FIRST HORIZON BANK

Understanding ACH:

An Originator's Compliance Responsibilities

All ACH Originators are required to obtain a current copy of the National Automated Clearing House Association Operating Rules and Guidelines (the "Nacha Rules") that are published annually. A copy of the Nacha Rules book may be purchased at www.nacha.org or through the Southern Financial Exchange at sfe.org, a payments association that First Horizon is a member of which.

This Understanding ACH document provides a brief overview of ACH transactions and summary of certain obligations of ACH Originators under the Nacha Rules. It is merely a reference guide to help you navigate the Nacha Rules. It is not intended to be a replacement or substitution for the Nacha Rules, which are subject to change.

REV 01/26

Table of Contents

Overview

The ACH Network, which provides for the interbank clearing of electronic payments, is governed by the Nacha Operating Rules and Guidelines (the "Nacha Rules"). The Nacha Rules apply to all entries and entry data transmitted through the ACH Network. As an ACH Originator or Third-Party Sender, you must comply with and are bound by the Nacha Rules. To ensure compliance, all ACH Originators must have access to a current copy of the Nacha Rules. First Horizon customers can obtain a recent copy of the Nacha Rules or register for educational classes at the Southern Financial Exchange. Visit www.sfe.org for details. The National Automated Clearing House Association provides various resources as well.

The purpose of this document is to provide a summary of certain ACH facts and ACH Originator/Third-Party Sender Responsibilities. It is not a replacement or substitution for the Nacha Rules, which are subject to change. Notes have been inserted to guide you to the appropriate section of the Nacha Rules where you can obtain additional information.

ACH Facts

- All ACH transactions fall into two broad categories: ACH credits such as payroll, expense reimbursement, accounts payable and tax payments move funds from your account to credit the Receiver's account. ACH debits are used for collection of account's receivables such as insurance payments, utility bills, dues or subscription payments to debit the Receiver's account.
- ACH is a batch system (not real time).
- All ACH entries are irrevocable once they have been sent for processing.

Key Participants

Note: An overview of the ACH Network is available in Section 1 of the Guidelines, which describes the participants in greater detail.

Originator – The Originator is the party that has a relationship with the Receiver and has obtained an authorization from the Receiver to initiate a transaction affecting the Receiver's account. All Originators are required under Nacha Rules to keep a copy or recording of the authorization for two years following the termination or revocation of the authorization.

ODFI – Originating Depository Financial Institution, such as First Horizon, that receives the payment instructions from the Originator and submits the entries into the ACH Network.

ACH Operator – An ACH Operator acts as a clearinghouse between financial institutions by receiving, sorting and distributing ACH transactions. First Horizon submits ACH entries to the Federal Reserve.

RDFI – Receiving Depository Financial Institution, such as a bank or credit union that receives the payment instructions from the ACH Operator and posts the transactions to the

Receiver's account.

Receiver – The business or consumer that has authorized the transaction affecting the Receiver's account.

Third-Party Service Provider – In some instances, an originator, ODFI, RDFI or another third party may choose to use the services of a third party for all or part of the process of handling ACH entries. Payroll processing companies and property management companies that process for homeowner associations are common examples of Third-Party Service Providers.

Third-Party Senders – A Third-Party Service Provider can take on the role of a Third-Party Sender when they function as an intermediary between the Originator and the ODFI. A Third-Party Sender situation exists when there is not a direct ACH Origination Agreement between the ODFI and the Originator. A Third-Party Sender is never the Originator for entries it submits on behalf of another organization, but it can be an Originator for entries in its own right.

Nested Third-Party Senders – Third-Party Senders can also provide services for other Third-Party Senders. When this occurs, Nacha refers to this situation as Nested Third-Party Senders. Third-Party Senders are required to have an ACH Origination Agreement with Nested Third-Party Senders that requires them to obtain ACH Origination Agreements with the Originator that binds them to the Nacha Rules.

Authorization Requirements

Note: Authorization requirements are described in greater detail within Section 2.3 of the Nacha Rules; below is only a high-level summary of key facts. Also see Section 1.15 of the Nacha Rules regarding Limitation of Claims Based on Unauthorized Entries.

Originators are responsible to obtain proper Authorizations based on transaction type, and retain Authorizations for two years past termination or revocation.

ACH Credit Consumer Authorizations
Use a direct deposit authorization form that collects information for payroll, expense reimbursements or other applications that send funds to a consumer. PPD is the Standard Entry Class Code for these types of entries.

ACH Debit Consumer Debit Authorizations
In September of 2021, Nacha updated the Nacha Rules to standardize authorization requirements to consumer accounts across all Standard Entry Class Codes. Originators are obligated under the Nacha Rules to obtain valid authorizations from the Receiver. Authorizations to debit a consumer account must include at a minimum:

- Language regarding whether the authorization is for a Single, Recurring (regular basis such as weekly, monthly, quarterly or annually) or one or more Subsequent Entries under the terms of a Standing Authorization.
- The amount of the Entry(ies) or a reference to the method of determining the amount of the Entry(ies).
- The timing (including start date), number or frequency of the entries.
- The Receiver's name or identity.
- The account to be debited (this includes if the account is a checking or savings account type).
- The date of the Receiver's authorization.
- Language that instructs the Receiver on how to revoke the authorization (including the time and manner in which the Receiver's communication must occur). For Single Entry scheduled in advance, the right to revoke must afford the Originator a reasonable opportunity to act on the revocation prior to initiating the Entry.
- Optionally, the authorization may also contain:
  The ability to initiate credit Entry(ies) as necessary to correct an erroneous Debit Entry.

