originator will retain a copy of the source document and related payment data* – The Originator will retain a reproducible and legible copy of the front of the Receiver's source document for two years from the Settlement Date of the BOC entry. The Originator must provide the ODFI with a copy of the source document upon request. In addition, the Originator must use commercially reasonable methods to securely store all BOC source documents until destruction and all banking information relating to BOC transactions.

- *ODFI will provide a copy of the source document to RDFI* – Upon receiving a written request from the RDFI, the ODFI warrants that it will send a copy of the front of the Receiver's source document within ten banking days. The copy must indicate that it is a copy on its face. The RDFI's written request must be received by the ODFI within two years of the Settlement Date of the BOC entry.

International ACH Transactions (IAT Entries)

- *Compliance with U.S. Legal Requirements* – The Originator and ODFI are in compliance with U.S. Legal Requirements, including their obligations under programs administered by the U. S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN).

- *Compliance with Foreign Laws or Payment System Rules Regarding Authorization* – If the laws or payment system rules of the receiving country require authorization with respect to an IAT Entry, the ODFI warrants that the authorization of the IAT Entry complies with the laws and payment system rules of the receiving country.

Point-of-Purchase Entries (POP Entries)

- *Return of voided source document to Receiver* – The Originator voided the source document used to initiate the POP entry and returned it to the Receiver at the time of the transaction.

- *Source document not used for prior POP entry* – The source document used for the POP entry was not used by the Receiver for initiating any prior POP entry.

Re-presented Check Entries (RCK Entries)

- *Good title to the returned item* – The ODFI has good title or is entitled to enforce the item related to the RCK entry. Alternatively, the ODFI is authorized to obtain payment on behalf of someone who has good title or is entitled to enforce the item.

- *Signatures are genuine* – All signatures on the item are authentic and authorized.

- *Item not altered* – The item has not been altered.

- *No defenses* – The item is not subject to a defense or claim that can be brought against the ODFI.

- *No knowledge of insolvency* – The ODFI is unaware of any insolvency proceeding involving the maker or acceptor of the item.

- *Entry accurately reflects the item* – The item is drawn on or payable through the RDFI. The re-presented check entry accurately reflects the amount of the item, the item number and the account number on the item.

- *Item will not be presented* – Unless the RCK entry is returned by the RDFI, neither the item nor any copy of the item will be presented to the RDFI.

- *Encoding is correct* – The information encoded after issue in magnetic ink on the item is correct.

- *Restrictive endorsement is void or ineffective* – The Originator agrees that any restrictive endorsement placed on the item is void or ineffective once the RCK entry is initiated.

Destroyed Check Entries (XCK Entries)

- *Good title to the check* – The ODFI has good title or is entitled to enforce the item related to the XCK entry. Alternatively, the ODFI is authorized to obtain payment on behalf of someone who has good title or is entitled to enforce the item.

- *Signatures are genuine* – All signatures on the item are authentic and authorized.

- *No alterations* – The item has not been altered.

- *No defenses* – The item is not subject to a defense or claim that can be brought against the ODFI.

- *No knowledge of insolvency* – The ODFI is unaware of any insolvency proceeding involving the maker or acceptor of the item.

- *Item drawn on RDFI* – The item is drawn on or payable through the RDFI.

- *Entry accurately reflects the item* – The destroyed check entry accurately reflects the amount of the item, the item number and the account number on the item.

- *Item will not be presented* – Neither the item nor any copy (including any image) of the item has been presented, and will not be presented, to the RDFI.

- *Authority and eligibility* – The ODFI has all necessary authority to initiate the XCK entry, and the item satisfies the eligibility requirements of the Nacha Operating Rules, Subsection 2.5.18.2 (XCK Eligible Items).

Machine Transfer Entries (MTE), Point-of-Sale Entries (POS) and Shared Network Entries (SHR)

- For MTE, POS and SHR Entries, the ODFI warrants that the Originator complies with the American National Standards Institute's (ANSI) Accredited Standards Committee (ASC) X9.8 concerning PIN Management and Security when a personal identification number (PIN) is required in connection with the authorization for the entry.

Reclamation Entries

- *Ensuring that information contained within reclamation entries is accurate* – For reclamation entries, the ODFI must ensure that:the information in the entry applies to the Receiver and account identified in the reclamation entry; the entry falls within the timing requirements governing reclamations; the entry satisfies defined prerequisites to origination; the entry is authorized by applicable legal requirements or the agreement governing the benefits to which the entry relates; and that any payments subject to reclamation are made with no restriction on the number of parties having an interest in the account.

Return Fee Entries

For Return Fee Entries, the ODFI warrants that the Originator imposing the Return Fee has not, and will not, impose any other Return Fee in relation to the underlying Entry or item that was returned unpaid. (NOTE: This warranty applies to all Return Fee Entries and is in addition to any other warranties specific to the Standard Entry Class Code used to initiate the Return Fee Entry.)

PIN Requirements

For Machine Transfer Entries (MTE), Point-of-Sale Entries (POS) and Shared Network Entries (SHR), the ODFI warrants that the Originator complies with the American National Standards Institute's (ANSI) Accredited Standards Committee (ASC) X9.8 concerning PIN Management and Security when a personal identification number (PIN) is required in connection with the authorization for the entry.

CHAPTER 10

ODFIs and Return, Dishonored Return and Contested Dishonored or Corrected Return Entries

RECEIPT OF RETURN ENTRIES

The ACH Network supports the capability to return entries for specific reasons. The process allows various participants in the Network to exercise their respective rights not to accept an entry and to return it to the Originator through the ACH Network. When the return has been transmitted by the RDFI and subsequently flows through the ACH Network to the ODFI, the ODFI has the right to dishonor the return under certain circumstances. The RDFI may react to that dishonor by accepting the dishonor, contesting the dishonor, or by correcting the return. The procedure is as follows:

1. The RDFI receives an ACH entry and returns it to the ODFI.

2. The ODFI evaluates and processes the return. In some situations, the ODFI may choose to dishonor the return if the return is untimely; contains incorrect information; is misrouted; is a duplicate; or results in an unintended credit to the Receiver related to the reversal process.

3. The RDFI either accepts the dishonored return, contests the dishonored return, or corrects the return.

This sequence can take place only once; there is no further recourse available to the parties within the ACH Network. Any disagreement beyond this point must be handled outside the ACH process.

Returns are transmitted by the ACH Operator to the ODFI (or its receiving point) and are included in regular ACH files. Therefore, the ODFI's receiving software must be able to recognize returns and sort them appropriately for action by the ODFI.

Returns can be initiated from one of two sources:

- ACH Operator – entries that cannot be processed through the ACH Network will be returned to the ODFI by the ACH Operator and will carry Return Reason Codes used only by ACH Operators. (A complete list of Return Reason Codes used by the ACH Operator appears in Appendix Two of the Nacha Operating Rules.)

  These entries were never received by the RDFI. The Originator should be notified immediately that entries were returned by the ACH Operator so that it can initiate a corrected entry or contact the Receiver about using an alternate method of payment.

- RDFI – entries are returned by the RDFI for specific reasons. (A complete list of Return Reason Codes used by the RDFI can be found in Appendix Four of the Nacha Operating Rules.)

Once returns are identified at the ODFI, the ODFI may:

- Forward the return to the Originator for action.

- Reinitiate an entry for the Originator if it has been returned for R01 (Insufficient Funds) or R09 (Uncollected Funds). (NOTE: The number of times that an entry returned for R01 or R09 can be reinitiated must not exceed the limits established by the Nacha Operating Rules.)

- Dishonor the Return. (See Dishonor of Returned Entries below.)

All ODFIs must be aware of specific processing windows offered by ACH Operators for the processing of returns. ODFIs may have returns available from ACH Operators toward the end of the business day; they should make sure that the files containing these returns are processed prior to the close of business for proper posting and handling.

When an ODFI receives a return bearing Return Reason Code R05, R07, R10, R11, R37, R51, or R53, the RDFI has warranted that it has obtained a Written Statement of Unauthorized Debit from the Receiver stating that the Receiver did not authorize the transaction or that the entry was improperly originated. The ODFI has up to one year from the return of the original entry to request, in writing, that the RDFI provide a copy of the Written Statement of Unauthorized Debit. ODFIs should establish procedures to accept requests from their Originators for copies of Written Statements of Unauthorized Debit and for making those requests to RDFIs.

ODFI Agreement to Accept Return in Lieu of Authorization

The Rules require the ODFI to provide the original, copy, or other accurate record of the Receiver's authorization in every instance in which it receives a written request for the authorization from an RDFI. However, to reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, ODFIs and Originators may agree to accept the return of the debit rather than provide the authorization to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI.

Even when the ODFI has accepted the return entry or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization. In these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the ODFI must provide the original, copy or other accurate record of the authorization to the RDFI within ten banking days of the RDFI's subsequent request. ODFIs and their Originators that choose to take advantage of this alternative should consider whether any changes or modifications to their business processes may be necessary.

CHAPTER 16

Relationship with Receiver and Authorization Requirements

The type of authorization arrangement entered into between the Receiver and the Originator, and the degree of detail required for that authorization, depends upon who the parties to the transaction are (either consumer, non-consumer) and the nature of the relationship between those parties. Corporate payments, where the Originator and Receiver have entered into a trading partner agreement, could require more intricate authorization and payment terms than consumer payments. For example, the corporate trading partner relationship could include the processing of payment related data or may be used to transfer large dollar amounts.

GENERAL AUTHORIZATION REQUIREMENTS FOR ALL ENTRIES

As a general rule, and regardless of the nature of the relationship or parties involved, certain minimum authorization standards apply to all ACH payments. Before transmitting one or more entries to any Receiver's account, the Originator must obtain the Receiver's authorization to originate those entries, except for credit entries where both the Originator and Receiver are natural persons. All authorizations must comply with any applicable legal requirements, must be readily identifiable as an ACH authorization, and must have clear and readily understandable terms. A purported authorization for any entry that is not clear and readily understandable as to its terms, or that is otherwise invalid under applicable legal requirements, does not meet the requirements of a valid authorization. The authorization must indicate whether it relates to entries directed to a demand deposit account, a savings account, a loan account or a general ledger account. Additional minimum standards for authorization apply based on whether an ACH entry is destined to a consumer account or a non-consumer account. These are discussed in detail within the consumer and non-consumer sections of this chapter.

It is important to note that the authorization requirements specified within the Rules address the minimum requirements needed for authorization of various types of ACH entries. The Rules permit ACH participants to obtain authorization in a manner that exceeds the minimum requirements, provided that all other requirements for that particular type of entry are met. As an example, the rule provisions related to certain types of electronic check transactions (e.g. ARC and BOC) permit Originators to obtain authorization by providing notice to the Receiver. In such cases, Originators may also obtain a signed, written authorization, provided that all other requirements for the type of entry are met. Originators will need to consider the impact of other requirements on any change in the manner of authorization chosen for a particular type of payment to ensure that they are also compliant with those requirements. For instance, although written authorization is permissible for BOC Entries, notice would still be required to comply with Regulation E.

CONSUMER RECEIVERS

Authorization for Credit Entries to Consumer Accounts

An Originator of a credit entry to a Receiver's consumer account may obtain the Receiver's authorization in any manner permitted by applicable legal requirements. Regardless of how the Originator obtains the Receiver's authorization for a credit, the Originator must ensure that the credit authorization is readily recognizable as an ACH authorization and has clear and readily understandable terms.

Consumers may provide authorizations for credit entries in writing, or they may be provided orally or by other non-written means. If both the Originator and Receiver are natural persons, no authorization from the Receiver is required.

Authorization for Debit Entries to Consumer Accounts

An Originator of a debit entry to a Receiver's consumer account must obtain a written authorization that is signed or similarly authenticated by the Receiver, except as otherwise expressly permitted by the Rules. In addition to meeting the general requirements for all authorizations, as discussed above, the Originator must ensure that each consumer debit authorization includes the following minimum information:

- Language clearly stating whether the authorization obtained from the Receiver is for a Single Entry, multiple entries initiated under the terms of a standing authorization, or recurring entries;
- The amount of the entry or entries, or a reference to the method of determining the amount of the entry(ies);
- The timing of the entries, including the start date, number of entries, and frequency of the entries;
- The Receiver's name or identity;
- The account to be debited and whether the account is a demand deposit account or a savings account;

- The date of the Receiver's authorization; and

- Language that instructs the Receiver how to revoke the authorization directly with the Originator. This must include the time and manner in which the Receiver must communicate the revocation to the Originator. For a single entry authorized in advance, the right of the Receiver to revoke authorization must provide the Originator a reasonable opportunity to act on the revocation instruction prior to initiating the entry.

Where an authorization is a standing authorization for the initiation of subsequent entries, the Originator may meet these requirements through a combination of the standing authorization and the Receiver's affirmative action to initiate a subsequent entry.

In any case where the Rules permit an Originator to obtain the Receiver's authorization for a debit by notice to the Receiver, the Originator also may choose, at its discretion, to obtain the Receiver's authorization by a signed, written authorization that meets the requirements described above.

Authentication of Authorization – With the exception of ARC, BOC, RCK, and Return Fee Entries, the authorization must be signed or similarly authenticated by the consumer.

Copy of Authorization to Receiver

An Originator must provide the Receiver with an Electronic or hard copy of the Receiver's authorization. The copy may be provided to the consumer via mail, internet/online network, in person or any other method allowable under applicable legal requirements. In circumstances where the consumer signs the written authorization or, alternatively, uses the telephone to similarly authenticate the written authorization by speaking or key entering a code for identification, the consumer has a paper authorization in his possession, which should be retained as the copy of the authorization. The consumer can also request an additional hard copy of the authorization from the Originator. For the Internet/online network alternative, the consumer reads the authorization that is displayed on the computer screen or other visual display. The consumer should print the authorization from his computer screen and retain this copy. The Originator must be able to provide the consumer with a hard copy of a debit authorization if requested to do so.

Similarly Authenticated

The similarly authenticated standard permits signed, written authorizations to be provided electronically. These writing and signature requirements are satisfied by compliance with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

To satisfy the requirements of Regulation E and the Nacha Operating Rules, the authentication method chosen must evidence both the consumer's identity and his assent to the authorization.

Examples of methods used to similarly authenticate an authorization include, but are not limited to, the use of digital signatures, codes, shared secrets, PINs, etc. Authentication of an authorization is strongest when the authorization and the authentication of that authorization occur simultaneously or nearly simultaneously. Although an initial website session log-in may constitute adequate authentication for a click-through authorization as part of the same session, Originators and ODFIs should consider the strength of the association of an initial log-in with a later authorization. The Originator and ODFI bear the burden of demonstrating that the authentication process is sufficiently linked to the authorization.

Retention of Authorization

The Originator must retain an original or copy of a written authorization, and readily and accurately reproducible records evidencing any other form of authorization. The record of authorization must be retained by the Originator for a period of two years following the termination or revocation of the authorization. The authorization may be retained as an electronic record that (1) accurately reflects the information in the record, and (2) is capable of being accurately

reproduced for later reference, whether by transmission, printing, or otherwise. Standing and oral authorizations have specific retention requirements that are discussed in their respective sections below.

Standing Authorizations

A Standing Authorization is an advance authorization obtained from a Receiver for one or more future entries (referred to as subsequent entries) that require the Receiver's affirmative action to initiate. An Originator of a standing authorization must meet the minimum standards for a consumer debit authorization identified above, but it may do so through a combination of the standing authorization and the Receiver's affirmative action to initiate each subsequent entry.

As part of the terms of a standing authorization, the Originator must clearly specify the action(s) that the Receiver can take to initiate a subsequent entry. These actions can include, but are not limited to, a telephone call, an internet interaction, or a text message.

Examples of standing authorizations include, among others:

- *Bill payment* - A standing authorization could allow a consumer to initiate payments on a credit card account intermittently and via various channels (phone, online, mobile app, text, virtual assistant technology, etc.)

- *E-wallet /personal financial management* - A consumer could provide a standing authorization for future debits related to using an e-wallet or other personal financial management service

- *Personal or home virtual assistants* - A standing authorization could be used in conjunction with services and apps that allow future e-commerce and payments to be initiated via virtual voice assistant or similar functionality

- *Account transfers* - A consumer could provide a standing authorization to authorize funding debits to a brokerage account based on investment activity

For a standing authorization, an Originator must retain the original or a copy of each standing authorization for two years following the termination or revocation of the authorization. The Originator must also retain proof that the Receiver affirmatively initiated each payment in accordance with the terms of the standing authorization for two years following the Settlement Date of the entry.

