WEB ACH Primer

The WEB ACH transaction type was introduced in March 2001. It is defined as a debit entry to a consumer bank account, for which the authorization was obtained from the Receiver (the consumer who owns the bank account) over the Internet. The specific designation for these types of transactions was created in order to address unique risks inherent to Internet payments. WEB entries require additional security procedures and obligations that address these risks.

Definitions Applicable to Web-Based Student Fee Payments at UC

Originator – UC or a 3rd Party Service Provider creating the ACH debits

Receiver – The person (for WEB transactions this must be a human being) who owns the bank account being debited.

ODFI – Originating Depository Financial Institution. UC’s or the 3rd Party’s bank.


PPD – Prearranged Payment and Deposit entry. An ACH debit or credit to a consumer bank account.

WEB – An ACH debit to a consumer account for which the authorization was provided via the Internet

Authorization - For debit entries to consumer accounts, the authorization must be in writing and signed or similarly authenticated by the consumer. Written authorization can be provided electronically if the writing and signature requirements comply with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. §7001 et seq.) which defines electronic records and electronic signatures. Generally speaking, this means that the authorization must be presented on a screen and in a form that can printed. Electronic signatures include, but are not limited to, digital signatures, PIN, password, shared secret, security codes, or a hard copy record may be authenticated via the telephone by the consumer’s speaking or key-entering a code provided on the record. The authorization process must evidence both the consumer’s identity and his assent to the authorization. The authorization must be clearly identifiable as an authorization, must clearly and conspicuously state its terms, and (with few exceptions) must provide that the Receiver may revoke the authorization only by notifying the Originator in the manner specified in the authorization. It is important to note that authentication and authorization must occur simultaneously. It is not acceptable to have identified a consumer at log-in of a session, then later consider that initial log-in as authentication for the purposes of authorizing an ACH debit. It is also not acceptable to authenticate an authorization simply by a click-through process. The authorization must be retained, in either physical or electronic form, for two years following the termination or revocation of the authorization. The authorization must be reproducible.
WEB ACH Primer

Prenotification – Prior to initiation of the first entry to a Receiver, an Originator may, at its option, send this type of transaction to “test” the routing of the ACH. “Live” entries can be initiated no sooner than six banking days following the settlement date of the prenote.

Facts about WEB transactions

- Only applies to consumer debits (only exception is a credit entry that is reversing a debit)
- Defined by a transaction for which authorization for the debit was given over the internet
- Can be used for both one-time and recurring debits
- UC must use commercially reasonable procedures for:
  - Verifying the validity of routing numbers
    - While there are databases and other tools available to assist in the validation of ABA routing numbers, the ability to validate an account number is very limited. Some databases/services might be able to validate the format of a particular bank’s account number string, but these would be considered premium services.
    - Banks are not required to confirm that the account number and account name within an ACH transaction record match. Therefore the liability for misrouted or fraudulent transactions sent to the wrong account number falls on UC, as the Originator.
    - There are certain financial institutions that use different routing information for ACH transactions versus checks. Relying on the check MICR line information alone will not be successful for ACH transactions routed to these financial institutions. Sometimes the ACH routing is printed on the face of the check, but this is not a requirement.
  - Security of the Internet session equivalent to 128-bit encryption must be used from the point that the Receiver key enters their banking information through transmission of the data to the Originator
- UC must conduct, or have conducted annual audits to ensure that the financial information it obtains from Receivers is protected by adequate security practices and procedures.
- Availability of funds in the account cannot be determined before initiation of the ACH debit.

Facts about Consumer Debit Authorizations

- Authorization must come from the owner of the bank account (the Receiver)
- The Receiver must be authenticated electronically at the same time authorization is given. It is not adequate to only authenticate the consumer at the time of log-on to the system. The consumer must be authenticated again at the time of authorization as well (e.g. password, PIN, shared secret etc. must be provided again).
- Authorization must be retained for two years following the termination or revocation of the authorization. Authorization must be stored in a reproducible form.
- For multiple, non-recurring debits, where the amount and time frame for the initiation of debits may vary, written authorization is not required for each debit as long as the written authorization establishes up front the relationship between the Originator (UC) and the Receiver (the student or payer).
WEB ACH Primer

- If authorization for an ACH consumer debit is given over the Internet, the transaction is deemed a WEB transaction. If authorization is done via signed hard copy authorization, but the initiation method is web-based, the transaction is not a WEB entry. Rather, it is a PPD (Prearranged Payment and Deposit) debit entry.