On recurring transactions (consistent or variable amount), if the scheduled date for the debit to be received changes, the Originator must notify the Receiver of the new schedule in writing at least seven (7) calendar days before the Entry is received.

Sample authorizations can be found in Appendixes F & G of the Nacha Operating Guidelines and are also available from First Horizon (ACH Credit Authorization Sample, ACH Debit Authorization Sample). While authorization requirements for business-to-business transactions are not as clearly defined within the Nacha Rules, First Horizon recommends that businesses model authorizations after consumer requirements.

Standing Authorizations

Standing Authorizations were also added to the Nacha Rules in 2021. This change was intended to support emerging technologies to allow a hybrid option between Single Entry and recurring transactions. This fills the gap to enable more flexible payment arrangements between businesses and consumers. Under a standing authorization, some components of the authorization are collected in advance, but the authorization is only completed via a subsequent action. The subsequent action determines the relevant SEC Code to be used on the transaction. Please note that the above Authorization Requirements are still required and must be available (both the initial authorization and the subsequent action to complete the authorization process) when requested by an RDFI.

Effective in June 2021, Nacha implemented a rule to provide limitations on warranty claims. For an entry to a non-consumer account, the warranty time frame is one year from the settlement date of the entry. For consumer accounts, the limitation includes two time frames: (1) An RDFI may make a claim up to two years after the settlement date of the entry, and (2) an RDFI may make a claim for entries posted within 95 calendar days from the first settlement date.

Authorizations for Variable Amount Debits
It is acceptable in certain situations to originate a variable amount recurring debit Entry. For example, utility bills frequently change in amount monthly, and an ACH Debit Entry can be used to collect these bills. The Originator can choose to provide the Receiver with a range. If the Receiver agrees, and the amount falls within the accepted range, the authorization is acceptable. However, when a range has not been established and the amount varies monthly or the amount is outside the agreed range, the Originator must send the Receiver a notice of the new payment amount at least ten (10) calendar days prior to date the debit is sent.

Authorizations and Check Conversion
In the case of ARC, BOC, POP and RCK, a notification can substitute for an Authorization. Please reference the Nacha Rules regarding each Standard Entry Class Code for additional information.

Warranty Claims
Most breach of warranty claims related to ACH transactions tend to be regarding proper authorization. Effective in June 2021, Nacha implemented a rule to provide limitations on warranty claims. For an entry to a non-consumer account, the warranty time frame is one year from the settlement date of the entry. For consumer accounts, the limitation includes two time frames: (1) An RDFI may make a claim up to two years after the settlement date of the entry, and (2) an RDFI may make a claim for entries posted within 95 calendar days from the first settlement date.

Same Day ACH

Note: Format requirements for Same Day entries are defined in Appendix Three of the Nacha Rules, and processing requirements are discussed in Chapter 25 of the Guidelines.

First Horizon offers Same Day ACH as an option to our business clients. To be eligible for Same Day ACH, origination files must contain today's date as the effective date in the file, and files must be submitted prior to processing windows. The per transaction limit is $1,000,000. Any batch submitted with an invalid or stale (in the past) effective date will be processed as a Same Day ACH Entry.

All entries received (either incoming or outgoing) will be posted on an intraday basis. The Same Day ACH cutoff time is 3:00 p.m. ET for online and 3:45 p.m. ET for direct transmission.

Risks of ACH Origination

Note: Information below is intended to provide some background regarding risks of ACH Origination. Third-Party Senders are required to conduct an ACH Risk Assessment under the Nacha Rules, and Originators are required to have policies and procedures in place to manage risks.

Operational Risk
ACH Originators like your company need to implement procedures to limit operational risk. This can occur when files are not submitted on time, due to a software or hardware failure, power or communication outage, inadequately trained staff, failure to develop, test or follow contingency plans, processing without dual control or failure to follow audit and balancing procedures. Submitting the wrong payroll file can be expensive and embarrassing to correct.

Origination Fraud
Origination fraud is a challenge for both financial institutions and ACH Originators. In one origination system hacking scheme, perpetrators hack into the Originator's computer system using compromised user IDs and passwords and originate ACH credits to "mule" accounts created for the express purpose of committing fraud. Those accounts are then emptied and abandoned. The credits are usually irretrievable by the time the fraud is discovered. The Originator's credentials may have been compromised by an insider within the organization or stolen through key loggers or Trojan Horse programs on the compromised computer.

Due to the risk of this type of fraud, it is essential that all computer equipment used by your company to access First Horizon is regularly updated and patched for security vulnerabilities (including the use of and updating of firewall, virus protection, anti-malware protection or anti-spam protection.) You may also want to consider having one computer in your office that is not used to browse the internet or read email to be your sole source of access to First Horizon's system. Limiting access to the computer that is used to house and transmit ACH data may help avoid the accidental downloading of harmful programs/viruses that could potentially compromise your transactions.

Appropriate steps should be taken within your company to ensure that all user IDs, passwords, authentication methods, and any other applicable security procedures issued to your employees are protected and kept confidential. All staff should be aware of the need for proper user security, password controls and separation of duties. As ACH Origination is a higher-risk commercial banking function, we suggest that your company perform your own internal risk assessment and controls evaluation periodically to be sure you are considering all available security options.