Receiver Account Information

In any case where the Receiver's affirmative action to initiate a subsequent entry involves the communication or confirmation of any of the Receiver's banking information (such as routing number, account number, PIN, or other identification symbol) via an unsecured electronic network, the Originator must comply with ACH data security requirements.

Standard Entry Class Codes for Subsequent Entries

In certain cases, an Originator may identify a subsequent entry using the Standard Entry Class Code appropriate either to (1) the manner in which the standing authorization was obtained from the Receiver, or (2) the manner in which the Receiver's affirmative action to initiate the subsequent entry was communicated to the Originator. However, the Rules do not allow an Originator that obtains the Receiver's standing authorization using the WEB or TEL Standard Entry Class Codes to identify subsequent entries using the PPD Standard Entry Class Code. For more information on selecting Standard Entry Class Codes, see Proper Use of Standard Entry Class Codes for Subsequent Entries later in this chapter.

Oral Authorizations

The Nacha Operating Rules permit Originators to obtain debit authorizations from consumers orally using a variety of verbal interactions and voice-related technologies. Examples of how oral authorizations could be used under the Rules include:

- the consumer's oral authorization communicated to the Originator via a traditional telephone call;
- the consumer's voice interactions with home digital assistants ("Voice Assistant, pay my bill");
- the consumer's oral authorization of a bill payment via a video chat via the Internet.

Each oral authorization must meet the minimum standards for all consumer debit authorizations identified above, regardless of the communication device or channel used to convey the Receiver's authorization. However, the requirement that an Electronic authorization must be visually displayed in a manner that enables the consumer to read the communication does not apply when the consumer's authorization is an oral authorization. In addition, where the Receiver's oral authorization is communicated (other than via a telephone call) over an Unsecured Electronic Network, the Originator must also comply with the security requirements specific to the secure transmission of ACH information over an Unsecured Electronic Network.

See Chapter 4 of these Guidelines for a discussion of an Unsecured Electronic Network.

Additional Requirements for Oral Authorization for Single Entries

- *Form of Authorization* – For a single entry authorized by the Receiver orally, the Originator is required to either make an audio recording of the consumer Receiver's oral Authorization or provide the consumer with written notice confirming the oral authorization prior to the settlement of the entry.
- *Retention of Authorization* – The Originator is required to retain the original or a duplicate audio recording of the oral authorization, or the original or a copy of the written notice confirming the oral authorization, for two years from the date of the authorization.

Additional Requirements for Oral Authorization for Recurring Entries

- *Form of Authorization* – For a recurring entry authorized by the Receiver orally, the Originator must comply with the requirements of Regulation E for the authorization of preauthorized transfers, including the requirement to send a copy of the authorization to the Receiver.
- *Retention of Authorization* – The Originator must retain the original or duplicate audio recording of the oral authorization, as well as evidence that a copy of the authorization was provided to the Receiver in compliance with Regulation E, for two years from the termination or revocation of the authorization.

Additional Requirements for Oral Authorizations that are Standing Authorizations

- *Form of Authorization* – For an oral authorization that is a standing authorization, the Originator must either make an audio recording of the consumer Receiver's oral authorization or provide the consumer with written notice confirming the oral authorization prior to the settlement of the first subsequent entry.
- *Retention of Authorization* – The Originator is required to retain the original or a duplicate audio recording of the standing oral authorization, or the original or a copy of the written notice confirming the standing oral authorization, for two years from the termination or revocation of the standing oral authorization. The Originator must also retain proof that the Receiver affirmatively initiated each payment in accordance with the terms of the standing oral authorization for two years following the settlement date of the entry.

Additional Authorization Requirements for ARC, BOC, POP, and RCK Entries

In addition to the meeting the requirements above, ARC, BOC, and POP, entry authorizations consist of notice from the Originator to the consumer and the receipt of the consumer's source document (for ARC and BOC entries) or item (for RCK entries) by the Originator.

For ARC entries for an in-person bill payment at a manned location and for BOC entries, the Originator must provide a copy of the notice or substantially similar language to the Receiver at the time of the transaction. For POP entries, the Originator must obtain the Receiver's written authorization, as discussed above, and must also provide the Receiver with notice at the point of purchase or manned bill payment location.

Please refer to Chapters 37, 38, 44, and 46 on ARC, BOC, POP, and RCK entries, respectively, for specific notice requirements.

Additional Authorization Requirements for TEL Entries

In addition to the requirements above, TEL entry authorizations may be obtained orally via the telephone for debits where there is (1) an existing relationship between the Originator and the consumer, or (2) no existing relationship between the Originator and the consumer, but the consumer has initiated the telephone call to the Originator. TEL entry authorizations must include a telephone number for Receiver inquiries that is answered during normal business hours.

Originators of TEL entries must establish and implement commercially reasonable procedures to verify that (1) the identity of the Receiver; and (2) the routing number used in the TEL entry is valid.

See Chapter 47 of these Guidelines for more information about TEL entries.

Authorization for Return Fee Entries

For a Return Fee Entry – that is, a debit entry to a consumer's account for the purpose of collecting a Return Fee – the Originator must obtain the Receiver's authorization prior to initiating the Return Fee Entry.

This can be accomplished in either of two ways:

(1) Authorization by Notice – Originators may obtain authorization for a Return Fee Entry by providing the Receiver/check writer with notice that conforms to the requirements of Regulation E at the time that the underlying ACH debit is authorized or the underlying check is accepted. Please refer to the chapter on Return Fee Entries for specific notice requirements.

(2) Authorization other than by Notice – Originators may also obtain authorization for a Return Fee Entry in any other form permitted by the Rules, dependent upon the Standard Entry Class Code used for the debit Entry to a Consumer Account (e.g., written authorization for PPD or WEB, oral authorization for TEL).

Please refer to Chapter 54 for more detailed information on authorization and specific notice requirements for Return Fee Entries.

Notice of Change in Amount/Change in Debiting Date for Recurring Debits to Consumer Accounts

When the amount of a recurring debit to a consumer account varies, specific requirements apply. If a preauthorized debit transfer varies from the immediately preceding transfer relating to the same authorization or from a fixed preauthorized amount, the Originator must send the Receiver written notification of the amount and the date on or after which of the transfer will be debited at least ten calendar days before the scheduled transfer date. Additionally, if the Originator informs the consumer of the right to receive notice of all varying transfers, the consumer may elect to receive notice only when a transfer does not fall within a specified range of amounts. Alternatively, the consumer may elect to receive notice only when a transfer differs from the most recent transfer by more than an agreed upon amount.

If the Originator changes the date on or after which a recurring debit entry to a consumer account is scheduled to be debited, the Originator must send the Receiver written notification of the new date. The Originator must send the notice at least seven (7) calendar days before the first entry to be affected by the change is scheduled to be debited to the Receiver's account.

Copy of Authorization

The Originator, upon request of the ODFI, must present the original, copy or other accurate record of the customer's authorization to an ODFI for its use or use by the RDFI. The RDFI should not ask for the customer authorization as a normal course of business but only if an exception is expected or has occurred.

In lieu of providing proof of authorization to the RDFI, the ODFI may agree to accept a return entry. However, if the RDFI subsequently still requests evidence of authorization of a debit entry to a consumer account, the ODFI must provide the original, copy, or other accurate record to the RDFI within ten banking days of the RDFI's subsequent request. The ODFI must provide this information to the RDFI without charge.

Data Passing

The Restore Online Shoppers' Confidence Act prohibits a merchant from initiating an Internet transaction unless the merchant has obtained certain authorization information, including account number and consumer's name and address, directly from the consumer. This law also prohibits a merchant from disclosing a customer's account number and other billing information to another merchant for use in an Internet-based sale.

The Nacha Operating Rules protect customers from such potentially confusing practices. Nacha's rule is similar to those currently in effect in major card brand rules. The rule is broader in scope than the requirements of The Restore Online Shoppers' Confidence Act in that it is not limited to Internet transactions and applies to all Receivers.

The Rules 1) prohibit an ODFI from disclosing a Receiver's account number or routing number to any third party for use in initiating a debit Entry that is not part of the original authorization; and 2) require the ODFI to ensure that the Originator and any Third-Party Service Provider do not disclose such information for use in initiating a debit Entry that is not part of the original authorization.

ACH Data Security Requirements

In addition to the ACH Data Security requirements discussed in Chapter 4, Originators have additional obligations under the Rules regarding the secure storage and destruction of banking information.

The Rules require that Originators of ARC and BOC entries employ commercially reasonable methods to securely store all related source documents until these source documents are destroyed by the Originator. Originators are also obligated to use commercially reasonable methods to securely store all banking information related to ARC and BOC entries. Banking information includes, but is not limited to, an entry, entry data, a routing number, an account number, PINs and other identification symbols, etc. (Note: Where the Receiver's instruction to initiate the entry is communicated via the Internet, data security requirements for secure communication apply regardless of the SEC Code used.)

PROPER USE OF STANDARD ENTRY CLASS CODE

Where entries are authorized in a particular way or through a specific communication channel, the Rules specify the minimum requirements that Originators must follow for each entry initiated in that particular manner and require the use of the appropriate Standard Entry Class Code for such entries. For instance, an Originator that wishes to convert a check received at the point of purchase to an ACH debit during back office processing may only use the BOC Standard Entry Class Code and must comply with the Rules related to such entries. No other Standard Entry Class Code may be used for such purposes. Similarly, an Originator that accepts ACH debit authorizations for Recurring or Single Entries from consumers via the Internet or via a mobile app must identify such entries as WEB debits and comply with appropriate data security standards.

However, where a consumer Receiver's Standing Authorization is involved, the Rules provide a degree of flexibility in an Originator's use of Standard Entry Class Code for Subsequent Entries. Except where noted below, an Originator may identify a Subsequent Entry to a consumer account using the Standard Entry Class Code that is appropriate

to either (i) the manner in which the Receiver's Standing Authorization was communicated to the Originator, or (ii) the manner in which the Receiver's affirmative action to initiate the Subsequent Entry was communicated to the Originator.

Exceptions:

- An Originator must use the POS, MTE, or SHR SEC Code, as appropriate, to identify a Subsequent Entry to a Consumer Account initiated at an "electronic terminal" (as that term is defined in Regulation E), regardless of the manner in which the Originator obtained the Receiver's Standing Authorization. Use of these formats is necessary for an Originator to identify the electronic terminal used at the point of sale (POS) or at an ATM location (MTE), as required by Regulation E.

- An Originator is prohibited from using the PPD SEC Code for a Subsequent Entry if it obtained the Receiver's Standing Authorization (i) as an Oral Authorization via a telephone call, or (ii) via the Internet or a Wireless Network.

SEC Codes for Subsequent Entries - Example #1:

An Originator obtains a Standing Authorization from a consumer Receiver in paper form with a wet signature. The terms of the Standing Authorization specify that the consumer Receiver may affirmatively initiate a Subsequent Entry via an Internet communication to the Originator, or via a telephone call to the Originator. The Originator may choose to identify Subsequent Entries as either PPD, WEB, or TEL.

SEC Codes for Subsequent Entries - Example #2:

An Originator obtains a consumer Receiver's Standing Authorization orally via a telephone call. The terms of the Standing Authorization specify that the consumer Receiver may affirmatively initiate a Subsequent Entries via an Internet communication to the Originator. The Originator may identify Subsequent Entries as either TEL or WEB.

SEC Codes for Subsequent Entries – Example #3

An Originator provides a debit card to a consumer that can be used for a variety of transactions in accordance with the terms of a Standing Authorization obtained from the Receiver in paper form with a wet signature. The Originator must assign the Standard Entry Class Code to each Subsequent Entry debit as follows:

- Each use of the debit card at a point-of-sale terminal must be initiated as a separate POS entry to convey terminal information required for the consumer's statement;

- Each use of the debit card at an ATM must be initiated as an MTE transaction; and

- Each use of the debit card to make purchases on the internet may be initiated using either the PPD or WEB SEC Code.

SEC Codes for Subsequent Entries – Example #4

An Originator provides a debit card to a consumer that can be used for a variety of transactions in accordance with the terms of a Standing Authorization obtained from the Receiver via the Internet. The Originator must assign the Standard Entry Class Code to each Subsequent Entry debit as follows:

- Each use of the debit card at a point-of-sale terminal must be initiated as a separate POS entry to convey terminal information required for the consumer's statement;
- Each use of the debit card at an ATM must be initiated as an MTE transaction; and
- Each use of the debit card to make purchases on the internet must be initiated using the WEB SEC Code.

CORPORATE RECEIVERS

Agreements/Authorizations for Corporate Transactions

As with consumer entries, the business Receiver must authorize all ACH credits and debits to its account. The Originator must ensure that the authorization complies with applicable legal requirements, is readily identifiable as an authorization, and has clear and readily understandable terms. The Originator may obtain the business Receiver's authorization in any manner permitted by applicable legal requirements.

An Originator must enter an agreement with each business Receiver of entries (other than ARC, BOC and POP Entries to non-consumer accounts) under which the Receiver has agreed to be bound by the Nacha Operating Rules. The nature of the agreement for corporate transactions can vary depending upon the complexity of the application and the relationship between the Originator and the Receiver. The Originator that is collecting or disbursing funds to its own subsidiaries, for example, may require an entirely different agreement for the funds transfer than it would if it were entering into a trading partner agreement with another corporation.

Originators of corporate debits to Receivers other than their own subsidiaries need to be aware of the sensitivity of this application. Many corporate Receivers are reluctant to allow debit activity to their accounts; therefore, it is imperative that the agreement that supports this type of activity is complete and accurate. Originators may be required to provide some proof that debit activity was, in fact, authorized if a transaction is questioned by the Receiver.

The ODFI's agreement with its Originator should address the Originator's requirement to provide an accurate record evidencing the Receiver's authorization or the contact information (specified below) to the ODFI upon request. The record or information must be provided in such a manner and time as to enable the ODFI to deliver the information to the requesting RDFI within ten banking days of the RDFI's request.

Upon receipt of an RDFI's written request for evidence of authorization for a CCD, CTX, or Inbound IAT to a non-consumer account, the ODFI must provide either (1) an accurate record evidencing the Receiver's authorization, or (2) the contact information for the Originator that, at a minimum, includes (i) the Originator's name, and (ii) the Originator's phone number or email address for inquiries regarding authorization of entries. This record of authorization or contact information must be provided to the RDFI within ten banking days of receipt of the request without charge.

In lieu of providing proof of authorization to the RDFI, the ODFI may agree to accept a return entry. However, if the RDFI subsequently still requests evidence of authorization of a CCD, CTX or Inbound IAT to a non-consumer account, the ODFI must provide the original, copy, or other accurate record to the RDFI within ten banking days of the RDFI's subsequent request. The ODFI must provide this information to the RDFI without charge.

Authorization for ARC and BOC Entries to Non-Consumer Accounts

With respect to ARC and BOC entries, authorization consists of notice from the Originator to the business Receiver and the receipt of the business' Eligible Source Document. For POP entries, authorization is comprised of both the Receiver's written authorization and notice regarding the check conversion policy provided to the Receiver by the Originator at the point of purchase or manned bill payment location.

Specific information on authorization and notice requirements for ARC, BOC, and POP entries can be found in Chapters 37, 38 and 44, respectively, of these Guidelines.

Authorization for Return Fee Entries to Non-Consumer Accounts

As with other entries, a Return Fee Entry to a non-consumer account must also be authorized by the Receiver. For a Return Fee related to an ARC, BOC or POP Entry, the Originator may obtain the Receiver's authorization by providing the Receiver/check writer with notice that conforms to the requirements of Regulation E at the time that the underlying ACH debit is authorized or the underlying check is accepted. Any notice meeting the form, process, and content permissible under Regulation E satisfies this authorization requirement, even though the account to be debited is a non-Consumer account.

Please see chapter 54 on Return Fees for specific authorization and notice requirements.

Remittance Information/Non-Monetary Entries

The nature of the agreement between the Originator and Receiver will include additional terms if the application includes the processing of payment-related data along with the payment.

Non-Monetary Entries are entries that carry no settlement value but do include payment-related remittance data. Examples of Non-Monetary Entries include CTX and CCD entries that carry remittance information indicating a credit position of the Originator to the Receiver or relating to a period of time during which no funds are owed by the Originator to the Receiver. Originators must ensure that corporate trading partner agreements include provisions for remittance data to be sent via the ACH Network for either live dollar or Non-Monetary Entries.