Other Important Things to Know About Consumer Debit Transactions (WEB or PPD)

- If an ACH debit is returned due to non-sufficient or uncollected funds in the Receiver’s account, the return should be posted to the ODFI (UC’s bank) by the second banking day after settlement (The ACH Rules define when Settlement occurs. The earliest Settlement can occur is one business day after Initiation, however due to ACH system cut-off times and banking holidays, Settlement may occur after the stated Settlement date in the ACH record).
- A consumer has up to 15 days after receipt of their bank statement to notify their bank in writing of an unauthorized ACH debit. The RDFI has up to 60 calendar days after the settlement date of the original debit transaction to return the debit to the ODFI.
- Banks have the right to post funds presented through the ACH network based on the account number alone. There is no requirement that an RDFI verify the name on the account matches the name on the ACH transaction.
- UC, as the Originator, is liable for erroneous and fraudulent ACH activity. This includes erroneous or fraudulent debits that may occur as a result of a customer/student/employee providing fraudulent bank routing information.

WEB ACH versus Web Credit Card Transactions

<table>
<thead>
<tr>
<th></th>
<th>WEB Credit Card Sale</th>
<th>WEB ACH Sale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validity of Credit</td>
<td>Real-time Authorization given by the Credit Card Network (using a Credit Card</td>
<td>ABA Databases and verification services increase the likelihood that the</td>
</tr>
<tr>
<td>or ACH Routing</td>
<td>Gateway) confirms that the credit card number is valid</td>
<td>Bank ABA number is valid. Account number validation is not generally</td>
</tr>
<tr>
<td>Information</td>
<td></td>
<td>confirmed.</td>
</tr>
<tr>
<td>Availability of</td>
<td>Real-time Authorization given by the Credit Card Network (using a Credit Card</td>
<td>No ability to confirm the availability of funds at the time of initiation</td>
</tr>
<tr>
<td>Funds</td>
<td>Gateway) approves or declines the sale based on funds available in the credit card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>account</td>
<td></td>
</tr>
<tr>
<td>Fraud Protection</td>
<td>AVS (Address Verification), CVV2, and Verified by Visa/MC SecureCode can be used to</td>
<td>Limited tools available to address the risk that Customer is supplying</td>
</tr>
<tr>
<td></td>
<td>confirm the cardholder’s identity</td>
<td>ACH routing information for a bank account they are not authorized to debit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not applicable due to Authorization process</td>
<td>Returns should be received by ODFI within two banking days after</td>
</tr>
<tr>
<td></td>
<td></td>
<td>settlement of the ACH debit</td>
</tr>
</tbody>
</table>
## WEB ACH versus Web Credit Card Transactions

<table>
<thead>
<tr>
<th></th>
<th><strong>WEB Credit Card Sale</strong></th>
<th><strong>WEB ACH Sale</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns due to Customer Dispute</td>
<td>Chargeback process allows cardholder to dispute a charge up to 180 days after the posting date. Merchant generally is given the opportunity to supply documentation supporting the disputed charge. If documentation provided is not acceptable to the Card Issuing bank then a chargeback will occur, debiting the merchant. There is a process for disputing chargebacks, but the dispute must be accepted by the Card Issuing bank.</td>
<td>An ACH debit can be returned up to 60 calendar days after the Settlement date of the debit if the Account Holder (Receiver) signs a written statement asserting that the ACH debit was not properly authorized. The debit is automatically reversed as long as NACHA requirements are met.</td>
</tr>
</tbody>
</table>
EXCERPTS FROM THE 2004 OPERATING GUIDELINES OF THE NATIONAL CLEARING HOUSE ASSOCIATION – CORPORATE EDITION

SECTION 1 DEVELOPMENT AND OVERVIEW OF THE SYSTEM (EXCERPT)
B. OVERVIEW OF THE SYSTEM

1. PARTICIPANTS

Five entities participate in the ACH system. They are defined as:

Originator

The Originator is the entity that agrees to initiate ACH entries into the payment system according to an arrangement with a Receiver. The Originator is usually a company directing a transfer of funds to or from a consumer's or another company's account. In the case of a customer initiated entry, however, the Originator may be an individual initiating funds transfer activity to or from his or her own account. The term "company" is intended to be representative of the Originator of electronic ACH entries and does not imply exclusion of other types of organizations.