Credit Fraud
Credit fraud can also occur when an employee of the Originator intentionally misdirects payments or alters transactional data. This type of fraud is often caught after the fact when it is too late to recover the funds.

Compliance Risk
Compliance risk can occur when the Originator fails to comply with the Nacha Rules and regulations regarding ACH transactions. The Originator will be held liable for all fines and penalties.

Respond to Requests

First Horizon is obligated to provide information when requested by Nacha in various situations. As a result, Originators and Third-Party Senders are also required to respond to requests for information (when received) from First Horizon.

Note: Appendix 9 – Rules Enforcement addresses situations regarding Nacha Rules Violations and Fines, which addresses most reporting requirements. See Section 2.3 of the Nacha Rules for additional detail regarding authorization requests.

Return Rates
The Nacha Rules are updated from time to time to maintain an elevated level of quality and security within the ACH Network. Quality of the ACH Network is often measured based on return item levels and exceptions that require manual processing. First Horizon is required to provide information to Nacha within ten (10) Banking Days for each Originator or Third-Party Sender after receiving a request from Nacha. These requests are triggered when established Return Rate levels are exceeded by the Originator and become a concern.

- *0.5% Unauthorized Return Rate (includes R05, R07, R10, R11, R29 and R51)*
- *3% Administrative or account data errors (includes R02, R03 and R04)*
- *15% Overall Return Rate (excludes RCK returns)*

First Horizon will need a statement explaining the reason for exceeding the Return Rate level and a detailed plan and timeline for reducing the Originator's or Third-Party Sender's Return Rate to a rate below the established level. Nacha will also require a description of the nature of the business and methods used to obtain proper authorizations for ACH transactions.

Third-Party Senders
Nacha requires each ODFI to report information on Third-Party Senders and Nested Third-Party Senders. Should Nacha believe that the Third-Party Sender represents escalated risk, First Horizon is required to provide additional information about the Third-Party Sender.

Authorizations
RDFIs are allowed under the Nacha Rules to request proof of authorization (copy of written authorization or other accurate record). Such proof must be returned to RDFI within ten (10) banking days. However, to reduce costs and improve efficiency. an Originator/Third-Party Sender may accept the return of the debit rather than provide proof. Written confirmation that the Originator/Third Party has agreed to accept the return of the Entry must be received within ten (10) banking days. If the RDFI makes a second request to provide proof, it must be provided within ten (10) banking days of the subsequent request.

Company Name Field

Note: Refer to Appendix 3 of the Nacha Rules, which describes each field used in a Nacha formatted file. Below is The Company Name field in the Formal Rules Interpretations section before the Nacha Rules.

The Company Name field used by the Originator should be known and readily recognized by the Receiver of the transaction. For example, your commonly known name found in advertisements or on signage should be used.

Prenotifications

Note: Refer to Section 2.6 of the Nacha Rules for additional information regarding prenotifications.

Prenotification Entries (or "Prenotes") are zero-dollar entries frequently used to validate the financial information provided to the Originator. This is an option that can ensure that the first live posting occurs accurately and in a timely manner. An Originator using a Prenotification Entry must wait three (3) banking days following the settlement date of the Prenotification Entry prior to submitting a live (dollar) Entry. The RDFI is then only required to validate the account number (not the name on the account). The RDFI is responsible to provide a return notification if the financial information (routing number or account number) is incorrect. The RDFI will not provide a positive confirmation that transactions were processed successfully (no news = good news).

- ACH entries are posted to the Receiver's account based on routing and account number information only. The receiving bank is not required to verify the name, individual identification or other information provided in the Entry.
- It is the responsibility of the Originator to verify that the individual authorizing the Entry is in fact the owner of the account. The method to authenticate the identity of the Receiver varies according to Standard Entry Code.

If a prenotification is returned, the Originator is responsible to correct the reason for the return. Upon receipt of returns relating to prenotifications indicating that the RDFI cannot accept such entries, such entries cannot be initiated.

Returns

Note: See Appendix 4 of the Nacha Rules, which provides a complete listing of all return reason codes as well as record formats.

A large number of return reason codes exist within the Nacha Rules. This exists to provide as accurate information as possible back to the Originator regarding the reason for the return. However, the RDFI is allowed to use an approximate Return Reason Code. With some exceptions allowed in the Nacha Rules, returns must be received by opening of

business on the second banking day following the original settlement date.

Unauthorized Returns – A RDFI may be returned so that it is available to the ODFI no later than opening of business on the banking day following the sixtieth calendar day following the original settlement date. For unauthorized transactions related to a consumer, the consumer is required to provide the RDFI a Written Statement of Unauthorized Debit that identifies the item as being unauthorized. Unauthorized Return Reason Codes include:

R05 – Unauthorized debit to a Consumer account using a Corporate SEC Code.
R07 – Authorization revoked by Consumer.
R10 – Customer advising Originator is not known to Receiver and/or Originator is not authorized.
R11 – Customer advises authorization is not in accordance with term of authorization.
R29 – Corporate Customer advises not authorized.
R51 – RCK Entry is ineligible or RCK Entry is improper.

Extended Return Time Frames – An RDFI can also submit an Extended Return Entry so that it is available to the ODFI no later than opening of business on the banking day following the sixtieth calendar day following the original settlement date for the following Return Reason Codes:

R33 – Return of an XCK Entry.
R37 – Source document presented for payment.
R38 – Stop payment on source document.
R52 – Stop payment on an RCK Entry.
R53 – Item and RCK Entry presented for payment.