ORIGINATING ACH ENTRIES

Originators that use the various ACH applications must be sure to comply with the requirements associated with the particular application. Each entry type has specific conditions that must be met in order for the entry to be considered properly authorized. These requirements are discussed in the chapter in these Guidelines dedicated to each SEC Code.

Originating ARC Entries

Prior to originating an ARC Entry, an Originator must:

- Prior to accepting each check, provide the Receiver with a conspicuous notice that has clear and readily understandable terms that meet the minimum authorization requirements;
- Provide a copy of the notice, or language that is substantially similar, to the Receiver at the time of the transaction when the source document for the ARC Entry is provided by the Receiver in-person for payment of a bill at a manned location;
- Obtain an eligible source document (i.e., a check) via the U.S. mail, dropbox, delivery service or in person for payment of a bill at a manned location;
- Use a reading device to capture MICR information;
- Retain a copy of the front of the Eligible Source Document for 2 years, and provide it to the ODFI upon request; and
- Securely store the Eligible Source Document until destroyed.

Originating BOC Entries

Prior to originating a BOC Entry, an Originator must:

- Provide the Receiver with a conspicuous notice that has clear and readily understandable terms that meet the minimum authorization requirements;
- Provide a copy of the notice or substantially similar language to the Receiver at the time of the transaction;
- Obtain an Eligible Source Document at the point of the in-person transaction;
- Verify the identity of the Receiver;
- Use a reading device to capture MICR information;
- Retain a copy of the front of the Eligible Source Document for 2 years, and provide it to the ODFI upon request;
- Securely store the Eligible Source Document until destroyed; and
- Maintain a telephone number for customer inquiries.

Originating CCD Entries

Prior to originating a CCD Entry to a non-consumer account, an Originator must:

- Obtain the corporate Receiver's authorization to originate entries to the Receiver's account that meets the minimum authorization requirements and
- Obtain the corporate Receiver's agreement to be bound by the Nacha Operating Rules.

Originating POP Entries

Prior to originating a POP Entry, an Originator must:

- Provide the Receiver with a conspicuous notice that has clear and readily understandable terms that meet the minimum authorization requirements;
- Obtain an Eligible Source Document at the point of the in-person transaction;
- Use a reading device to capture MICR information;
- Void the Eligible Source Document and return it to the Receiver;
- Obtain a written, signed authorization; and
- Provide a copy of the notice at the time of the transaction.

Originating POS Entries

Prior to originating a POS debit Entry to a consumer account, an Originator must:

- Provide the Receiver with a written authorization that is readily identifiable as an ACH debit authorization and contains clear and readily understandable terms that meet the minimum authorization requirements .
- Obtain the Receiver's agreement to the terms of the authorization via his signature or electronic signature equivalent (i.e., the authorization must be similarly authenticated).
- Provide the Receiver with a disclosure explaining the difference between the ACH card issued by the Originator and a debit card issued by the Receiver's own financial institution.

For sample POS disclosure language, please refer to Appendix M of these Guidelines.

Originating PPD Entries

Prior to originating a PPD debit Entry to a consumer account, an Originator must:

- Provide the Receiver with a written authorization that is readily identifiable as an ACH debit authorization and contains clear and readily understandable terms that meet the minimum authorization requirements.

- Obtain the Receiver's agreement to the terms of the authorization via his signature or electronic signature equivalent (i.e., the authorization must be similarly authenticated).

When originating a PPD Entry for a Return Fee Entry to a consumer account, an Originator must:

• Obtain the Receiver's authorization for a Return Fee Entry originated using the PPD Standard Entry Class Code by either (1) obtaining the Receiver's written authorization, or (2) providing the Receiver with the required notice.

For detailed information on Return Fee Entries and authorization requirements, please refer to Chapter 54 within the Special Topics section of these Guidelines.

When originating a PPD credit Entry to a consumer account, an Originator must:

• Obtain an authorization from the Receiver that is readily identifiable as an authorization and has clear and readily understandable terms. Authorization for a PPD credit entry is not required to be in writing.

Originating RCK Entries

Prior to originating an RCK Entry to a consumer account, an Originator must:

- Agree with its ODFI that any restrictive endorsement made by the Originator or its agent on the item to which the RCK Entry relates is void or ineffective upon initiation of the RCK Entry.

- Provide the Receiver with a conspicuous notice that has clear and readily understandable terms that meet the minimum authorization requirements.

- Use an eligible item.

- Retain a copy of the front and back of the eligible item for 7 years, and provide it to the ODFI upon request. If the item has been paid, the copy provided to the ODFI must be so marked.

- Not reinitiate an RCK entry more than one time within 180 days of the Settlement Date of the original entry, provided that the item to which the RCK relates has been presented no more than one time through the check collection system, and one time as an RCK entry.

Originating TEL Entries

Prior to originating a TEL Entry to a consumer account, an Originator must:

- Obtain oral authorization from the Receiver via the telephone. The authorization must be readily identifiable as an authorization and must have clear and readily understandable terms that meet the minimum authorization requirements .

- Provide the Receiver with a telephone number for inquiries that is answered during normal business hours.

- Verify the identity of the Receiver.

- Verify that the routing number is valid.

Originating WEB Entries

Prior to originating a debit WEB/Mobile Entry to a consumer account, an Originator must:

- Obtain written authorization from the Receiver that meet the minimum authorization requirements (1) via the Internet or a wireless network, except for an oral authorization via a telephone call ; or (2) in any manner permissible under the Rules, if the Receiver's instruction for the initiation of the debit entry is designed by the Originator to be communicated, other than orally via a telephone call , via a wireless network.

- Use a fraudulent transaction detection system to screen each debit WEB entry that, at a minimum, validates the account to be debited for the first use of the account number, and for any subsequent change to the account number.

- Verify the Receiver's identity.

- Verify that the routing number is valid.

- Conduct annually an audit of data security practices for Receivers' financial information.

CHAPTER 26

Initiation of Return Entries by RDFI

TIMING OF RETURNS

In general, return entries must be received by the RDFI's ACH Operator by its deposit deadline for the return entry to be made available to the ODFI no later than the opening of business on the second banking day following the Settlement Date of the original entry. For RCK entries, the RDFI must transmit the return entry to its ACH Operator by midnight of the second banking day following the banking day of receipt of the presentment notice. Common exceptions to these general timing requirements are described below.

For credit entries that are refused by the Receiver, the credit return must be made available to the ODFI by opening of business on the second banking day following the RDFI's notification from the Receiver that it has refused the entry.

For credit entries subject to Article 4A of the Uniform Commercial Code, the RDFI must transmit the return entry to its ACH Operator prior to the time the RDFI accepts the credit entry as provided in Article 4A, subject to certain exceptions.

For a CCD or CTX entry with respect to which the RDFI has received written notification from a a Receiver that the debit was not authorized, the RDFI may transmit a return entry to the ODFI if the ODFI agrees, either orally or in writing, to accept the late return.

If a return entry is being initiated for R05, R07, R10, R11, R33, R37, R38, R51, R52, R53, the RDFI must transmit the extended return entry so that it is made available to the ODFI no later than the opening of business on the banking day following the sixtieth calendar day following the Settlement Date of the original entry.

RDFIs need to be aware of return processing schedules offered by their ACH Operator in order to meet these requirements. All RDFIs should also be aware that ACH Operators offer return processing schedules that will allow return entries to be processed and settled quickly. For example, an RDFI could initiate a return the same day as the settlement of the original entry and receive settlement for the return on that day.

REQUEST FOR COPY OF AUTHORIZATION; ODFI AGREEMENT TO ACCEPT RETURN ENTRY IN LIEU OF PROVIDING COPY OF AUTHORIZATION

An RDFI that requires a copy of the Receiver's authorization must send a written request for such a copy to the ODFI. Upon receipt of the RDFI's written request, the ODFI must provide the RDFI with the original, copy, or other accurate record of the Receiver's authorization within ten banking days. However, to reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, ODFIs and Originators may agree to accept the return of the debit rather than provide the authorization to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI.

Even when the ODFI has accepted the return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization. In these situations, the RDFI will need to submit a subsequent request to the ODFI for evidence of the Receiver's authorization. The ODFI then must provide the original, copy or other accurate record of the authorization to the RDFI within ten banking days of the RDFI's subsequent request. Because RDFIs may receive different responses to their requests for copies of authorization, RDFIs may wish to review their practices and procedures to ensure that they are prepared to send subsequent requests for proof of authorization in cases where a copy is still needed if ODFI has agreed to accept the return in lieu of providing the authorization.

WRITTEN STATEMENTS OF UNAUTHORIZED DEBIT

An RDFI should establish internal procedures to obtain a signed or similarly authenticated Written Statement of Unauthorized Debit when necessary. If the similarly authenticated requirements are satisfied, an account holder does not need to sign the Written Statement of Unauthorized Debit in person at the financial institution. By initiating the extended return entry for the transaction in question, the RDFI warrants that, when required, it has obtained a Written Statement of Unauthorized Debit from the Receiver that complies with the requirements of the Rules, including that it is dated on or after the Settlement Date of the original entry. The RDFI indemnifies each ODFI, ACH Operator and Gateway against any and all claims, demands, losses, liabilities, or expenses resulting from the breach of this warranty. An RDFI may refer to the specific definition of what constitutes an unauthorized entry in its evaluation of a consumer's claim that an entry was not authorized.

RDFIs should be aware, when recrediting their consumers for unauthorized or improper debit entries, that the requirement to obtain a Written Statement of Unauthorized Debit is the minimum requirement under the Nacha Operating Rules. At its discretion, an RDFI may choose to obtain an affidavit from its account holder. When making the decision to use a Written Statement of Unauthorized Debit or an affidavit, it is important for RDFIs to note that some state laws require that all affidavits be notarized. With respect to a Written Statement of Unauthorized Debit, other states preclude a person from being charged with perjury unless he or she has taken an oath before an authorized public official, which, in most cases is a notary. An RDFI may wish to consult its legal counsel to determine which document is most appropriate for its use.

The Rules explicitly state that an RDFI may obtain a consumer's Written Statement of Unauthorized Debit as an Electronic Record, and an RDFI may accept a consumer's Electronic Signature, regardless of its form or the method used to obtain it. WSUDs may be obtained and signed electronically, which could include the same methods permissible for obtaining a consumer debit authorization, such as orally via a telephone call or via a writing over the internet.

Appendix I of these Guidelines contains a sample Written Statement of Unauthorized Debit.

CHAPTER 37

Accounts Receivable Entries (ARC)

OBLIGATIONS OF ORIGINATORS

Retention/Secure Storage of Source Documents and Payment Information

Each Originator of ARC entries must retain a reproducible image or other copy of the front of the Receiver's source document for a period of two years from the Settlement Date of the entry. Originators may also choose, at their discretion, to retain a copy of the back of the Receiver's source document. The Originator must be prepared to provide such a copy to the ODFI, as the ODFI is required to send a copy of the front of the source document to the RDFI within 10 banking days of receipt of the RDFI's written request, provided that the RDFI's request is received within two years of the Settlement Date of the entry.

To reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, Originators and their ODFIs may agree to accept the return of the debit rather than provide a copy of the authorization (notice plus a copy of the front of the source document) to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI. Even when the ODFI has accepted a return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization for an ARC entry. In these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the Originator must provide the original, copy or other accurate record of the authorization (the notice and a copy of the front of the source document) to its ODFI for provision to the RDFI within ten banking days of the RDFI's subsequent request. Originators and ODFIs that choose to take advantage of this alternative to providing proof of authorization should consider whether any changes or modifications to their business processes may be necessary.

The Rules do not explicitly require an Originator to destroy the source document to which the ARC entry relates. Although an Originator may use its discretion in determining how long to retain the original source document, Originators are encouraged to establish policies and procedures to destroy ARC source documents as soon as is reasonable to protect against the risk of fraud or erroneous entry of the check into the check processing system. Until such time that the source document is destroyed by the Originator, it must be securely stored using commercially reasonable methods.

The Rules do require Originators to use commercially reasonable methods to securely store all banking information related to the ARC transaction. Banking information includes, but is not limited to, an entry, entry data, a routing number, an account number, PINs and other identification symbols, etc.

RESPONSIBILITIES OF ODFIS

Retention/Secure Storage of Source Documents and Payment Information

The ODFI is required to provide the RDFI with a copy of the front of the Receiver's source document, along with the required notice, to the RDFI, within 10 banking days of receipt of a written request by the RDFI, provided that the RDFI's request is received within two years of the Settlement Date of the entry. ODFIs should establish procedures with their Originators to obtain necessary copies of ARC source documents.

To reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, ODFIs and their Originators may agree to accept the return of the debit rather than provide a copy of the authorization (notice plus a copy of the front of source document) to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI. Even when the ODFI has accepted a return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization for an ARC entry. In

these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the ODFI must provide the original, copy or other accurate record of the authorization (the notice and a copy of the front of the source document) to the RDFI within ten banking days of the RDFI's subsequent request. ODFIs that choose to take advantage of this alternative to providing proof of authorization should consider whether any changes or modifications their business processes may be necessary.

The ODFI warrants that its customer (the Originator) has employed commercially reasonable methods to securely store (1) all source documents until destruction, and (2) all banking information related to ARC Entries. ODFIs should work closely with their Originators to ensure that these secure storage and destruction obligations are met. Although the Rules do not explicitly require an Originator of ARC entries to destroy the source document to which the ARC entry relates, it is recommended that the Originator destroy ARC source documents as soon as is reasonable to protect against the risk of fraud or erroneous entry of the check into the check processing system. Until destroyed, however, Originators must use commercially reasonable methods to securely store such source documents, as well as any banking information related to an ARC entry. Refer to the Obligations of Originator section of this ARC chapter for guidance on secure storage and destruction of such information.

RESPONSIBILITIES OF RDFIS

Copy of Source Document

RDFIs may send the ODFI a written request to provide a copy of the front of the Receiver's source document for an ARC entry, provided such request is made within two years of the settlement date of the ARC entry. The ODFI must provide the copy of the source document and required notice to the RDFI within ten banking days of receipt of the RDFI's written request unless it agrees to accept the return of the entry in lieu of providing the copies. When the ODFI has accepted a return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization. In these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the ODFI must provide the original, copy or other accurate record of the authorization (the notice and a copy of the front of the source document) to the RDFI within ten banking days of the RDFI's subsequent request. RDFIs should expect to receive varying responses from ODFIs to their requests for proof of authorization and will need to develop practices and procedures to send subsequent requests for proofs of authorization in cases where a copy is still needed when the ODFI has agreed to accept the return in lieu of providing the copy.

RDFIs should be aware that the Originator is only required to retain a reproducible image or other copy of the front of the Receiver's source document for a period of two years from the Settlement Date of the entry; a copy of the back of the source document is not required. The Originator may, however, choose to retain a copy of the back of the Receiver's source document at its discretion.

CHAPTER 38

Back Office Conversion Entries (BOC)

OBLIGATIONS OF ORIGINATORS

Retention/Secure Storage of Source Documents and Payment Information

Each Originator of BOC entries is required to retain a reproducible, legible image or other copy of the front of the Receiver's source document for a period of two years from the Settlement Date of the entry. Originators may also choose, at their discretion, to retain a copy of the back of the Receiver's source document. The Originator must be prepared to provide such a copy to the ODFI, as the ODFI is required to send a copy of the front of the source document to the RDFI within 10 banking days of receipt of a written request for such copy by the RDFI, provided that the RDFI's written request is received by the ODFI within two years of the settlement date of the BOC entry.

To reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, Originators and their ODFIs may agree to accept the return of the debit rather than provide a copy of the authorization (notice plus a copy of the front of the source document) to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI. Even when the ODFI has accepted a return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization for a BOC entry. In these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the Originator must provide the original, copy or other accurate record of the authorization (the notice and a copy of the front of the source document) to its ODFI for provision to the RDFI within ten banking days of the RDFI's subsequent request. Originators and ODFIs that choose to take advantage of this alternative to providing proof of authorization should consider whether any changes or modifications to their business processes may be necessary.

The Rules do not explicitly require an Originator to destroy the source document to which the BOC entry relates. Although an Originator may use its discretion in determining how long to retain the original source document, Originators are encouraged to establish policies and procedures to destroy BOC source documents as soon as is reasonable to protect against the risk of fraud or erroneous entry of the check into the check processing system. Until such time that the source document is destroyed by the Originator, it must be securely stored using commercially reasonable methods.