Originating Depository Financial Institution

The Originating Depository Financial Institution (ODFI) is the institution that receives the payment instructions from Originators and forwards the entries to the ACH Operator. A DFI may participate in the ACH as a Receiving Depository Financial Institution (RDFI) without being an ODFI; however, if a DFI chooses to originate ACH entries, it must also agree to act as an RDFI.

Automated Clearing House Operator

An Automated Clearing House (ACH) Operator is the central clearing facility, operated by a Federal Reserve Bank (FRB) or a private organization, that receives entries from ODFIs, distributes the entries to appropriate RDFIs, and performs the settlement functions for the affected financial institutions. For a complete description of an ACH Operator, refer to the chapter on ACH Operators within Section II of these Guidelines.

Receiving Depository Financial Institution

The Receiving Depository Financial Institution (RDFI) is the DFI that receives ACH entries from the ACH Operator and posts them to the accounts of its depositors (Receivers).

Receiver

A Receiver is a natural person or an organization that has authorized an Originator to initiate an ACH entry to the Receiver's account with the Receiving DFI.

2. PAYMENT APPLICATIONS (Excerpt)

PPD - Prearranged Payment and Deposit Entry

Direct Deposit

Direct deposit is a credit application that transfers funds into a consumer's account at the Receiving Depository Financial Institution. The funds being deposited can represent a variety of products, such as payroll, interest, pension, dividends, etc.

Preauthorized Bill Payment

Preauthorized payment is a debit application. Companies with billing operations may participate in the ACH through the electronic transfer (direct debit) of bill payment entries. Through standing authorizations, the consumer grants the company authority to initiate periodic charges to his or her account as bills become due. This concept has met with appreciable success in situations where the recurring bills are regular and do not vary in amount -- insurance premiums, mortgage payments, and installment loan payments being the most prominent examples. Standing authorizations have also been successful for bills where the amount does vary, such as utility payments.
WEB ACH Primer

WEB - Internet-Initiated Entry

This Standard Entry Class Code is used for the origination of debit entries (either recurring or Single Entry) to a consumer's account pursuant to an authorization that is obtained from the Receiver via the Internet. This SEC Code helps to address unique risk issues inherent to the Internet payment environment through requirements for added security procedures and obligations.

SECTION II -- PARTICIPANT RELATIONSHIPS AND RESPONSIBILITIES (EXCERPT)

CHAPTER I -- ORIGINATORS

A. INTRODUCTION

An Originator initiates entries into the Automated Clearing House Network through a relationship with an Originating Depository Financial Institution (ODFI).

Examples of Originators are:

An employer offering its employees direct deposit of payroll or an organization (company, financial institution) offering direct deposit of certain funds (interest, dividends, retirement funds, etc.).

A company or billing firm that offers direct payment (debts) to those consumers that owe a recurring or one time obligation.

An organization that consolidates or disburses funds from or to its subsidiaries or branches.

A corporate entity that enters into a trading partner agreement with a corporate receiver for the purpose of transferring funds according to that agreement.

A merchant or financial institution that offers point of sale activity to consumers.

An individual that initiates an entry via a bill payment service to a company for monies owed.

The ACH Network enables an Originator to prepare a batch of debit and/or credit entries to effect the transfer of funds via the ACH from or to Receivers' accounts. The Originator must initiate the batch(es) into the ACH Network according to an arrangement with an ODFI.

The primary participant relationships for the Originator are with the Receiver and the ODFI. The Originator's relationship with the ODFI and the Receiver involves both legal responsibilities and processing issues.

B. LEGAL RESPONSIBILITIES - AGREEMENTS AND AUTHORIZATIONS

1. ELECTRONIC RECORDS AND ELECTRONIC RECORD RETENTION

The NACHA Operating Rules permit ACH participants to obtain and store ACH records electronically as an alternative to obtaining and retaining such documents in hard copy format. Specifically, the Rules allow any agreement, authorization, written statement under penalty of perjury, or other record required by the NACHA Operating Rules to be in writing to be obtained and retained in either hard copy or electronic form.