Clients of First Horizon can request the bank to automatically represent return items that are received with a return code of "R01 Insufficient Funds" or "R09 Uncollected Funds." This feature only returns items automatically within 180 days of the original settlement date of the Entry.

Other common Return Reason Codes:

R07, R08 (Payment Stopped) & R10 – An Originator is not allowed to reinitiate an Entry unless a subsequent authorization has been obtained.
R05 – An Originator is not allowed to reinitiate an Entry unless a subsequent authorization has been obtained and the SEC has been corrected.
R11 – An Originator may correct the defect or error and transmit a new Entry without obtaining a new authorization. However, a new Entry is not allowed (1) if the Originator did not provide the required notice for an ARC, BOC or POP Entry or (2) the source document was not eligible for check conversion.

Originators are prohibited from sending live entries when a prenote return indicates the RDFI cannot accept such entries.

Reporting
First Horizon has an automated process in place to send information via email for:

- Originated items that are returned by the RDFI.
- Notifications of Change that are received from the RDFI.
- Rejected Origination Items – items that may fail due to formatting or other issues.

Reversals

See Section 2.9 of the Nacha Rules for details regarding Reversal Entries.

When the Originator recognizes that an error has been made on a file that has been sent to the bank, two options exist. If the file has not yet been processed by First Horizon, the file can be deleted and a new file submitted. If the file has been processed, a reversing file, batch or Entry can be made to correct the error. Requests for deletion or reversals must be made in writing by an authorized signer on the settlement account at First Horizon. Contact the Business Service Center (888-382-4968) to obtain the correct form. Requests to reverse files, batches or Entries must be made within five (5) banking days following the settlement date of the erroneous Entry or file and within twenty-four (24) hours of the discovery of the error. The Originator is responsible to notify the Receiver before the reversing Entry is passed to the Receiver's account.

When a reversal is requested, the Originator takes on additional risk. For example, if the original Entry was a credit, it is possible that the Receiver may have withdrawn funds from the account prior to the reversal (debit) Entry is passed to the Receiver's account. If the funds are not available to pay the Debit Entry, the reversal will be charged back to the Originator's account. If the original Entry was a debit transaction, it is possible that the debit transaction may be returned as insufficient, prior to reversal (credit) reaching the Receiver's account. Frequently, it takes time and effort outside the ACH Network to clean up problems created by files containing errors.

The Originator must notify the Receiver before the reversing Entry settles to the Receiver's account. The Entry must be properly formatted with the term "REVERSAL" in the Company Entry Description field of the Company/Batch Header Record. The Company ID/Originator ID, SEC Code and Amount fields of the Reversing Entry must be identical to the original Entry. The name of the Originator must reflect the same Originator identified in the Erroneous Entry to which the Reversal relates. (Minor variations to the Originator's name will be permissible for accounting or tracking purposes if the name remains readily recognizable to the Receiver.) The contents of other fields may be modified only to the extent necessary to facilitate proper processing of the reversal. A Debit Reversing Entry must not contain an Effective Entry Date that is earlier than the Effective Entry Date of the credit Entry to which it relates. A reversal can only be initiated for erroneous entries as defined in the Nacha Rules. The initiation of Reversing Entries or Files for any reason other than those explicitly permissible under the Nacha Rules is prohibited. The RDFI is permitted to return an improper reversal.

Notifications of Change (NOCs)

Note: See Section 2.12 of the Nacha Rules for greater detail regarding Notifications of Change. A complete list of NOC Codes is available in Appendix 5.

In some instances, the receiving bank will process an Entry that contains inaccurate information. When this happens, the receiving bank may send a Notification of Change (NOC) to the originating bank (First Horizon).

Notifications of Change can be sent for a variety of reasons. The most common NOC Codes are:

C01 – Account number is incorrect or is formatted incorrectly.
C02 – Due to a merger or consolidation, a once valid routing number must be changed.
C03 – Customer has changed name.
C06 – Transaction code is incorrect (savings or checking).

When this occurs, First Horizon will provide a report to the Originator that contains both NOC information with any return item entries that are received. The Originator is required to make the correction within six (6) banking days or prior to the initiation of the next Entry.

Data Security Management

Note: See Section 1.6 of the Nacha Rules and Chapter 4 of Guidelines (General Rules) for additional information regarding Risk Assessments, Record Retention, ACH Data Security, Transmission of Data via Unsecured Electronic Networks and Secured Storage of Source Documents and Other Sensitive Data.

Originators, Third-Party Service Providers and Third-Party Senders are contractually obligated to establish, implement and update security policies, procedures and systems related to the initiation, processing and storage of entries. All Originators and Third-Party Service Providers and Third-Party Senders originating more than two million ACH Entries annually must protect DFI account numbers by rendering them unreadable when stored electronically.

This security framework is aimed to protect the security and integrity of certain ACH data throughout its life cycle. These policies and procedures should be designed to protect:

- The confidentiality and integrity of Protected Information (financial and sensitive non-financial information) until destruction.
- Against anticipated threats or hazards to the security or integrity of Protected Information until its destruction.
- Against unauthorized use of Protected Information that could result in substantial harm to a natural person.

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

Originators are also required to perform periodic self-assessment exams ensuring that they are in full compliance with required standards.