The Rules also require Originators to use commercially reasonable methods to securely store all banking information related to the BOC transaction. Banking information includes, but is not limited to, an entry, entry data, a routing number, an account number, PINs and other identification symbols, etc.

Secure storage requirements may also be governed by state or Federal laws and regulations. Originators should be familiar with any such laws when determining the commercial reasonableness of their storage methods.

When choosing a commercially reasonable method for secure data storage, Originators should consider the following guidance provided by the Federal Trade Commission for complying with the Safeguards Rule, which implements security measures within the Gramm-Leach-Bliley Act.

- know where sensitive information is stored and that it is stored securely;
- ensure that only authorized personnel have access to sensitive data;
- ensure that storage areas are protected against destruction or damage from physical hazards such as fire or floods;
- store records in a room or cabinet that is locked when unattended;
- when information is stored on a server or other computer, ensure that the computer is accessible only with a strong password and that it is kept in a physically secure area;
- avoid storing sensitive information on an electronic device with an Internet connection;
- maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area;
- maintain a careful and accurate inventory of the company's electronic devices and of the storage location of any other sensitive information.

When destroying BOC source documents or other banking information, Originators should establish reasonable measures for destroying such information that may include:

- burning, pulverizing, or shredding papers that contain such information so that the information cannot be read or reconstructed;

- the use of an outside disposal company that has been certified by a recognized industry group;

- the destruction and/or erasure of data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, smartphones, cell phones, or any other electronic media or hardware containing banking information.

RESPONSIBILITIES OF ODFIS

Retention/Secure Storage of Source Documents and Payment Information

The ODFI is required to provide the RDFI with a copy of the front of the Receiver's source document within 10 banking days of receipt of a written request by the RDFI, provided that the RDFI's request is received within two years of the Settlement Date of the entry. ODFIs should establish procedures with their Originators to obtain necessary copies of BOC source documents.

The ODFI warrants that its customer (the Originator) has employed commercially reasonable methods to securely store (1) all source documents until destruction, and (2) all banking information related to BOC Entries. ODFIs should work closely with their Originators to ensure that these secure storage and destruction obligations are met. Although the Rules do not explicitly require an Originator of BOC entries to destroy the source document to which the BOC entry relates, it is recommended that the Originator destroy BOC source documents as soon as is reasonable to protect against the risk of fraud or erroneous entry of the check into the check processing system. Until destroyed, however, Originators must use commercially reasonable methods to securely store such source documents, as well as any banking information related to a BOC entry. Refer to the Obligations of Originator section of this BOC chapter for guidance on secure storage and destruction of such information.

To reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, Originators and their ODFIs may agree to accept the return of the debit rather than provide a copy of the authorization (notice plus a copy of the front of the source document) to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI. Even when the ODFI has accepted a return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization for a BOC entry. In these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the Originator must provide the original, copy or other accurate record of the authorization (the notice and a copy of the front of the source document) to its ODFI for provision to the RDFI within ten banking days of the RDFI's subsequent request. Originators and ODFIs that choose to take advantage of this alternative to providing proof of authorization should consider whether any changes or modifications to their business processes may be necessary.

For a discussion on the concept of commercial reasonable standards, please refer to the chapter on General Rules within the General Information section of these Guidelines.

RESPONSIBILITIES OF RDFIS

Copy of Source Document

RDFIs may send the ODFI a written request to provide a copy of the front of the Receiver's source document for a BOC entry, provided such request is made within two years of the settlement date of the BOC entry. The ODFI must provide the copy to the RDFI within ten banking days of receipt of the RDFI's written request unless it agrees to accept the return of the entry in lieu of providing the copies. When the ODFI has accepted a return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization. In these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the ODFI must provide the original, copy or other accurate record of the authorization to the RDFI within

ten banking days of the RDFI's subsequent request. RDFIs should expect to receive varying responses from ODFIs to their requests for proof of authorization and will need to develop practices and procedures to send subsequent requests for proofs of authorization in cases where a copy is still needed when the ODFI has agreed to accept the return in lieu of providing the copy.

RDFIs should be aware that the Originator is only required to retain a reproducible image or other copy of the front of the Receiver's source document for a period of two years from the Settlement Date of the entry; a copy of the back of the source document is not required. The Originator may, however, choose to retain a copy of the back of the Receiver's source document at its discretion.

CHAPTER 39

Corporate Credit or Debit and Corporate Trade Exchange Entries (CCD & CTX)

OBLIGATIONS OF ORIGINATORS

Agreement with Receiver

With business-to-business payments, ACH transactions originated by a buyer are credit transactions because the buyer (the party that owes funds) "pushes" funds to the seller's (party that is owed the payment) account. ACH transactions originated by a seller are debit transactions because the seller "pulls" funds from the buyer's account.

As with all ACH transactions, the Originator of a CCD or CTX entry must receive the Receiver's authorization to debit or credit the Receiver's account. The Nacha Operating Rules do not require the CCD/CTX authorization to be in a specific form, however, the authorization must be readily recognizable as an authorization and have clear and readily understandable terms. In addition, the Rules require the Originator and Receiver to have an agreement that binds the Receiver to the Rules. This trading partner agreement should contain the authorization requirements and procedures as determined by the parties; the companies negotiate the terms.

In some instances a seller may have specialized data remittance requirements for an electronic credit payment (e.g., specific data elements and formats) and/or may require that remittance be sent through a specific channel (e.g., the ACH, or a private remittance network — sometimes referred to as a value-added network). If the buyer is unable to meet the exact specifications for making a credit ACH payment, it is possible that the seller will not be able to post the payment correctly, meaning the buyer's account will not be properly credited. The seller may, therefore, only allow the buyer to originate a credit ACH payment once the buyer agrees to the remittance requirements. As above, the terms of the agreement would be dictated by the trading partner agreement.

Sellers and buyers should discuss special payment requirements prior to conducting business. The range of payment terms and conditions should be covered in their trading partner agreement.

The agreement should also specify the manner in which dispute resolution will be handled.

Provision of the Record of Authorization for a CCD or CTX Entry

Upon receipt by the ODFI of an RDFI's written request for evidence of authorization for a CCD or CTX entry, the ODFI must provide either (1) an accurate record evidencing the Receiver's authorization, or (2) the contact information for the Originator that, at a minimum, includes (i) the Originator's name, and (ii) the Originator's phone number or email address for inquiries regarding authorization of entries. This record of authorization or contact information must be provided to the RDFI within ten banking days of receipt of the request without charge.

The Originator must be able to provide an accurate record evidencing the Receiver's authorization or the contact information as stated above to the ODFI upon request. The record or information must be provided in such a manner and time as to enable the ODFI to deliver the information to the requesting RDFI within ten banking days of the RDFI's request.

To reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, Originators and their ODFIs may agree to accept the return of the debit rather than provide a copy of the authorization to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI. Even when the ODFI has accepted a return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization. In these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the Originator must provide the original, copy or other accurate record of the authorization to its ODFI for provision to the RDFI within ten banking days of the RDFI's subsequent request. Originators and ODFIs that choose to take advantage of this alternative to providing proof of authorization should consider whether any changes or modifications to their business processes may be necessary.

CHAPTER 44

Point of Purchase Entries (POP)

OBLIGATIONS OF ORIGINATORS

Authorization/Notification Requirements

Originators are required to provide notice to the Receiver and to obtain a written authorization from the Receiver to satisfy the authorization requirement for a POP entry. (For specific details on the minimum requirements for written authorization, please refer to Chapter 16 – Relationship with Receiver and Authorization Requirements – within these Guidelines.) The provision of the notice by the Originator to the Receiver, the receipt of the source document and the written authorization from the Receiver together constitute authorization for the POP entry. The check is used solely as a source document for capturing the Receiver's routing number, account number, and check serial number for the entry. The rules governing POP incorporate Regulation E safe harbor language into the required notice, requiring that the notice include the following, or substantially similar, language:

"When you provide a check as payment, you authorize us either to use information from your check to make a one-time electronic fund transfer from your account or to process the payment as a check transaction."

The Originator must post the notice in a prominent and conspicuous location and a copy of such notice, or similar language, must be provided to the Receiver at the time of the transaction.

At the Originator's discretion, the receipt and the authorization required for POP Entries may be provided to the Receiver on the same document or on different documents.

NOTE: Originators should be aware that some Receivers may choose to opt out of check conversion activity by declining to sign a written authorization at the point of purchase. In other cases, Receivers may have chosen to opt out of check conversion activity by having their checks reprinted to include an Auxiliary On-Us Field in the MICR line. In both of these situations, Originators may not convert the check to a POP entry and are encouraged to work with these customers to establish alternative payment methods.

Retention and Provision of Copy of Authorization

Each Originator of POP entries must retain the original or a copy of the Receiver's authorization for a minimum of two years following the settlement date of the entry. At the request of its ODFI, the Originator must provide the original or copy to the ODFI for its use, or for the use of an RDFI requesting the information, in such time and manner so that the ODFI is able to deliver the authorization to the requesting RDFI within ten banking days of the RDFI's request.

To reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, Originators and their ODFIs may agree to accept the return of the debit rather than provide a copy of the authorization to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI. Even when the Originator and its ODFI have accepted a return or have agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization for a POP entry. In these situations, the RDFI must submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the Originator must provide the original, copy or other accurate record of the authorization to its ODFI for provision to the RDFI within ten banking days of the RDFI's subsequent request. Originators and ODFIs that choose to take advantage of this alternative to providing proof of authorization should consider whether any changes or modifications to their business processes may be necessary.

CHAPTER 45

Prearranged Payment and Deposit Entries (PPD)

OBLIGATIONS OF ORIGINATORS

Authorization Requirements

As with any ACH transaction, the Originator must obtain the Receiver's authorization to initiate PPD entries through the ACH Network to the Receiver's account. For PPD debit entries, the authorization must

1. be in writing;
2. be readily identifiable as an ACH authorization;
3. have clear and readily understandable terms;
4. meet the minimum authorization requirements as discussed in Chapter 16 of these Guidelines; and
5. be either signed or similarly authenticated by the consumer. (Refer to the discussion below on the use of the similarly authenticated standard with PPD entries.)

The Originator must provide the Receiver a copy of the authorization for all debit entries.

For credit entries to a consumer account, the authorization may be obtained in writing, or it may be obtained orally or by other non-written means.

The Rules do not require the consumer's authorization to initiate reversing entries to correct erroneous transactions. However, Originators should consider obtaining express authorization of credits or debits to correct errors.

An Originator must retain the original or a reproducible copy of the Receiver's authorization for two years from the termination or revocation of the authorization and must be able to provide the ODFI with an accurate copy within the time period required by the ODFI.

To reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested, Originators and their ODFIs may agree to accept the return of the debit rather than provide a copy of the authorization to the RDFI. In these cases, the ODFI must provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI. Even when the ODFI has accepted a return or has agreed to accept the return of the entry, it is still possible that the RDFI may require a copy of the Receiver's authorization. In these situations, the RDFI will need to submit a subsequent request for evidence of the Receiver's authorization to the ODFI, and the Originator must provide the original, copy or other accurate record of the authorization to its ODFI for provision to the RDFI within ten banking days of the RDFI's subsequent request. Originators and ODFIs that choose to take advantage of this alternative to providing proof of authorization should consider whether any changes or modifications to their business processes may be necessary.

CHAPTER 47

Telephone-Initiated Entries (TEL)

Telephone-Initiated Entries (TEL) are consumer debit transactions. The Nacha Operating Rules permit TEL entries when the Originator obtains the Receiver's authorization for the debit entry orally via the telephone. An entry based upon a Receiver's oral authorization provided during a telephone call must utilize the TEL (Telephone-Initiated Entry) Standard Entry Class (SEC) Code.

INITIATING A TEL ENTRY — AN OVERVIEW

A TEL Entry is initiated by an Originator in response to a Receiver's oral authorization that is spoken over the telephone and includes certain elements of the Receiver's banking information as specified in the Rules. Based on the Receiver's oral authorization, an ACH debit is initiated to the Receiver's account to collect payment for goods or services. TEL Entries may be used for debit transactions only. Originators may not utilize the TEL SEC Code to transmit credit entries to the Receiver's account, unless those entries are credits to reverse erroneous debits.

Existing Relationship

A TEL Entry may be transmitted only in circumstances in which:

1. there is an existing relationship between the Originator and the Receiver, or

2. there is not an existing relationship between the Originator and the Receiver, but the Receiver initiated the telephone call to the Originator.

The Originator and the Receiver are considered to have an existing relationship when either:

1. there is a written agreement in place between the Originator and the Receiver for the provision of goods or services (e.g., the Receiver has an insurance policy with the Originator), or

2. the Receiver has purchased goods or services from the Originator within the past two years.

No Relationship

A TEL Entry may not be used by an Originator when there is no existing relationship between the Originator and the Receiver, and the Originator has initiated the telephone call. For purposes of the Rules, an Originator is not deemed to have such an existing relationship with the Receiver with respect to TEL entries on the basis of a pre-existing relationship of one of its affiliates.

Oral Authorization

An oral authorization is one that is spoken by the Receiver. The Receiver's oral authorization for a TEL entry may be provided during a conversation with the Originator, or the Receiver's spoken authorization may be captured through the use of voice-related technologies, such as an automated voice response system.

- Response Unit (VRU): A Voice Response Unit is also commonly referred to as Interactive Voice Response Unit or IVR, which is interactive technology that allows a computer to detect voice and keypad inputs.

RISK MANAGEMENT

The Nacha Operating Rules require Originators to implement specific risk management procedures relating to TEL entries.

Verification of Identity of Receiver

Originators of TEL entries are required to establish and implement commercially reasonable procedures to verify the identity of the Receiver (e.g. name, address, and telephone number). Originators need to establish a commercially reasonable method (e.g., use of a directory, database, etc.) to comply with this requirement. The Originator is also advised to further verify the Receiver's identity by verifying pertinent information with the Receiver (e.g., past buying history, mother's maiden name, Caller ID information, shared secrets, account passwords, challenge responses, credit bureau information, etc.)

Verification of Routing Numbers

Originators of TEL entries are required to establish commercially reasonable procedures to verify that routing numbers are valid. A TEL entry is a debit entry in which the Receiver is responsible for providing his routing number. In most instances, the Receiver provides the routing number by reading it from a source document (e.g., the Receiver's check) or mobile banking application, which increases the potential for Receiver error in providing accurate information.

In some instances, the MICR information on the Receiver's check may not be appropriate for ACH processing resulting in increased exception processing. Originators can minimize the potential for exception processing by employing commercially reasonable procedures to verify that routing numbers are valid.

Verifying the validity of routing numbers can be accomplished by:

- a component of a fraudulent transaction detection system,
- through a separate database or directory (either commercial or proprietary), or
- through other methods devised by the Originator, for example manual intervention such as calling the Receiver's financial institution .

Although TEL entries provide a streamlined method for Receivers to authorize ACH debit entries, this process may be subject to misuse through the origination of unauthorized ACH debit transactions. TEL entries are susceptible to origination that is the result of deceptive and fraudulent telemarketing practices by Originators that use fraudulent intent to:

- Debit the Receiver without obtaining the Receiver's authorization for such a transaction;
- Cold call consumers with whom they have no existing relationship and subsequently debit the Receiver; and/or
- Use mail solicitations to instruct the consumer to initiate the telephone call to the Originator and subsequently attempt to sell goods or services using deceptive marketing practices.

Commercially Reasonable

For discussion on the concept of commercially reasonable standards, please refer to Chapter 4 of these Guidelines.

OBLIGATIONS OF ORIGINATORS

Agreements with ODFIs

Originators that wish to use the ACH Network to transmit TEL entries should consider modifications to their agreements with their ODFIs to address the origination of this type of transaction. At a minimum, additions to the ODFI/Originator agreement should include, but not be limited to:

- the Originator's responsibilities and obligations with respect to the provision of specific information to the Receiver during the telephone call;
- the Originator's requirement to audio record the oral authorization or provide written confirmation of the Receiver's authorization for Single-Entry TEL entries;
- the Originator's requirement to audio record the Receiver's oral standing authorization or provide written confirmation of the Receiver's oral standing authorization prior to the settlement date of the first subsequent entry.
- the Originator's requirement to comply with Regulation E with respect to recurring TEL entries, including its requirement to audio record the oral authorization and provide a written copy of the Receiver's authorization;
- verification of the identity of the Receiver; and
- verification of routing numbers.

The agreement should also address the allocation of liability between the Originator and ODFI for any failure on the part of the Originator to comply with these and other requirements of the Nacha Operating Rules.

Authorization Requirements

Originators of TEL entries must obtain the Receiver's explicit oral authorization prior to initiating a debit entry to a consumer's account. The authorization must meet minimum authorization requirements for a consumer debit entry(ies) and evidence the Receiver's identity and the Receiver's assent to the authorization. As part of the oral authorization process for TEL single entries, recurring TEL entries, and for a Receiver's standing authorization obtained orally via a telephone call, the Originator must clearly state during the telephone conversation that the consumer is authorizing one ore more ACH debit entries to his account. The Originator must ensure that the Receiver explicitly express consent. Silence is not express consent.

For more information on the minimum authorization requirements for consumer debit entries, see Chapter 16 of these Guidelines.

Single Entry TEL Entries

Originators of SingleEntry TEL entries are obligated either to audio record the Receiver's oral authorization or to provide, prior to the settlement of the entry, written notice to the Receiver that confirms the oral authorization. When the Originator of a Single Entry TEL entry elects to provide the Receiver with written notice confirming the Receiver's oral authorization, that notice must include the minimum authorization requirements for a consumer debit entry. The Originator should disclose to the Receiver the method by which written notice will be provided if this option is used by the Originator.

Standing TEL Authorizations and Subsequent Entries

Originators that obtain standing TEL authorizations must either audio record the Receiver's oral authorization or provide, prior to the settlement of the first subsequent entry, written notice to the Receiver that confirms the oral authorization. When the Originator that obtains a standing TEL authorization elects to provide the Receiver with written notice confirming the Receiver's oral authorization, that notice must include the minimum authorization requirements for all consumer debit entries. The Originator should disclose to the Receiver the method by which written notice will be provided if this option is used by the Originator.

When initiating a subsequent entry, the Originator must retain proof that the Receiver affirmatively initiated each payment in accordance with the terms of the standing authorization. The Originator must retain this proof for two years following the Settlement Date of the subsequent entry.

For more information on standing authorizations and subsequent entries, see Chapter 16 of these Guidelines.

Recurring TEL Entries

Originators of recurring TEL entries are obligated to both audio record the Receiver's oral authorization and to provide a written copy of the authorization to the Receiver, to the extent required by Regulation E. The Originator should disclose to the Receiver the method by which the written copy will be provided. The authorization must meet the minimum authorization requirements for consumer debit entries and include a telephone number that is available to the Receiver and answered during normal business hours for customer inquiries.

Authorizations for recurring TEL Entries need to meet the writing and signature requirements of Regulation E for preauthorized transfers, which can be done by conforming to the e-Sign Act. However, neither Regulation E nor its Commentary provides additional guidance as to how ODFIs and Originators can comply with e-Sign. Although Nacha cannot formally interpret Regulation E, the guidance below provides additional information on how to comply with the Rules for authorization of recurring TEL entries. This guidance is not intended to be legal advice regarding compliance with Regulation E. ODFIs and Originators using recurring TEL entries are responsible for determining their own compliance with Regulation E and the e-Sign Act.

Authorization of Recurring TEL Entries under Regulation E and e-Sign Act

Under the Rules, an ODFI is responsible for the compliance of the telephone authorization process with applicable law and for the validity of any authorization obtained using such a process. To facilitate ACH participants' understanding of such processes, the following provides high-level outlines of two distinct situations that Originators and ODFIs might face when considering whether to permit consumers to authorize recurring ACH debits from their accounts via the telephone. The first scenario is based on the Rules as they existed prior the effective date of the recurring TEL rule (September 16, 2011), and results in "telephone-initiated PPD transactions" in which a written authorization is electronically signed. This remains a permissible transaction format for institutions that follow the process outlined below. The second scenario is based on the current rule for recurring TEL payments with an oral authorization. These are merely two examples; there are many other variations of the scenarios below that Originators and ODFIs may wish to consider.

Scenario 1 – Telephone-Initiated PPD Entries by Electronically Signed Authorization

The consumer has received the clear and readily understandable terms of the preauthorized transfer in writing (either in a physical writing or in an electronic manner that satisfies the e-Sign Act or other applicable law) prior to the telephone call. The writing includes spaces for the consumer to record any variable information (e.g., transaction amount, transaction frequency, account number and/or routing number). The consumer then initiates a telephone call to the Originator, during which the consumer authorizes a recurring debit to his or her consumer account, and "signs" the written authorization either by inputting a code into the telephone keypad or by providing the code orally to a customer service representative on a recorded line. This scenario could apply to an existing billing relationship, in

which the billing company regularly sends bills in writing (either paper or electronic) to an existing customer. The bill would contain the clear and readily understandable terms of the preauthorized transfers, and a code for the customer to input during the telephone call.

Scenario 2 – Recurring TEL Entries by Oral Authorization

The consumer has not received the terms of the preauthorized transfer in writing (either in a physical writing or in an electronic manner that satisfies the e-Sign Act or other applicable law) prior to the telephone call. The consumer initiates a telephone call to the Originator, during which the consumer authorizes a recurring debit to his or her consumer account. The consumer provides his or her authorization, including his or her "signature" or "authentication" of the authorization, via a recorded conversation. The consumer either repeats or expressly confirms the authorization, including the account to be debited, the timing of the debits (e.g., monthly on the 1st business day of the month), and the amount (e.g., $500 per month), as well as other required elements of the authorization. The Originator provides a written copy of the authorization to the consumer (either in a physical writing or in an electronic manner that satisfies e-Sign Act or other applicable law). This scenario could apply to both: 1) an existing billing relationship in which terms of the preauthorized transfer are not contained in writing on a bill; and 2) a new billing relationship in which a new customer wants to authorize recurring payments during the same telephone call that establishes a new service (e.g., a new car insurance policy), provided that the authorization is the result of an inbound customer call.

Other Considerations for TEL Entry Authorizations

Originators should understand that the term "provide" is intended to mean that the Originator has utilized a medium (e.g., U.S. mail, fax, or other mail delivery method) to send the written notice to the Receiver. Any written notice or disclosure required by the Nacha Operating Rules, including those for TEL entries, may be provided in electronic form (e.g., e-mail and SMS text message to a smartphone or mobile device). However, state and federal laws may require Receiver consent before using electronic notices/disclosures.

The term "provide" does not imply receipt of such notice by the Receiver. Originators that send a copy of the written authorization or use a written notice to confirm the authorization must afford the Receiver the right to contact the Originator to correct any erroneous information contained within the notice using a provided telephone number. Compliance with the Nacha Operating Rules does not eliminate the obligation to comply with other applicable laws, such as the e-Sign Act.

An Originator using a voice response unit (VRU) to capture a Receiver's authorization for a TEL entry must understand that key-entry responses by the Receiver to input data and to respond to questions does not qualify as an oral authorization. A VRU may be used by the Receiver to key enter data and to respond to questions, provided that the actual authorization by the Receiver is provided orally.

Retention of Record of Authorization for TEL Entries

For Single Entry TEL entries, the Originator must retain either the original or a duplicate audio recording of the Receiver's oral authorization or the original or a copy of the written notice confirming the Receiver's oral authorization for two years from the date of the authorization. With respect to Standing Authorizations, the Originator must retain the original or duplicate audio recording of the standing oral authorization for two years from the termination or revocation of the standing oral authorization, as well as proof that the Receiver affirmatively initiated each payment in accordance with the terms of the standing authorization for two years following the settlement date of the entry. For recurring TEL entries, an Originator must retain for two years from the termination or revocation of the authorization (i) the original or a copy of the oral authorization, and (ii) evidence that a copy of the authorization was provided to the Receiver in compliance with Regulation E. At the request of the ODFI, the Originator must provide a copy of the Receiver's authorization.

Formatting Requirements

The Payment Type Code field in the Entry Detail Record may be used to indicate whether a TEL entry is a recurring entry, a single entry, or a subsequent entry initiated as part of a standing authorization. At their discretion, Originators

may identify a recurring entry, single entry, or subsequent entry through the use of an optional indicator of "R," "S," or "ST," respectively, Originators may also use this field to include other codes, of significance to them, to enable specialized handling of an entry.

The Individual Name Field of the Entry Detail Record of a TEL entry is a mandatory field. Originators must ensure that the name of the Receiver is included within each TEL entry. Any TEL entry where the Individual Name Field contains all spaces or all zeros will be rejected and returned by the ACH Operator.

NOTE: The inclusion of all spaces or all zeros in any other mandatory filed will also cause the entry to be returned by the ACH Operator.

OBLIGATIONS OF ODFIS

Return of TEL Entries

Return by ACH Operator

The Individual Name Field within the TEL Entry Detail Record is a mandatory field and any TEL entry in which the Individual Name Field contains all spaces or all zeros will be rejected and returned by the ACH Operator. The inclusion of all spaces or all zeros in any other mandatory field will also cause the entry to be returned by the ACH Operator.

Return by RDFI

TEL entries may be returned by the RDFI for any valid reason. RDFIs are subject to the typical return time frames for transmitting TEL entry returns. Specifically, an RDFI must transmit a returned TEL entry to its ACH Operator by the ACH Operator's deposit deadline for the return entry to be made available to the ODFI no later than the opening of business on the second banking day following the Settlement Date of the TEL entry.

In the event that a Receiver claims that he did not authorize the Originator to transmit a TEL entry, the RDFI may transmit a return for the TEL entry to its ACH Operator by the ACH Operator's deposit deadline for the return to be made available to the ODFI no later than the opening of business on the banking day following the sixtieth calendar day following the Settlement Date of the TEL entry.

In circumstances in which an entry was not authorized, the RDFI must obtain a Written Statement of Unauthorized Debit from the Receiver before returning the entry. Any subsequent dispute regarding an unpaid debt must be addressed between the Originator and Receiver outside of the ACH return process.

OBLIGATIONS OF RDFIS

Return of TEL Entries

RDFIs are subject to the typical return time frames for transmitting TEL entry returns. Specifically, an RDFI must transmit a TEL return entry to its ACH Operator by the ACH Operator's deposit deadline for the return entry to be made available to the ODFI no later than the opening of business on the second banking day following the Settlement Date of the TEL entry.

In the event that a Receiver claims that he did not authorize the Originator to transmit a TEL entry, the RDFI may transmit a return for the TEL entry to its ACH Operator by the ACH Operator's deposit deadline for the return to be made available to the ODFI no later than the opening of business on the banking day following the sixtieth calendar day following the Settlement Date of the TEL entry.

In circumstances in which an entry was not authorized, the RDFI must obtain a Written Statement of Unauthorized Debit from the Receiver before returning the entry. Any subsequent dispute regarding an unpaid debt must be addressed between the Originator and Receiver outside of the ACH return process.

Stop Payments on TEL Entries

The Nacha Operating Rules for stop payments require Receivers to place a stop payment order on a recurring debit at least three banking days prior to the scheduled date of the entry. In the case of Single Entry TEL entries, the Originator generally processes TEL entries quickly; therefore, Receivers are usually unable to meet the three day advance notice requirement for placing a stop payment order on such entries.

To ensure that a Receiver has the ability to place a stop payment order on a Single-Entry TEL entry or a subsequent TEL entry initiated in accordance with the terms of a standing authorization, the Nacha Operating Rules allow a Receiver to provide a stop payment order to his financial institution so long as it is given in such a time and manner that allows the RDFI a reasonable opportunity to act on the stop payment order prior to acting on the TEL entry.

CHAPTER 48

Internet Initiated/Mobile Entries (WEB)

Internet Initiated/Mobile Entries (WEB entries) are entries transmitted to a consumer Receiver's account. These entries can be either debits (when the Internet or mobile devices are used to initiate the payment) or credits (when payments are exchanged between consumers). WEB entries may be single entry, recurring entry, or subsequent entry transactions and must meet the following consumer payment requirements.

Debit WEB entries are used by non-consumer Originators to debit a consumer based on an authorization that is communicated, other than by an oral communication via a telephone call, from the Receiver to the Originator via the Internet or a Wireless Network. This Standard Entry Class Code also includes debit entries authorized under any form of authorization when the instruction for the initiation of the entry is designed by the Originator to be communicated, other than orally via a telephone call, over a Wireless Network.

Credit WEB entries are used for the origination of credit entries between consumer accounts (Person-to-Person or P2P transactions), regardless of the manner in which the consumer Originator communicates the payment instruction to his financial institution or payment service provider. While most P2P payments are originated electronically via the Internet or using a mobile device, P2P payments may also be originated by other means, such as an in-person instruction provided at a bank branch, and a credit WEB entry is appropriate in either case.

The manner in which the consumer Originator funds its bank or service provider for the credit WEB entry transmitted on the consumer's behalf is not addressed as part of these P2P credit WEB rules. These funding transactions are handled in accordance with the agreement between the consumer originator and the bank or P2P service provider. (NOTE: WEB credit entries may not be used by a non-consumer Originator to transmit a credit entry to a consumer account, even when the consumer's authorization for the credit is provided via the Internet or mobile device.)

Use of the WEB SEC Code for debit entries includes requirements for added security procedures and obligations to help address the following unique risk characteristics inherent to the Internet and Wireless payment environments:

1. the anonymity of the Internet environment in which parties are not certain with whom they are doing business poses unique opportunities for fraud,

2. the Internet as an open network requires special security procedures to be deployed to prevent unauthorized access to Receiver financial information, and

3. the sheer speed with which a large number of payments can be transacted over the Internet (volume and velocity).

Technical solutions and business practices to support WEB payments continue to evolve. Therefore, the Nacha Operating Rules balance the need for security with the desire to maintain some flexibility regarding the methods ACH Network participants use to comply with the Rules. These Operating Guidelines recommend methods ACH participants can use to implement and comply with the Nacha Operating Rules for WEB entries. (NOTE: In any case where these key components are not specifically required under the Nacha Operating Rules, all are recommended by Nacha as sound business practices.)

INITIATING A WEB ENTRY — AN OVERVIEW

When to Use the SEC Code WEB:

1. WEB is appropriate for a non-Consumer Originator to use when initiating debit entries that have been authorized by a consumer Receiver via the Internet or a Wireless Network.

   Example: A consumer's authorization for a debit entry is obtained over the Internet accessed from a device that uses a wired or Wireless Network.

2. WEB is appropriate if the consumer Receiver's instructions for initiation of the debit entry are communicated to the Originator via a Wireless Network, even if the authorization has been given in some other manner.

   Example: An authorization was obtained from the Receiver in person or via a telephone call, but the Receiver sends a text message to communicate when to initiate the debit entry.

3. WEB is appropriate to use when initiating credit entries transmitted between consumers or between consumer accounts belonging to the same person, regardless of the manner in which the payment is initiated.

   Example: A consumer's payment instruction to send funds to another consumer is obtained from a consumer over the Internet accessed from a device that uses a wired or Wireless Network, or via in-person instruction at a bank branch.

4. WEB is appropriate if the consumer's authorization for the debit entry is provided orally, other than via a telephone call, over a Wireless Network.

   Example: A consumer provides a payment instruction during a video chat with a power company, or a consumer provides an oral instruction to a virtual voice assistant to pay a bill or place an order for goods or services.

5. WEB may be used in certain situations involving the initiation of a subsequent entry under the terms of a standing authorization if either the Receiver's standing authorization was obtained via the Internet, or if the Receiver's affirmative action to initiate the payment is communicated via the Internet.

   Example: An Originator obtains a consumer Receiver's standing authorization orally via a telephone call. The terms of the standing authorization specify that the consumer Receiver may affirmatively initiate a subsequent entries via an Internet communication to the Originator. The Originator may identify subsequent entries as either TEL or WEB.

Note: The flexibility for an Originator to use the WEB SEC Code for subsequent entries initiated under the terms of a standing authorization may be superseded by other SEC Code requirements if subsequent eare initiated at an electronic terminal.

When NOT to use the SEC Code WEB:

1. WEB is not appropriate if the consumer's authorization for the debit entry is provided orally via a telephone call.

   Example: Authorization is given during a telephone conversation via a device over a Wireless Network.

2. WEB is not appropriate to initiate entries to non-consumer (business) accounts, even when the non-consumer Receiver (business) provided authorization for the transaction via the Internet.

3. WEB is not appropriate if the POS code would otherwise apply, because the WEB format does not contain the necessary fields for communication of terminal identification information.