First Horizon may conduct audits of the Originator to ensure compliance with these requirements.

Third-Party Senders

Note: While information on Third-Party Senders can be found in many locations throughout the Nacha Rules and Guidelines, Chapter 50 of Guidelines, Appendix C and Appendix N are excellent references for additional information.

Third-Party Senders take on all warranties of an ODFI for the Nested Third-Party Senders and Originators that they agree to process on behalf of. While the use of a third party can offer benefits, the use of a third party may also elevate risks, including operational, compliance and strategic risks. First Horizon has developed the list below to ensure that activities are performed in a safe and sound manner and compliant with the Nacha Rules when setting up ACH Origination services for their clients. Contractual ACH Origination agreements must be established between the Third-Party Sender and Nested Third-Party Senders and their Originators that includes but is not limited to:

- The Third-Party Sender and Nested Third-Party Senders must ensure that their Originators are obtaining Authorizations from the Receiver that are consistent with Authorization requirements within Nacha Rules. An Originator must retain the original or copy of the authorization for two years from the revocation or termination of the authorization and be able to provide proof of authorization within an acceptable time frame for First Horizon to comply with Nacha Rules.
- The Third-Party Sender must agree that, before permitting a Nested Third-Party Sender to originate any Entry directly or indirectly through itself or First Horizon, it will enter into an agreement with the Nested Third-Party Sender that satisfies the requirements of Nacha Rules.
- The Third-Party Sender and Nested Third-Party Senders must agree that, before permitting an Originator to originate any Entry directly or indirectly through itself or the ODFI, it will enter into an agreement with the Originator that satisfies the requirements of Nacha Rules.
- The Third-Party Sender and Nested Third-Party Senders and their Originators must be bound to Nacha Rules.
- The Third-Party Sender and Nested Third-Party Senders must authorize First Horizon as the ODFI to originate entries on behalf of the Originator to Receiver's accounts.
- Third-Party Sender and Nested Third-Party Sender and their Originators agree not

to originate entries that violate the laws of the United States.

- Third-Party Sender and Nested Third-Party Senders must include any restrictions on the types of Entries that may be originated.
- The right of First Horizon to suspend or terminate the agreement or any Originator or Nested Third-Party Sender for breach of Nacha Rules.
- The right of First Horizon to audit compliance with the Treasury Management Services Master Agreement and the Nacha Rules by the Nested Third-Party Sender, any further Nested Third-Party Senders, and their respective Originators.
- Establishing and monitoring Originators' exposure limits.
- Conducting adequate due diligence for Nested Third-Party Senders and Originators consistent with unsecured credit exposures based on the above exposure limits with periodic review (no less than annually).
- Third-Party Sender and Nested Third-Party Senders agree to provide information to First Horizon in order to comply with Third-Party Sender registration on Nacha's Risk Management Portal and other requests for information.

Transmission of Data via Unsecured Electronic Networks (includes the Internet)

Note: See Section 1.7 of the Nacha Rules or Chapter 4 of Guidelines for additional information on this topic.

For all ACH transactions that involve the exchange or transmission of banking information (which includes, but is not limited to, an Entry, Entry data, routing number, account number and a PIN or other identification symbol) via an Unsecured Electronic Network, the Rules require that such banking information be either:

- encrypted communications using a commercially reasonable security technology that complies with current applicable regulatory guidelines, or
- transmitted via secure session using a commercially reasonable security technology that complies with current applicable regulatory guidelines.

Transmissions or exchanges of banking information over an Unsecured Electronic Network by means of voice or keypad inputs from a wireline or wireless telephone to a live operator or voice response unit are not subject to this data security requirement.

Business Reclamations

Note: See Chapter 12 (Reclamations for Benefit Payments) in Guidelines for additional information.

A reclamation entry is a Debit Entry initiated by the Originator to reclaim from the RDFI any amount received by a Recipient after death or legal incapacity of a Recipient. These are used for pension; annuities are other benefit payments and may be initiated if the Receiver is deceased and neither the Receiver's estate nor any other account holder is entitled to the

payment. The entry must be originated within five (5) banking days of the Originator learning of the death of the Receiver. Reclamation entries must contain:

- *the name of the Receiver.*
- *the deceased Receiver's account number.*
- *the exact amount of the entry being reclaimed (must be in an amount equal to or less than the original entry).*
- *the approximate date the entry being reclaimed was initiated.*
- *the word RECLAIM in the company Entry Description Field of the Company/Batch Header Record.*

Standard Entry Codes (SEC Codes)

Note: Section V (Chapters 36 – 49) of the Guidelines cover each of the Standard Entry Class Codes in detail. Below is simply a high-level summary of the most commonly used SEC Codes.

In general, Nacha uses Standard Entry Classes (SEC Codes) to designate the method by which an ACH Entry is authorized. The Nacha Rules regarding each SEC varies and Nacha monitors various statistics by Originator and SEC. If your company is interested in originating multiple SEC Codes, discuss this with your Relationship Manager or Treasury Management Sales Officer. Below is recap of information related to each SEC Code.

A. Consumer Applications

Originators that use the various SEC Codes must be sure to comply with the requirements associated with the particular application. Consumer SEC Codes with the highest levels of volume flowing through the ACH Network are PPD, WEB and TEL, so let us start with them.