   Example: A Receiver uses a near field communication mobile payment service to initiate a debit to his or her bank account to pay for goods at the point-of-sale The merchant (Originator) must use the POS SEC code so that information regarding the merchant identity and terminal location can be properly communicated to the RDFI.

5. WEB is not appropriate to initiate credit entries from a consumer to a non-consumer (business) account. The CIE SEC Code should be used for a bill payment credit from a consumer to a business (this includes a consumer-initiated credit to a loan account).

6. WEB is not appropriate to initiate credit entries between accounts owned by the same party if one account is titled as a consumer account and the account at the other financial institution is titled as a non-consumer (business) account. When an ACH credit entry is originated from the owner's consumer account at one financial institution to his business account at the other financial institution, the entry must be coded as a CIE entry. Conversely, when a credit entry is originated from the owner's business account at one financial institution to his consumer account at the other financial institution, the entry must be coded as a PPD entry.

Other Considerations on When to Use WEB Rather Than Other SEC Codes for Scenarios Involving Mobile Devices

Mobile technologies are creating new mechanisms for initiating ACH entries. The following discussion and scenarios provide additional guidance on when it is, or is not, appropriate to use the WEB SEC code.

When a consumer Receiver key enters information into a mobile device or computer as a means to communicate that information over the Internet to the Originator's servers, the transaction should be coded as a WEB entry, even if the mobile device or computer is owned by the Originator. An example of this scenario is when a consumer enters his or her account information on an insurance company's web page to authorize a debit to pay for an insurance premium, even if the consumer does so on an insurance agent's laptop or tablet computer. The WEB SEC code should be used in this scenario regardless of the physical location where the consumer and the agent meet (e.g., consumer's home, agent's office, local coffee shop). The fact that the consumer and the agent are meeting together does not result in the use of the POS SEC code because the agent's laptop is being used as a means to communicate information over the Internet, not as a POS device.

By contrast, a Point of Sale (POS) Entry is a debit entry to a Consumer Account that is initiated by a Receiver to pay for a purchase of goods or services at an "electronic terminal" at the point of sale or to receive cash back at such a location. This term is intended to be interpreted as defined in Regulation E, and the reference to "point of sale" means the Entry must be initiated by the Receiver in-person at the Originator's electronic terminal. (Adjustments and other credit Entries related to an original POS debit Entry are also coded as "POS," but may be initiated through back office reconciliation processes.)

Examples of electronic terminals for this purpose are traditional terminals at stationary point-of-sale locations such as grocery store cash registers or automated gasoline pumps. The term also includes mobile devices owned or leased by a merchant that are used as mobile check-out terminals, even if the merchant uses the mobile device at a location that is not owned or rented by the merchant. For example, a mobile tablet device that is used by a farmer to accept payments at various farmers' markets around the state would be a point-of-sale electronic terminal for this purpose, and ACH transactions initiated at such a device should be coded as POS.

It is also important to differentiate for this purpose the proper use of the POS, MTE, POP and BOC SEC codes. The following scenarios would not result in the use of the WEB SEC code, even if any part of the transaction utilizes a mobile device:

- If a transaction at a point-of-sale electronic terminal is initiated with an "access device" (as that term is defined in Regulation E) or with account and routing and transit information that is not machine-read from the MICR line, then POS is the correct SEC code to use.

- If the electronic terminal is an ATM (automated cash dispensing machine), then MTE is the appropriate SEC code to use.

- If the transaction is initiated by capturing information from the MICR line of a check through a reading device at the point-of-purchase and returning the check to the consumer, then POP is the correct SEC code to use.

- If the transaction is initiated by capturing information from the MICR line of a check through a reading device at the point-of-purchase itself or later for subsequent conversion during back-office processing, and the check is not returned to the Receiver, then BOC is the correct SEC code to use.

UNSECURED ELECTRONIC NETWORK

The Internet is an unsecured electronic network, even though secure transmissions may be made over that otherwise unsecure network.

A network, public or private, is an unsecured electronic network if:

1. it is not located entirely within a single, contiguous, physical facility, and

2. transmits data via circuits that are not dedicated to communication between two end-points for the duration of the communication, or

3. transmits data via wireless technology

    - excluding a communication that begins and ends with a wireline connection, but that is routed by a telecommunications provider for a portion of the connection over a wireless system.

In addition to the obligations of ACH participants to protect the security and integrity of certain ACH data throughout its lifecycle, the Nacha Operating Rules also impose specific data security requirements for all ACH transactions that involve the exchange or transmission of banking information (which includes, but is not limited to, an entry, entry data, a routing number, an account number, and a PIN or other identification symbol) via an Unsecured Electronic Network. Refer to Chapter 4 of these Guidelines for more detailed information on ACH participants' obligations with respect to ACH security.

COMMERCIALLY REASONABLE

For all debit WEB entries, each Originator is obligated to ensure that certain aspects of the transaction have been handled in a commercially reasonable manner. Those aspects include commercially reasonable methods of authentication to verify the identity of the Receiver, fraudulent transaction detection systems, methodology to establish a secure Internet session, and procedures to verify the validity of the RDFI's routing number.

For a discussion on the concept of commercially reasonable standards, please refer to Chapter 4 of these Guidelines.

SINGLE, RECURRING AND SUBSEQUENT ENTRIES

The WEB Standard Entry Class Code applies to single-entry (i.e., one-time), recurring entry, and subsequent Internet/Mobile debit entries, as well as Person-to-Person (P2P) credits. At their discretion, non-consumer Originators and service providers may choose to identify a recurring entry, a single entry, or a subsequent entry by placing the value "R," "S," or "ST", respectively, within the Payment Type Code field of a Single Entry.

- A Single-Entry WEB entry is a credit or debit initiated by an Originator based on the Receiver's authorization for a one-time transfer of funds to or from the Receiver's account.

  Example: A Single-Entry WEB transaction would be initiated if a consumer purchases a book online.

- A recurring WEB entry is an entry that has been set up to occur at regular intervals without any additional intervention by the Receiver. These instructions are based on a consumer Originator's instructions to pay another consumer (WEB credit) or a consumer Receiver's authorization for a debit, where the authorization is provided to the non-consumer Originator via the Internet or a Wireless Network (WEB debit).

  Example: A monthly debit to the Receiver's account for a mortgage payment.

- A subsequent entry is originated individually upon the affirmative action of the Receiver, based on a standing authorization provided by the Receiver that establishes a relationship with the Originator for a specific type of activity.

  Example: An instruction via mobile device to a broker to purchase securities.

For more information on standing authorizations and subsequent entries, see Chapter 16 of these Guidelines.

OBLIGATIONS OF ORIGINATORS

Agreements with ODFIs

Originators choosing to utilize the ACH Network for initiating debit WEB transactions should consider modifications to their agreements with their ODFIs to address the origination of these entries. These modifications should address:

- the extent to which the Originator and ODFI will share liability for debit WEB transactions, and

- should define any specific processing obligations relating to such transactions

Example: The Nacha Operating Rules require an Originator of debit WEB entries to conduct or have conducted on its behalf, annual audits to ensure that the financial information it obtains from Receivers is protected by security practices and procedures.

The Originator of a P2P entry is not required to enter into an origination agreement with the ODFI in order to transmit credit WEB entries. The requirements of an ODFI/Originator agreement are not suitable to transactions in which a consumer is the Originator and thus are not applicable. This is consistent with the requirements for CIE Entries, which are also exempted from the requirements for an ODFI/ Originator agreement because the Originator is a consumer.

For more information on agreements, refer to Chapter 5 in these Guidelines.

Authorization Requirements

Credit WEB Entries

A Person-to-Person (P2P) entry is intended to involve a credit transmitted on behalf of one natural person (i.e., a consumer Originator) to the account of another natural person (i.e., a consumer Receiver), or between accounts belonging to the same natural person. For these credit WEB entries, no authorization by the Receiver is required.

Debit WEB Entries

Non-consumer Originators of debit WEB entries must obtain the Receiver's authorization prior to initiating a debit entry under this application. Although the Nacha Operating Rules do not prescribe specific authorization language for

the WEB application, the authorization must conform to the requirements of the Rules, which require that:

1. the authorization must be in a writing that is signed or similarly authenticated by the Receiver via the Internet or a Wireless Network, or

2. the authorization is obtained in any manner permissible for other Standard Entry Class Codes, but the Receiver's instructions for the initiation of the debit entry is communicated via a Wireless Network (other than by an oral communication), and

3. the authorization includes the minimum required information for a consumer authorization.

To meet the first requirement that the authorization be in writing, in the context of WEB entries, the Receiver must be able to read the authorization language displayed on a computer screen or other visual display. The Originator should prompt the Receiver to print the authorization and retain a hard copy or electronic copy. The Originator must be able to provide the Receiver with a hard copy of the authorization if requested to do so. Only the Receiver may authorize the WEB transaction, and not a Third-Party Service Provider on behalf of the Receiver.

The Nacha Operating Rules allow the use of a digital signature or code to similarly authenticate a written authorization. Examples of methods used to similarly authenticate an authorization include, but are not limited to, the use of digital signatures, codes, shared secrets, PINs, biometrics, etc. To satisfy the requirements of the Nacha Operating Rules, which parallel Regulation E, the authentication method chosen must identify the Receiver and demonstrate the Receiver's assent to the authorization.

Originators should understand the distinction between authenticating a Receiver for general use on a website (or marketing purposes, etc.) and authentication in the context of an authorization. Authentication of an authorization is strongest when the authorization and the authentication of that authorization occur simultaneously or nearly simultaneously. Although an initial website session log-in may constitute adequate authentication for a click-through authorization as part of the same session, Originators and ODFIs should consider the strength of the association of an initial log-in with a later authorization. The burden of demonstrating that the authentication process is sufficiently linked to the authorization will be on the Originator and ODFI.

For a discussion on the concept of similarly authenticated, please refer to Chapter 16 within these Guidelines.

One of the practical considerations for an Originator is how to present an authorization to a Receiver over the Internet that both meets the requirements of the Nacha Operating Rules and is easily understood. As long as the required information is included in the authorization language, Originators have the flexibility to draft the language in any way that is user-friendly for their customers.

Originators must retain records of a Receiver's authorization in accordance with the requirements discussed in Chapter 16 of these Guidelines. In the physical world this record would be an original or copy of the signed authorization. In the electronic world where the authorization will be similarly authenticated, the Originator must keep a copy of the authorization and a record of the authentication. The Originator must also be able to provide these records to the ODFI upon its request. The ODFI may request these records either for its own use or to forward to the RDFI (the Receiver's financial institution).

In the event that an Originator must demonstrate proof of a Receiver's authorization for a debit WEB entry, it should provide documentation that provides transaction details including Receiver information.

Example: Originators can provide a screen shot of the authorization language and then the date/timestamp of the Receiver login and the authorization process that evidenced both the consumers' identity and his assent to the authorization.

RISK MANAGEMENT

To help mitigate the added risk associated with Internet/Mobile payments, Originators are obligated to comply with stringent risk management requirements when originating debit WEB entries. At a minimum, Originators of such entries must implement the following risk management techniques:

Authentication

The best way Originators can minimize the potential for fraudulent Internet/Mobile initiated ACH transactions is to employ robust authentication methods to verify the identity of the Receiver before accepting ACH debit authorizations online. The more robust the authentication, the less likely the transaction will be fraudulent and the less likely the payment will be returned to the Originator as unauthorized. Since the Originator may ultimately be responsible for unauthorized or fraudulent ACH transactions when those transactions are returned, it is to their benefit to incorporate adequate levels of authentication into their online ACH payment processes.

When considering which authentication methods to use, Originators should determine whether their debit WEB entry transactions will be conducted with existing customers, new customers or both. Originators with an established business relationship with the Receiver — whether established online, in person, over the telephone, or some other method — can usually authenticate those customers using shared secrets such as a PIN, password or previous transaction history.

The Originator has the responsibility to choose an appropriate solution for authentication that will minimize the potential for fraudulent transactions. Common examples in use today include asking for several forms of identifying information and checking that information against databases; asking challenge questions based upon credit bureau or other information; or sending the Receiver a specific piece of information, either online or offline, and then asking the Receiver to verify that information as a second step in the authentication process.

Originators should understand financial industry trends in the adoption of multifactor authentication and layered security, or additional risk mitigation controls to verify the identity of the Receiver. The Federal Financial Institution Examination Council (FFIEC) released guidance to financial institutions in October 2005, Authentication in an Internet Banking Environment, to which it issued a supplement in 2011. The guidance provides information on several of the authentication techniques, processes and methodologies that are widely available in the marketplace. Originators should periodically refer to the FFIEC for any updates to this guidance.

Though user ID/PIN/password are still the most common solution for online authentication, there is a growing trend toward replacing passwords with more robust authentication such as use of additional authentication factors or securities layers.

Multifactor authentication uses multiple characteristics to determine a Receiver's identity, for example by obtaining and verifying more than one of the following:

- something the Receiver knows (password),
- something the Receiver has (a personal computer),
- something the Receiver is (voice or fingerprint), and
- someplace the Receiver is (geolocation).

Some other factors to consider in selecting an authentication method that is commercially reasonable include typical transaction amount, type of goods offered, method of delivery, and control of goods or funds. It is important to note that it will never be considered commercially reasonable to have done nothing. Similarly, simply assigning a password without validation of user identity and allowing the Receiver to use that password in the same Internet session as the sole method of authenticating the Receiver is also not commercially reasonable.

Fraudulent Transaction Detection Systems

Using fraudulent transaction detection systems to screen debit WEB entries reduces the potential for fraudulent ACH transactions. Fraudulent transaction detection systems employ different methodologies and different features at varying costs. At a minimum, the system must validate the account number to be debited upon the number's first use and for any subsequent changes to the account number. The choice of which other features should be included in a fraudulent transaction detection system for a particular Originator is generally a decision to be made by the Originator.

Examples of fraudulent transaction detection systems are systems that ensure the account is open and available for ACH processing, track payment history, behavior, purchase type, delivery information, etc. Factors to consider when choosing a fraudulent transaction detection system for debit WEB entries include, but are not limited to:

- the number of transactions processed by the Originator,
- the average dollar size of each transaction,
- the typical relationship with the Receiver (existing or new), and
- the type of goods or services being sold.

An important element of a commercially reasonable fraudulent transaction detection system is the adoption of risk-based mechanisms designed to confirm the validity of an account to be debited. For example, the use of an ACH prenotification entry or an ACH micro-deposit confirmation would result in a return entry indicating "No Account" (R03) or similar return reason, thereby indicating that the related live entry should not be sent. Other available account validation methods also can provide a similar indication that there would be a problem with the underlying live entry. The greater the value, volume or velocity of transactions, the more robust the account validation system needs to be.

Guidance for ODFIs and their Originators of Debit WEB entries

- In compliance with the Nacha Operating Rules, Originators must utilize a commercially reasonable fraudulent transaction detection system that includes account number validation to screen debit WEB entries.
  - ODFIs should communicate with their Originators of debit WEB entries regarding this requirement, including internal Originators (card, mortgage, lending, account opening, etc.).
  - ODFIs should consider risk-based affirmative outreach to Originators most likely to be exposed to the above activity.
- Identify and act on red flags for debit WEB entries. Examples related to this specific scenario include:
  - Large numbers of customers changing the routing number for payments.
  - A significant increase in the use of a specific routing number over a short period of time.
  - An early payoff of a loan (e.g., a student loan), in conjunction with a change in the source of payment.
  - Atypical large-dollar funding of a new or existing account.
  - Multiple payment attempts by the same person.
  - An overpayment of a bill or tax payment.
- Use an appropriate commercially reasonable method of account validation

- ACH prenotifications and micro-deposits can be accelerated through the use of Same Day ACH processing.

- Commercial account validation solutions are available, including those enabled by APIs .

- Act on returns of prenotifications and micro-deposits, or the results of other account validation methods, prior to sending any related live entries.

- Monitor the use of Federal Reserve and U.S. government routing numbers when used for originating debit payments; and monitor returns of those debits.

  - The receipt of a return with Return Reason Code R34 (Limited Participation DFI) is a red flag. R34 is a return from the ACH Operator, and means that the RDFI for the routing number is limited in its ACH participation.

- RDFIs may use Return Reason Code R17 (File Record Edit Criteria/Entry with Invalid Account Number Initiated Under Questionable Circumstances) with QUESTIONABLE in the Addenda Information field to highlight these potential abuses of the system. Accordingly, although there are some other uses of the R17 code, receiving debit entries returned from RDFIs with Return Reason Code R17 with QUESTIONABLE in the Addenda Information field indicates a different scenario from other routine administrative returns.

- Assess, and act on in good faith, a request from an RDFI to temporarily block the use of its routing number in originating consumer debit transactions.

A fraudulent transaction detection system must be used no matter how small the transaction amount or type. To not deploy any method or procedure to detect transaction fraud and validate the account number used in a WEB entry is not considered commercially reasonable.

Annual Data Security Audits

Data loss or compromise not only hurts the Receiver, but can also damage a business's reputation. Receiver trust is a key factor in building loyalty. It is in the Originator's best interest to develop and deploy practices that protect the integrity of Receiver information and the transaction, and to ensure that these practices are audited for their effectiveness.

The Nacha Operating Rules for debit WEB transactions require Originators to conduct an annual data security audit to ensure that Receivers' financial information is protected by security practices and procedures that ensure the financial information the Originator obtains from Receivers is protected by commercially reasonable security practices that include adequate levels of:

1. physical security to protect against theft, tampering, or damage,

2. administrative, technical, and physical access controls to protect against unauthorized access and use, and

3. network security to ensure secure capture, transmission, storage, distribution and destruction of financial information.

While the Nacha Operating Rules only require Originators of debit WEB Entries to conduct an audit of their security practices and procedures once a year, many companies are now opting to audit these practices bi-annually or even quarterly due to the rapid change of technology and security risks. It is therefore highly recommended that Originators of debit WEB entries conduct more frequent audits.

This audit requirement can be met in several ways. It can be a component of a comprehensive internal or external audit, or it can be an independent audit that uses a commercially reasonable generally accepted security compliance program. An Originator that is already conducting an audit of these practices and procedures for another area of its

business is not required to have two separate audits. However, the audit should address adequate levels of data security for the Originator's ACH operations.

The following sections detail the minimum components that need to be audited in order to be in compliance with the audit requirement. (NOTE: In any case where these key components are not specifically required under the Nacha Operating Rules, all are recommended by Nacha as sound business practices.)

1. Physical security to protect against theft, tampering or damage

   • Critical network, server, and telecommunications equipment should be placed in physically secure locations that permit access only to authorized personnel.

   • Firewalls must be fully deployed with secured processes for administering those firewalls.

   • Firewalls must protect websites from inappropriate and unauthorized access.

   • Disaster recovery plans must be developed and reviewed periodically.

2. Personnel and access controls to protect against unauthorized access and use

   • A formal set of security policies and procedures must be developed that clearly outline the corporate rules governing access to sensitive financial data.

   • Hiring procedures should be developed that will, at a minimum, verify application information and check references on new employees that will have access to Receiver financial information.

   • Relevant employees must be educated on information security and company practices and their individual responsibilities.

   • Access controls should be in place to ensure adequate administrative, technical, and physical controls:

     – Limit employee access to secure areas and to documents/files that contain Receiver financial information.

     – Ensure that terminated employees have no access to secure information and areas.

     – Permit visitors only when absolutely necessary to these areas and information and ensure they are accompanied by an employee at all times.

     – Authenticate all access to any database containing sensitive ACH information such as financial information (e.g., passwords or passphrase, multifactor authentication such as token devices, smart cards, biometrics, or public keys).

     – Implement key-management procedures to require split knowledge for dual control of keys (e.g., requiring two or three people (or processes or procedures) to cooperate in gaining authorized access to a system resource (data, files, devices) – a separation of duties).

     – Establish policies and procedures to monitor and audit all user activity for personnel with access to Receiver information in order to detect exceptions.

3. Network security to ensure secure capture, transmission, storage, distribution, and destruction.

   • Install and maintain a firewall configuration to protect all Receiver financial information, including but not limited to the company network and databases, and portable electronic devices (e.g., employee laptops, smartphones, etc.)

- Install and update anti-virus software on a regular basis.
- Ensure all system components have the latest vendor-supplied security patches installed.
- Change vendor-supplied defaults before installing a system on the network.
- Minimize retention and/or storage of all Receiver financial information.
- Develop a data retention and disposal policy and schedule to include a process (manual or automatic), to remove, at least on a quarterly basis, any unnecessary Receiver financial information. Monitor these retention schedules regularly.
- Receiver financial information should only be stored permanently if it is required by law, regulation, rule, or a governing organization.
- Limit distribution of Receiver financial and personal information and implement procedures and policies to govern the distribution of sensitive financial information.
- Review data distribution policies and procedures periodically.
- Encrypt Receiver data and financial information at all points in the transaction lifecycle from transmission to storage via a secure, electronic means that provides a commercially reasonable level of security compliant with current, applicable regulatory guidelines.
- Render account numbers used in the origination and transmission of ACH transactions unreadable when stored electronically.
- Regularly test security systems and processes (e.g., vulnerability scans, external and internal penetration testing, intrusion detection, file integrity monitoring).

It is important to note that for transactions that involve some use of the Internet but are not defined as WEB transactions, Originators must incorporate the security and risk management principles of the WEB rules, as applicable. For example the Originator is required to authenticate the Receiver and conduct a data security audit to ensure the Receiver's data is stored securely.

Verification of Routing Numbers

Many debit WEB entries are Single-Entry payments, and Receivers frequently enter their routing numbers manually using a keyboard. To minimize exception processing related to debit WEB entries, each Originator is required to employ commercially reasonable procedures to verify that routing numbers are valid. Originators should try to ensure that the Receiver enters the routing number correctly and that it is a valid RDFI routing number for ACH transactions.

Verifying the validity of routing numbers can be accomplished by:

- a component of a fraudulent transaction detection system,
- through a separate database or directory (either commercial or proprietary), or
- through other methods devised by the Originator, for example manual intervention such as calling the Receiver's financial institution.

RESPONSIBILITIES OF ODFIS

Agreements with Originators

ODFIs are not required to have origination agreements with the consumer Originators of P2P entries in order to transmit credit WEB entries. The requirements of an ODFI/Originator agreement are not suitable to transactions in which a consumer is the Originator and thus are not applicable. This is consistent with the requirements for CIE Entries, which are also exempted from the requirements for an ODFI/Originator agreement because the Originator is a consumer.

However, ODFI/Originator agreements are required for Originators of debit WEB entries. Each ODFI that chooses to transmit debit WEB entries on behalf of its Originators should make modifications to its agreements with its Originators to address the origination of these entries. These modifications should address:

- the allocation of liability between the Originator and ODFI for WEB transactions, and
- any specific processing obligations relating to such transactions.

In addition, these agreements should address the procedures, practices, and systems Originators are using to comply with their obligations under the Nacha Operating Rules governing debit WEB entries.

For example, the agreement may need to address the authentication methods and the fraudulent transaction detection systems the Originators are using for debit WEB entries. ODFIs may also want to see proof of the Originator's annual data security audit prior to or as a condition of transmitting debit WEB entries for the Originator.

Additional issues that should be considered in the agreements between the Originator and the ODFI are provided in Appendix C of these Guidelines.

Additional ODFI Indemnification for Credit WEB Entries

In addition to the general indemnifications the ODFI makes to the RDFI with respect to any ACH Entry, the ODFI of a credit WEB entry also indemnifies and holds harmless any RDFI that suffers any loss or liability from accurately providing the contents of the Payment Related Information field to the Receiver.

Formatting Requirements

As with all ACH entries, ODFIs must ensure that, prior to transmission to the ACH Operator, WEB entries comply with all technical specifications and formatting requirements in accordance with the Nacha Operating Rules. ODFIs must ensure that:

- "WEB" must appear within the Standard Entry Class Code Field of the Company/Batch Header Record;
- the Individual Name Field of the Entry Detail Record of a WEB transaction includes the name of the Receiver; and
- a WEB entry may be accompanied by one optional addenda record (type "05").

At their discretion, Originators may identify a recurring entry, single entry, or subsequent entry through the use of an optional indicator code of "R," "S," or "ST" in the Payment Type Code Field of the Entry Detail Record.

For credit WEB entries only:

- P2P service providers (i.e., ODFIs or Third-Party Service Providers) must identify the consumer Originator (the sender) of the P2P payment within the Individual Identification Number field of the WEB credit's Entry Detail Record.

- the P2P service provider (i.e., the consumer's ODFI or the Third-Party Service Provider) must identify itself within the Company Name and Company Identification fields of the Company/Batch Header Record.

- The Company Entry Description field within the Company/Batch Header Record must contain a descriptive statement that identifies the P2P transaction in a way that is meaningful to the consumer. For example, the text could use "P2P," or it could refer to the trade name of a specific P2P payment service.

- ODFIs may transmit up to 80 characters of plain-text remittance information with a credit WEB entry. While ODFIs and/or Third Party Senders must ensure that valid characters are used within the Payment Related Information field of the credit WEB entry's addenda record (see ACH File Exchange Specifications within Appendix One of the Rules), ODFIs and Third Party Service Providers do not need to ensure that remittance data is conveyed within ANSI ASC X12 data segments or Nacha-endorsed banking conventions.

Return of WEB Entries

WEB entries, like other ACH entries, may be returned for a variety of valid reasons in accordance with the return time frames prescribed by the Nacha Operating Rules.

For further guidance on return entries, please refer to Appendix Four of the Nacha Operating Rules.

Return by ACH Operator

Any WEB entry that contains all spaces or all zeros in the Individual Name Field will be rejected and returned by the ACH Operator because the Individual Name Field within the WEB Entry Detail Record is a mandatory field. [NOTE: The inclusion of all spaces or all zeros in any other mandatory field will also cause the entry to be returned by the ACH Operator.]

Return by RDFI

ODFIs should be aware that the Receiver may:

1. request his RDFI to stop payment on a debit WEB entry (Return Reason Code R08);

2. request his RDFI to return an unauthorized debit WEB entry (Return Reason Code R10);

3. request his RDFI to return a debit WEB entry authorization revoked (Return Reason Code R07).

Occasionally the financial information the Receiver provides to the Originator for a WEB entry is incorrect. When this occurs, the entry may be returned using the following Return Reason Codes:

- R03 (No Account/Unable to Locate Account), or

- R04 (Invalid Account Number).

In this situation, for a debit WEB entry, the ODFI must handle the return according to its agreement with the Originator. If a credit WEB entry is returned R03 or R04, the ODFI must handle the return according to its agreement with the P2P provider. Because the Originator of a P2P transaction is a consumer customer, the Originator of a credit WEB entry is not likely to be in a position to receive ACH return data.

Stop Payments on WEB Entries

ODFIs should be aware that for recurring debit WEB Entries, the Nacha Operating Rules regarding ACH stop payments require Receivers to place a stop payment order on a debit at least three banking days prior to the scheduled date of the entry. The RDFI may, at its discretion, honor such a stop payment order received within such three banking day period.

To ensure that a Receiver has the ability to place a stop payment order on a Single-Entry debit WEB transaction, the Nacha Operating Rules allow a Receiver to provide a stop payment order for Single-Entry debit WEB entries to his financial institution so long as it is given in such a time and manner that allows the RDFI a reasonable opportunity to act on the stop payment order prior to acting on the debit entry.

Reversals

The Nacha Operating Rules do not address the use of reversals for credit WEB Entries. However, Nacha recommends that ODFIs consider prohibiting a consumer Originator of a credit WEB entry from originating a reversal for the entry without the intervention of the ODFI or its Third Party Service Provider, since doing so would result in one consumer debiting another consumer's account. Instead, Nacha recommends that third party service providers or ODFIs originate any necessary reversing entries if such corrections are warranted and in accordance with the Rules.

Notifications of Change (NOCs) for P2P WEB Credit Entries

When the ODFI receives a Notification of Change in response to a recurring credit WEB entry, the ODFI must make the changes itself, or provide the P2P provider with the necessary information within two banking days of the Settlement Date of the NOC or corrected NOC. Because a consumer customer is the Originator of the Entry, the Originator is not likely to be in a position to receive or make the changes contained within the NOC. As a result, it is the financial institution and/or third-party P2P service provider that should be using the information in the NOC to update its systems. As with any other NOC for recurring entries, the ODFI or the P2P provider must make the changes specified in the NOC or corrected NOC within six banking days of receipt of the NOC information or prior to initiating another entry to the Receiver's account, whichever is later. For Single-Entry P2P WEB credits, action on an NOC is at the discretion of the ODFI or P2P service provider .

Periodic Statements

Because a credit WEB entry is originated by a consumer customer of the ODFI (similar to CIE), the ODFI is required to satisfy periodic statement requirements in accordance with Regulation E and Nacha Operating Rules by providing certain transaction information to the consumer Originator of a WEB credit. This information includes the posting date of the offsetting debit to the consumer Originator's account; the dollar amount of the entry; the payee name, etc.

RESPONSIBILITIES OF RDFIS

Return of WEB Entries

WEB entries may be returned for a variety of valid reasons in accordance with the requirements of the Nacha Operating Rules. With the exception of entries for which the Receivers claims there was no authorization, the RDFI must transmit WEB entry returns by its ACH Operator's deposit deadline for the return entry to be made available to the ODFI no later than the opening of business on the second banking day following the Settlement Date of the original entry.

For a debit entry that the Receiver claims is unauthorized (Return Reason Code R10) or for which authorization was revoked (Return Reason Code R07), the RDFI must transmit the return by its ACH Operator's deposit deadline for the return to be made available to the ODFI no later than the opening of business on the banking day following the 60th calendar day following the Settlement Date of the original entry. For the return of these entries, the RDFI must obtain a written statement of unauthorized debit from the Receiver stating that the entry was not authorized prior to returning the entry.

Stop Payment on WEB Entries

For recurring debit WEB Entries, the Nacha Operating Rules regarding ACH stop payments require Receivers to place a stop payment order on a debit at least three banking days prior to the scheduled date of the entry. The RDFI may in its discretion honor such a stop payment order received within this three banking day period.

Originators generally process Single-Entry debit WEB transactions quickly; therefore Receivers are usually unable to meet the three day advance notice requirement for placing a stop payment order on such entries.

To ensure that a Receiver has the ability to place a stop payment order on a Single-Entry debit WEB entry, the Nacha Operating Rules allow a Receiver to provide a stop payment order to his financial institution so long as it is given in such a time and manner that allows the RDFI a reasonable opportunity to act on the stop payment order prior to acting on the debit entry.

Periodic Statements

For each entry to a consumer account, the RDFI must provide or make available to the consumer Receiver specific information concerning the entry, including, among other things, the dollar amount of the entry, the date the entry was posted to the consumer's account, and the name of the Originator of the entry. (Please refer to the Nacha Operating Rules for a detailed listing of information that RDFIs must provide regarding ACH entries to a consumer's account.)

Like any other entry, RDFIs must also properly identify the sender of a credit WEB entry on the Receiver's periodic statement and other transaction reports (e.g., online statement) in order to comply with Regulation E. For credit WEB Entries, the sender of the funds is identified within the Individual Identification Number field of the Entry Detail Record rather than the Company Name field of the Company/Batch Header Record. RDFIs need to provide the contents of the Individual ID Number field on the Receiver's periodic statement and other transaction reports. Because the placement of the sender's name in a credit WEB entry differs from other ACH entries, RDFIs will need to ensure their software has the appropriate coding to accommodate this placement of this information on consumers' periodic statements.

Some Originators make a practice of including a consumer's SSN or ITIN or other personally identifiable information in the Individual ID Number field for other SEC Codes. While the contents of this field must be provided for credit WEB Entries, Nacha generally recommends for other types of entries that RDFIs avoid, to the extent possible, displaying the contents of this field on documents that may be mailed or otherwise delivered to a consumer in an unsecure manner.

NOTE: While the RDFI is not required to provide the consumer Receiver with any Payment Related Information that may be transmitted with a credit WEB entry, it may do so at its discretion. If it does so, the ODFI indemnifies the RDFI against any loss or liability associated with the accurate provision of that remittance information.

CHAPTER 56

Rules Compliance Audits

ODFI AUDIT REQUIREMENTS

Proof of Authorization

- Does the ODFI:

  – provide 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 of receipt of the request without charge? (NOTE: For entries other than XCK entries)

  – provide to the RDFI, upon receipt of the RDFI's written request, an accurate record evidencing the Receiver's authorization, or the contact information for the Originator (that at a minimum, includes (a) the Originator's name and (b) the Originator's phone number or email address) within ten Banking Days of receipt of the request without charge)? (NOTE: for CCD, CTX, or Inbound IAT entries to a Non- Consumer Account)

• When the ODFI agrees to accept the return of an entry in lieu of providing the original, copy, or other accurate record of the Receiver's authorization to the RDFI, does the ODFI

- provide the RDFI with written confirmation that the ODFI has agreed to accept the return of the entry at any time within ten banking days of providing the confirmation to the RDFI?