1. ***Prearranged Payment and Deposit (PPD)***
   PPD can be used for credit or debit transactions. Most PPD transactions are authorized in writing in advance of the transactions. PPD is normally used for recurring transactions (consistent or variable amounts) such as payroll or direct debit. However, the Nacha Rules do not exclude the use of PPD for single Entry authorizations. PPD transactions can also be authorized under the standard of similar authentication, which allows the use of electronic signatures, digital signatures and security codes.

   Risks Unique to PPD

   Because the Nacha Rules allow digital authentication, ACH transactions can be accepted by Interactive Voice Response (IVR) or touch-tone systems and be processed under the PPD Standard Entry Class (SEC). This is frequently misunderstood by Originators who may try to use the TEL SEC in error.

   Unauthorized returns may be returned so that it is available to the ODFI no later

than opening of business on the banking day following the sixtieth calendar day following the original settlement date.

2. Internet Initiated/Mobile (WEB)

The Nacha Rules permit the internet or a mobile device to be used to authorize single or recurring debits to a consumer's account.

Sample Web Notification Language

Authorizations that are internet initiated must be displayed on a computer screen or other visual format in a clear manner. The consumer should be prompted to print and retain a copy of the authorization. The Originator must be able to provide a copy of the authorization if requested. Only the consumer can authorize a transaction, not a Third Party on behalf of the consumer. Use of a digital signature or code to similarly authenticate the written authorization is acceptable but does not preclude the other methods of authentication such as shared secret, passwords, biometrics, etc. The authentication method must demonstrate the consumer's assent to the authorization.

"On <today's date>, I <consumer name>, acknowledge that I am authorizing a <one time or recurring> electronic debit to my account for <amount>, which will be debited on or after <date>. My <checking or savings> account number is <insert account> and my bank's routing number is <insert routing>. For inquiries or to revoke this authorization, I can reach <retailer or biller> during normal business hours of <state hours> at <retailer or biller phone number>. Revocation is only possible to prevent the next recurring entry if provided < number of days> in advance of the payment date."

- *Language regarding whether the authorization is for a Single, Recurring (regular basis such as weekly, monthly, quarterly, or annually) or one or more Subsequent Entries under the terms of a Standing Authorization.*
- *The amount of the Entry(ies) or a reference to the method of determining the amount of the Entry(ies).*
- *The timing (including start date) and number or frequency of the entries.*
- *The Receiver's name or identity.*
- *The account to be debited (this includes if the account is a checking or savings account type).*
- *The date of the Receiver's authorization.*
- *Language that instructs the Receiver how to revoke the authorization (including the time and manner in which the Receiver's communication must occur). For Single Entry scheduled in advance, the right to revoke must afford the Originator a reasonable opportunity to act on the revocation prior to initiating the Entry.*

Optionally, the authorization may also contain:

- *The ability to initiate credit Entry(ies) as necessary to correct an erroneous Debit Entry.*

Authentication

The best way to minimize the potential for fraudulent internet/mobile transactions is to employ robust authentication methods to verify the identity of the Receiver before authorizing the Entry. The more robust the authentication process the less likely the transaction will be fraudulent. Since the Originator is held responsible for unauthorized or fraudulent transactions when they are returned, it is to the benefit of the Originator to incorporate adequate levels of authentication. While ID/Password are still the most common solution for online authentication, there is a growing trend toward replacing passwords with additional authentication factors or security layers.

Multifactor authentication uses multiple characteristics to determine a Receiver's identity. For example, verification of:

- *Something the Receiver knows (password, ID PIN)*
- *Something the Receiver has (internet ID)*
- *Something the Receiver is (voice or fingerprint)*

Fraudulent Detection Systems

Many debit web entries are Single-Entry payments, and Receivers frequently enter their account numbers manually. To minimize exception processing, each Originator is required to employ commercially reasonable procedures to verify that the routing numbers are valid. A decision not to deploy any method or procedure to detect transaction-level fraud and validate the account number is not considered commercially reasonable.

- *A fraudulent detection system must validate the account number to be debited upon the number's first use and for any subsequent changes to the account number.*
- *Verification of routing numbers – to minimize errors related to key Entry mistakes, each Originator is required to verify that routing numbers are valid. This can be considered a component of a fraudulent detection system.*
- *Security of internet sessions – does your system meet the Commercially Reasonable standard?*
- *The choice of other features is a decision made by each Originator. Examples of fraudulent detection systems are systems that ensure that the account is open and available for ACH processing, track payment history, behavior, purchase type, etc. Factors to consider include dollar size of the transaction, number of transactions processed, types of goods/services sold, and existing/new relationship with Receiver.*

Red flags that identify increased levels of risk include:

- *Large numbers of customers changing their routing number for payments.*
- *A significant increase in the use of a specific routing number over a brief period of time.*
- *Early payoff of a loan in conjunction with a change in the source of the payment.*
- *Atypically large-dollar funding of a new or existing account.*
- *Multiple payment attempts by the same individual.*
- *Overpayment of a bill or tax payment.*

Audit Data Security Audits

Annual data security audit requirements exist for all Originators of web transactions. The purpose of this audit is to ensure that Receivers' financial information is protected by security practices and procedures. While Nacha only requires an annual audit, an Originator with significant volume should consider biannual or even quarterly audits due to the rapid changes in technology and security risks. These audits can be a component of a comprehensive audit and conducted by external or internal independent auditors with a generally accepted security compliance program. Below are the minimum requirements:

1. Physical security to prevent 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 access controls to deter unauthorized access and use.