- provide the RDFI with the original, copy, or other accurate record of the Receiver's authorization within ten banking days if the RDFI submits a subsequent request for a copy of the authorization?

Reference: Article Two, Subsection 2.3.2.7 – Retention and Provision of the Record of Authorization; Subsection 2.5.18.6 – Rules Exceptions for XCK entries; and Article Two, Subsection 2.3.3.3 – Provision of the Record of Authorization

APPENDIX G

Sample Authorization for Direct Payment via ACH (ACH Debit)

CONSUMER AUTHORIZATION FOR DIRECT PAYMENT VIA ACH (ACH DEBITS)

Direct Payment via ACH is the transfer of funds from a consumer account for the purpose of making a payment.

I (we) authorize _____[Company Name]_____ ("COMPANY") to electronically debit my (our) account (and, if necessary, electronically credit my (our) account to correct erroneous debits[1]) for (select one)

- ☐ a single (one-time) entry
- ☐ recurring entries (that recur at substantially regular intervals without my affirmative action to initiate future entries)
- ☐ subsequent entries (initiated under the terms of my standing authorization) that require my affirmative action to initiate those future entries

as follows:

☐ Checking Account / ☐ Savings Account (select one) at the depository financial institution named below ("DEPOSITORY"). I (we) agree that ACH transactions I (we) authorize comply with all applicable laws.

Depository Name _____

Routing Number_____ Account Number_____

Amount of debit(s) or method of determining amount of debit(s) [or specify range of acceptable dollar amounts authorized]: _____.

Date(s) including the start date and/or frequency of debit(s):[2] _____.

Action(s) the Receiver must take to initiate a subsequent entry to a standing authorization[3] _____

_____.

I (we) understand that this authorization will remain in full force and effect until I (we) notify COMPANY [insert manner of revocation, i.e., in writing, by phone, location, address, etc.] that I (we) wish to revoke this authorization. I (we) understand that COMPANY requires at least [X days/weeks] prior notice in order to cancel this authorization.[4]

Receiver's Name(s) _____

Date_____ Signature(s) _____

[1] *The Nacha Operating Rules do not require the consumer's express authorization to initiate Reversing Entries to correct erroneous transactions. However, Originators should consider obtaining express authorization of debits or credits to correct errors.*

[2] *That this information will be defined by the Originator.*

[3] *That this information will be defined by the Originator.*

[4] *Written debit authorizations must provide that the Receiver may revoke the authorization only by notifying the Originator in the time and manner stated in the authorization. The reference to notification should be filled with a statement of the time and manner that notification must be given in order to provide company a reasonable opportunity to act on it (e.g., "In writing by mail to 100 Main Street, Anytown, NY that is received at least three (3) days prior to the proposed effective date of the termination of authorization").*

APPENDIX H

Proper Use of SEC Codes for Consumer Entries

EXPLANATION OF SEC CODE ALLOCATIONS

This appendix provides users of the ACH Network with guidance on the proper use of Standard Entry Class (SEC) Codes for common types of Single Entries, Recurring Entries and Subsequent Entries (pursuant to a Standing Authorization) to Receivers' Consumer Accounts. The charts below are not intended to provide exhaustive guidance on SEC Code selection for all possible scenarios. Further, the charts below are intended to provide guidance on SEC Code selection and do not provide a restatement of all requirements applicable to the Entry, including those related to compliance with the E-Sign Act, Regulation E or the Telemarketing Sales Rule.

Comprehensive details on SEC Codes used for entries to consumer accounts can be found in Article Two, Section 2.5 (Provisions for Specific Types of Entries) and Article Eight (Definitions of Terms Used in These Rules). Complete information on authorization requirements for entries to consumer accounts (including requirements related to oral authorizations) is located within Article Two, Section 2.3 (Authorization and Notice of Entries) of the Nacha Operating Rules.

Single and Recurring Debit Entries

The chart below identifies the appropriate Standard Entry Class Codes to be used for the transmission of debit single entries and debit recurring entries and is based on the manner/communication channel used to convey the Receiver's authorization for the debit(s) to the Originator. A single entry debit to a consumer account is initiated by an Originator in accordance with the Receiver's authorization for a one-time transfer of funds from the Receiver's account. A recurring entry debit to a consumer account is one that is initiated by an Originator in accordance with the Receiver's authorization to debit the Receiver's account on a recurring basis at substantially regular intervals, without further affirmative action by the Receiver to authorize those future entries.

The chart identifies appropriate Standard Entry Class Codes for single entries and recurring entry debits for which enrollment/authorization occurred in physical form via hard copy (Box A), via the internet (Box B), or via the telephone (Box C). SEC Codes for transactions relying on physical enrollment/authorization via hard copy (including telephone-based acceptance of a hard copy authorization form) or via the Internet are the general codes that apply based on the form of enrollment/authorization for the service — WEB for internet-based enrollment/authorization, and PPD for all others. The TEL Code applies to orally-provided telephone-based authorizations except when the terms of a previously-provided written authorization are being signed via telephone (by entry of a code or orally).

SINGLE AND RECURRING DEBIT ENTRIES TO CONSUMER ACCOUNTS

TRANSACTION INITIATION METHOD	AUTHORIZATION METHOD		
	Physical Authorization	**Authorization Via Internet**	**Authorization Via Telephone**
Single Entry and Recurring Entries **(i.e., no additional direct action from Receiver required for initiation of entries)**	Examples: Customer executes a written authorization in person or delivers a written authorization via mail for a one-time (single entry) debit or a recurring monthly ACH (recurring entry) debit to pay a bill Customer executes a written authorization in person or delivers a written authorization via mail for a monthly ACH debit to transfer funds into another account (recurring entry) ***Proper SEC Code: PPD*** ***Box A***	Examples: Customer executes an authorization on a biller's web site for a one-time (single entry) debit or a monthly ACH (recurring entry) debit to pay a bill Customer executes an authorization on a bank's web site for a monthly transfer into a savings account (recurring entry) ***Proper SEC Code: WEB*** ***Box B***	Examples: Customer receives in writing the terms of an ACH authorization in a billing statement and "signs" the authorization to pay the bill (single entry) or future recurring bills (recurring entry) by entering a code into the biller's VRU Customer receives in writing the terms of an ACH authorization in a billing statement and "signs" the authorization to pay the bill (single entry) or future recurring bills (recurring entry) by providing an orally-authenticated signature into a recorded line ***Proper SEC Code: PPD*** Customer has not received written terms of ACH authorization, calls into a biller customer service line, is provided the terms of the authorization orally and orally authorizes a one-time debit (single entry) Customer has not received written terms of ACH authorization, initiates a call into a recorded biller customer service line, is provided the terms of the authorization orally, and orally authorizes monthly debits (recurring entry) ***Proper SEC Code: TEL*** ***Box C***

Standing Authorizations and Subsequent Entries

The following chart addresses Standard Entry Class Codes appropriate for the transmission of subsequent entries initiated in accordance with the terms of a standing authorization. A standing authorization is an advance authorization by a Receiver for future entries (that is, subsequent entries) to the Receiver's consumer account, where the Receiver must take further affirmative action to initiate each of those subsequent entries. The terms of a standing authorization must clearly specify the action(s) that the Receiver must take to initiate a subsequent entry.

Where a standing authorization is involved, the Rules allow for some flexibility in how an Originator may identify subsequent entries. In general and subject to certain exceptions described below, an Originator may identify a subsequent entry using the Standard Entry Class Code that is appropriate to either (i) the manner in which the Receiver's standing authorization was communicated to the Originator, or (ii) the manner in which the Receiver's affirmative action to initiate the subsequent entry was communicated to the Originator.

Exceptions:

- An Originator **must** use the POS, MTE or SHR SEC Code, as appropriate, to identify a subsequent entry to a Consumer Account initiated at an "electronic terminal" (as that term is defined in Regulation E), regardless of the manner in which the Originator obtained the Receiver's standing authorization. Use of these formats is necessary for an Originator to identify the electronic terminal used at the point of sale (POS), at an ATM location (MTE) or at the point of sale in a shared network where the ODFI and RDFI have an agreement in addition to these Rules to process entries (SHR), as required by Regulation E.
- An Originator **may not** use the PPD SEC Code for a subsequent entry if it obtained the Receiver's standing authorization (i) as an Oral Authorization via a telephone call, or (ii) via the internet or a wireless network.

Subsequent Entries Initiated via the Internet or Telephone

Boxes D, E, and F address ACH products that are used on the internet.

Boxes G, H, and I address the authorization of ACH transactions over the phone pursuant to a previously obtained standing ACH authorization.

When an ODFI (or Originator) has a pre-existing standing authorization obtained through a physical channel (e.g., a physically signed authorization for insurance payments), the fact that the customer later uses the ODFI's or Originator's internet or telephone service to confirm an individual payment does not require conversion from PPD to a WEB or TEL code. Many of the risks associated with remote-based transmission of the original account information are not present in such circumstances.

Subsequent Entries Initiated at the POS or over a Shared Network

The second row of the chart addresses products that are physically used at the point-of-sale for retail purchases, including when initiated in a shared network where the ODFI and RDFI have an agreement in addition to the Rules to process the Entries.

Box J addresses products for which both enrollment and use occurs at the point-of-sale. This is the primary type of transaction for which the POS code was originally developed.

Box K addresses products for which the original enrollment occurred on the internet, but which are then used at the physical point-of-sale. The Rules require 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. Accordingly, the POS code must 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.

Box L 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 correct code, enabling the communication of the individual transaction data to the RDFI.

Subsequent Entries Initiated via the ATM

Boxes M, N, and O address the use of ACH products at the ATM and raise issues very similar to the boxes related to POS and SHR in the second 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.

STANDING AUTHORIZATION WITH SUBSEQUENT ENTRIES

SUBSEQUENT ENTRY TRANSACTION INITIATION METHOD	ENROLLMENT/STANDING AUTHORIZATION METHOD		
	Standing Authorization Obtained Via Physical Enrollment	**Standing Authorization Obtained Via Internet Enrollment**	**Standing Authorization Obtained Via Telephone Enrollment**
Subsequent Entry Initiated via the Internet or Wireless Network	Examples: Customer opens account at a bank branch and authorizes in writing debits to transfer funds into the account, and initiates such debits via the bank's web site Customer enrolls in writing 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 in writing 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 purchases at a web site ***Proper SEC Code: PPD or WEB*** ***Box D***	Examples: 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 Customer enrolls via the Internet with a virtual assistant service provider, and initiates individual, oral instructions to the virtual assistant via voice recognition technology to make online purchases Customer enrolls with a mobile payment and digital wallet service over the Internet or Wireless Network and initiates individual payments at a merchant's website ***Proper SEC Code: WEB*** ***Box E***	Examples: Customer orally 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 orally 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: TEL or WEB*** ***Box F***

SUBSEQUENT ENTRY TRANSACTION INITIATION METHOD	ENROLLMENT/STANDING AUTHORIZATION METHOD		
	Standing Authorization Obtained Via Physical Enrollment	**Standing Authorization Obtained Via Internet Enrollment**	**Standing Authorization Obtained Via Telephone Enrollment**
Subsequent Entry Initiated via Telephone	Examples: Customer opens account at a bank branch and authorizes in writing debits to transfer funds into the account, and initiates such debits via the bank's telephone payment system Customer enrolls in writing 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 payment system Customer enrolls in writing at a merchant store or a bank branch for an ACH-based debit card, and uses the card to make purchases over the phone ***Proper SEC Code: PPD or TEL*** ***Box G***	Examples: 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 or TEL*** ***Box H***	Examples: Customer receives a written ACH authorization with a billing statement and "signs" the authorization to pay future bills by entering a code into the biller's VRU or providing an orally-authenticated signature into a recorded line and initiates each initiates each subsequent bill payment orally over the telephone. ***Proper SEC Code: PPD or TEL*** ***Box I***
Subsequent Entry Initiated at Point-of-Sale	Examples: Customer enrolls in writing 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 purchases at a POS terminal ***Proper SEC Code: POS or SHR (if initiated in a shared network)*** ***Box J***	Examples: Customer enrolls at a merchant or bank web site for an ACH-based debit card, and uses the card to make purchases 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 to make purchases at a POS terminal ***Proper SEC Code: POS or SHR (if initiated in a shared network)*** ***Box K***	Example: Customer enrolls through a merchant or bank telephone system for an ACH-based debit card, and uses the card to make purchases at a POS terminal ***Proper SEC Code: POS or SHR (if initiated in a shared*** ***Box L***
Subsequent Entry Initiated at ATM	Examples: Customer enrolls in writing 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 M***	Examples: 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 N***	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 O***

APPENDIX I

Sample Written Statement of Unauthorized Debit (ACH)

Following is a sample Written Statement of Unauthorized Debit. This sample written statement is provided for illustrative purposes only. The RDFI's legal department should review any written statement it develops to ensure that it meets the needs of the organization and is in compliance with the Nacha Operating Rules.

[FINANCIAL INSTITUTION NAME]

SAMPLE WRITTEN STATEMENT OF UNAUTHORIZED DEBIT (ACH)

1. Account/Transaction Information

Name_____

Account Number _____

Amount of Debit_____

Date of Debit _____

Party Debiting the Account _____

2. Statement

I (the undersigned) hereby attest that (i) I have reviewed the circumstances of the above electronic (ACH) debit to my account; (ii) the debit was not authorized, or did not conform to the terms of my authorization; and (iii) the following, to the best of my ability to identify, is the reason for that conclusion.

I did not authorize the debit to my account.

- ☐ I do not know or did not authorize the party listed above to debit my account.
- ☐ The signature of a check that was processed electronically is not my signature.

I authorized the party listed above to debit my account, but the entry does not conform to the terms of my authorization.

- ☐ My account was debited before the date that I authorized.
- ☐ My account was debited for an amount different than I authorized.
- ☐ My account was debited by an authorized third party, but that third party failed to make my payment as instructed.
- ☐ My check was improperly processed electronically.
- ☐ A debit to my account that was previously returned was improperly reinitiated.
- ☐ A debit to my account was an improper reversal.

I authorized the party listed above to debit my account, but:

- ☐ I revoked the authorization I had given to the party to debit my account before the debit was initiated.
- ☐ Other (must specify) _____

_____

3. Signature

I am an authorized signer, or otherwise have authority to act, on the account identified in this statement. I attest that the debit above was not originated with fraudulent intent by me or any person acting in concert with me.

I have read this statement in its entirety and attest that the information provided on this statement is true and correct.

Signature_____ Date_____

SAMPLE WRITTEN STATEMENT OF UNAUTHORIZED DEBIT

The sample on the preceding page is intended as a guide for developing a written statement form that is as easy as practicable for an RDFI and its customer to complete.

In Section 1, the statement must show the customer's name, account number, the amount of the debit, the date the debit posted to the customer's account, and the identity of the party debiting the account. For the purpose of completing the statement, the date of the debit and the party debiting the account can be identical to the information that is provided to the customer via a paper or electronic account statement.

In Section 2, the customer must state the reason the debit is unauthorized, to the best of his or her ability. A reason must be provided in this section in order for this form to be considered complete. The reasons offered on this sample generally correspond to the reasons provided in the Nacha Operating Rules as to why a debit would be considered unauthorized, but a selection for "Other" is offered as well. If "Other" is selected, additional information must be included in the space shown.

In Section 3, the form must be dated and signed by the customer. The date must be on or after the date of the debit as indicated in Section 1.

An RDFI may obtain a consumer's Written Statement of Unauthorized Debit as an electronic record and may accept a consumer's electronic signature, regardless of the form or method used to obtain it. Written Statements of Unauthorized Debits may be obtained and signed using the same methods permissible for obtaining a consumer debit authorization.

RDFIs can use other formats for a Written Statement of Unauthorized Debit, but the statement must meet the minimum information requirements of the new rule.

An RDFI may document more than one unauthorized debit Entry from a single Originator on a Written Statement of Unauthorized Debit, provided that all of the information detailed above is provided for each debit Entry for which the Receiver is seeking recredit.

An RDFI may also use a single form to document both unauthorized debits and stop payment orders. As long as such a form meets the minimum information requirements, it would be considered a valid Written Statement of Unauthorized Debit.