    - A formal set of security policies and procedures that clearly outline the corporate rules governing access to sensitive data.
    - Hiring procedures that, at a minimum, verify application information and check references on new employees that will have access to sensitive data.
    - Relevant employees must be educated on information security, 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 documents/files that contain Receiver financial information.

- Ensure 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 always accompanied by an employee.
- Authenticate access to any database containing sensitive ACH information such as financial information (e.g., passwords or pass phase, 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 – a separation of duties.
- Establish policies and procedures to monitor and audit all user activity for personnel with access to Receiver information 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 life cycle 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 any use of the internet or mobile device 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.

Risks Unique to the Web

There are three unique internet transaction characteristics that elevate risk levels.

- *Because of the anonymity of the internet, parties do not always know who they are doing business with, which increases the opportunity for fraud.*
- *Since the internet is an open network, special security procedures need to be in place to prevent unauthorized access to consumer financial information.*
- *The sheer volume and speed of transactions increases risk levels.*

Nacha Rules refrain from developing rigid standards that may become outdated easily due to technological changes in a rapidly changing environment. Terms such as "commercially reasonable" are used, which makes it more difficult to determine compliance.

3. Telephone-Initiated (TEL)

Nacha Rules enable an ACH Entry to be initiated in response to a consumer's oral authorization, which includes the consumer's banking information captured by telephone to transmit an ACH debit for goods or services. This authorization can be valid for a recurring or single-entry TEL transaction. TEL entries can only be created:

- *When there is an existing relationship between the Originator and the Receiver, or*
- *When there is not an existing relationship, but the Receiver has initiated the call.*

An existing relationship is defined:

- *As a written agreement being in place between the Originator and the Receiver, or*
- *By the consumer purchasing goods or services from the Originator in the past two years.*

Sample TEL Notification Language

The Receiver must be provided and acknowledge during the conversation the following terms of the transaction:

- *Date on or after which the consumer's account will be debited.*
- *The amount of the Debit Entry.*

- *The consumer's name: The account to be debited.*
- *A telephone number that is available during normal business hours for customer inquiries.*
- *The method by which the consumer can revoke the authorization.*
- *The date of the consumer's oral authorizations.*
- *A statement that the authorization obtained will be used to create a single ACH debit to the consumer's account.*

The above terms must be clearly stated, and Receiver must specifically acknowledge consent. Silence is not express consent.

Risks Unique to TEL
Nacha Rules were specifically written to exclude marketing to consumers through cold calling efforts. Violations of TEL rules normally result in high rates of unauthorized returns. ODFIs are required to provide Nacha with specific information related to Originators of TEL entries whose unauthorized return rates exceed 1.0%.

Originators of TEL are required to either record the consumer's oral authorization or provide in advance of the Settlement Date written confirmation addressing the above terms of the transaction to the Receiver. Authorization is evidenced by the recording or a copy of the confirmation.

Check Conversion Standard Entry Class Codes

The following SEC Codes are used when checks are converted into ACH Entries. Volumes of checks being used have been declining over time and as a result, the volume of ACH Entries using these SEC Codes are also in decline.

1. **Accounts Receivable Entries (ARC)**
   Nacha Rules enable an Originator to convert a check into an ACH debit. This process enables a single-entry debit, which is provided to the Originator via US mail or at a drop box location to be converted into an ACH debit for payment of goods or services. Notification must be provided for each conversion event prior to the receipt of each check, which explains that the check will be used as a basis for the origination of an ARC entry. Check can only be converted to ARC when a reading device electronically captures the MICR line. Authorization is provided by receipt of the signed check.

   Sample ARC Notification Language
   "When you provide a check as payment, you authorize us to use information from your check to make a one-time electronic fund transfer from your account. In certain circumstances, such as for technical or processing reasons, we may process your payment as a check transaction."

   The following checks are not eligible for ARC:
   - *Checks that do not contain a pre-printed serial number.*

- *Checks that do contain an auxiliary on-us field in the MICR line (auxiliary on-us fields are only found on larger, 9-inch check stock and are not present on smaller, consumer-sized 6-inch checks).*
- *Checks greater than $25,000.*
- *Third-party checks.*
- *Demand drafts or other checks that do not contain the signature of the Receiver.*
- *Checks provided by a lender for purposes of accessing a credit card account, home equity line or other form of credit.*
- *Obligations of financial institutions (cashier's checks, money orders, etc.).*
- *Checks drawn on the US Treasury, a Federal Reserve Bank, or a Federal Home Loan Bank.*
- *Checks drawn on a state or local government.*
- *Checks drawn on an investment company as defined by the Investment Company Act of 1940.*
- *Checks payable in a medium other than US currency.*

Risks Unique to ARC

ARC entries can be returned up until 60 days from the settlement date for the following reasons:

- *Improper source document (a Written Statement of Unauthorized Debit is required).*
- *No notice of conversion provided to the Receiver.*
- *If the original check was presented and cleared.*
- *The ARC transaction was initiated in an amount other than the amount indicated on the source document.*

First Horizon has enabled ARC through the Retail Lockbox processing platform. Vendor-supplied software converts the MICR line information into ARC transactions and houses the logic to recognize ineligible items.

2. Back Office Conversion (BOC)

BOC is used for single-entry debits to a customer account and would typically be used in a retail application such as a grocery store. Checks would be provided to the Originator by the Receiver at the point of purchase or at a staffed bill payment location. The store is required to provide notice that the check could be subject to processing as an electronic debit. Checks in this process are collected from the customer and converted through a back-office conversion process. The merchant will keep the check and is required to use a reading device to capture the MICR line. Authorization is provided by the combination of the notification sign and the signed check.

Sample BOC Notification Language

"When you provide a check as payment, you authorize us to 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. For inquiries,

please call <retailer phone number>."

The same checks that are not eligible for ARC are not eligible for BOC.

Risks Unique to BOC

BOC entries can be returned up until 60 days from the settlement date for the following reasons:

- *Improper source document (a Written Statement of Unauthorized Debit is required).*
- *No notice of conversion provided to the Receiver (BOC requires a copy of the notice to be provided at the time of the transaction).*
- *If the original check was presented and cleared.*
- *The BOC transaction was initiated in an amount other than the amount indicated on the source document.*

The business is required to:

- *Maintain source document images for a period of two years – the front image is required, and back image is optional (this should be controlled easily by our Remote Deposit Capture software when that is the tool used to create the BOC transaction).*
- *Store the converted check securely and to destroy it when necessary.*
- *Adequately verify the check presenter's identity through commercially reasonable means.*

3. Point of Purchase (POP)

The POP SEC is used by Originators as a method of payment for in-person purchase of goods and services. Checks can be accepted at the point of sale and then scanned to capture the MICR line, voided and handed back to the customer. The scanned MICR line is used to initiate an ACH Entry to debit the customer's account. These entries are also single-entry debits, requiring that the consumer sign an authorization at the time of purchase.

Sample POP Notification Language

"When you provide a check as payment, you authorize us to 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."

Risks Unique to POP

- *POP entries have the same exclusion of items that are addressed earlier under ARC.*
- *The Originator must ensure ineligible items are not submitted.*
- *Because the check is not retained, the Originator must take additional steps to capture information in case the check is returned.*
- *POP entries can be used for corporate checks only if the check does not contain an auxiliary on-us field in the MICR line.*

4. **Re-Presented Check Entries (RCK)**
   Nacha Rules permit the ACH network to be used to transmit a single-entry debit transaction to re-present electronically after a paper check has been returned for insufficient or uncollected funds. These entries are subject to UCC, Regulation CC and Nacha Rules, but are not covered under Regulation E or the Electronic Funds Transfer Act. Items are only eligible if:
   - *Under $2,500*
   - *Contain a pre-printed serial number.*
   - *Negotiable items drawn on an ACH participating bank other than the Federal Reserve Bank or the Federal Home Loan Bank.*
   - *Payable in US dollars.*
   - *Items that include the signature of the Receiver.*
   - *Returned for insufficient or uncollectible funds and this is clearly indicated on the face of the item.*
   - *Dated 180 days or less from the date of entry transmitted to the RDFI.*
   - *Drawn on a consumer account.*
   - *Not presented more than a total of three times: 1 paper and 2 electronic or 2 paper and 1 electronic.*
   - *Items cannot be a US Postal Service money order.*
   - *Items cannot be a third-party check.*

Sample RCK Notification Language

The manner for providing notification for RCK is not specific; however, notice at a point of sale must be clearly displayed. Notice provided by a billing company of intent to collect a return check electronically must be clearly displayed on or with the billing statement. Fees related to return check collection must be authorized separately under WEB, PPD or TEL Rules and cannot be included with the face amount of the returned item.

"When you provide a check as payment, if the check is returned for insufficient or uncollected funds, your check may be collected electronically."

Risks Unique to RCK

- By the nature of these items, return rates will be high. This is reflected in both normal returns and in unauthorized returns.
- Notice of possible conversion can be displayed at the point of check acceptance stating if the check is returned for NSF or uncollected funds that it may be collected electronically. The consumer does not always recall that notice was provided, and this results in higher unauthorized returns since actual conversion to ACH is delayed.

B. Corporate Applications

Corporate entries are limited to two standard entry classes, CCD and CTX.

1. Corporate Credit or Debit (CCD)

- This is the most commonly used corporate entry. This can be used for either debit or credit transactions to distribute or collect between corporate entities. Tax payments also use this standard entry class for federal and state payments.

2. Corporate Trade Exchange (CTX)

- This is used to move funds and information related to the payments. This transaction supports up to 9,999 addenda records to communicate ANSI ASC X12 message sets or UN/EDIFACT information.

Risks Unique to Cash Concentration

In general, corporate transactions carry additional risk issues when used for Cash Concentration. Cash Concentration is the consolidation of funds from multiple financial institutions where the accounts at each financial institution are all owned by the corporate entity. Since deposited funds are available to the corporate entity on the effective date of the transaction, it is possible for the corporate entity to withdraw funds, and then declare bankruptcy. If this sequence of events should occur, the ACH debit entries presented to the receiving financial institution are likely to be returned and First Horizon would have unsecured credit exposure.

Timing of Returns

- Most entries will need to be returned by the RDFI so that the return entry is available to the ODFI no later than the opening of business on the second business day following the original settlement date of the transaction.
- For the Receiver of CCD or CTX transactions, this shorter return time frame requires daily reconciliation to recognize and return unauthorized or other ACH debits in a timely manner. Originators are held liable under the First Horizon Treasury Management Services Master Agreement and ACH Service Description for any breach of warranty (which includes, but is not limited to, any breach of warranty regarding proper authorization).