Electronic Signatures and Records

Electronic records include agreements, authorizations, written statements under penalty of perjury, or other records created, generated, sent, communicated, received, or stored by electronic means. Electronic records may have a signature requirement.

Electronic signatures are electronic sounds, symbols, or processes attached to or logically associated with an agreement, authorization, written statement under penalty of perjury, or other record executed or adopted by a person with the intent to sign the record. These writing and signature requirements can be satisfied by compliance with the Global and National Commerce Act (E-Sign Act). Originators should be aware that any record that is signed according to the terms of an applicable state version of the Uniform Electronic Transaction Act is considered to have been signed in conformance with the terms of the E-Sign Act.

To satisfy the requirements of the NACHA Operating Rules (and Regulation E for preauthorized debits), electronic signatures must "similarly authenticate" the electronic records. The authentication method chosen must evidence both the signer's identity and his assent to the terms of the record. For purposes of the NACHA Operating Rules, ACH records may also be similarly authenticated using the same authentication methods currently prescribed for consumer debit authorizations that is, the record may be similarly authenticated via the Internet through the use of a digital signature, PIN, password, shared secret, etc., or a hard copy record may be authenticated via the telephone by the consumer's speaking or key-entering a code provided on the record.
WEB ACH Primer

Any other written notice or disclosure required by the NACHA Operating Rules but not requiring a signature may also be provided in electronic form, including e-mail. (This includes the notice for TEL entries. Please note that state and federal laws may require consumer consent before using electronic notices/disclosures.)

Record Retention

Originators are permitted to retain copies of ACH records in electronic form, provided that the electronic record (1) accurately reflects information contained within the record, and (2) is capable of being accurately reproduced for later reference, whether by transmission, printing, or other reproduction.

Originators choosing to utilize electronic communications methods for the retention of ACH records should implement practices and procedures to ensure that electronic records of ACH documents accurately reflect the information contained within the document and that both the electronic record and a recorded record of the authentication can be accurately reproduced for future reference.

Originators should be aware that other ACH participants may also utilize electronic methods to obtain and retain records of ACH documents. In such cases, Originators can expect to receive electronic versions, rather than hard copies, of documents that they request from other ACH participants.

2. RELATIONSHIP WITH ODFI

The Originator must execute an agreement or contract with the ODFI that, at a minimum, binds the Originator to the NACHA Operating Rules. The agreement, among other things, defines the parameters of the relationship between the two parties, identifies processing requirements for the specific application(s), and establishes liability and accountability for certain procedures related to the application(s). Originators should be aware that, under the terms of this agreement, such liabilities may include, but are not limited to, the amount of any fines assessed against the ODFI for a rules violation caused by the Originator. In some instances, provisions of the agreement may be superseded by applicable federal or state law (e.g., Uniform Commercial Code Article 4A or the Electronic Fund Transfer Act). The following table lists specific issues that either may or may not be addressed in the NACHA Operating Rules, but which the Originator and its ODFI may wish to specifically define in their agreement. The matrix to the left of each item indicates whether the issue pertains to debit and/or credit consumer applications or debit and/or credit corporate applications. Originators must be aware that they are subject to applicable U.S. law when initiating ACH transactions. This includes, among other things, that the Originator is not violating the Office of Foreign Assets Control (OFAC)-enforced sanctions, and is not acting on behalf of, or transmitting funds to or from, any party subject to such sanctions. For additional information about OFAC requirements as they relate to Originators, refer to the discussion on Processing Requirements and Responsibilities -- Relationship With ODFI within this chapter. Detailed information on OFAC compliance can be found within Section IV, Special Topics, of these Guidelines. Originators are encouraged to interface with their ODFIs via a secured telecommunications link for all ACH-related activity. This includes the origination and/or receipt of all current ACH transactions, related reports, returns, NOCs, and any future related applications.

3. RELATIONSHIP WITH RECEIVER

For the majority of consumer applications, the Receiver authorizes the Originator to initiate entries through the ACH Network to the Receiver's account. The authorization agreement must be readily identifiable as either an ACH credit or an ACH debit authorization and must clearly and conspicuously state the terms of the authorization in order that the Receiver understands the authorization to which he is agreeing. The type of arrangement entered into between the Receiver and the Originator depends upon the type of application that is being initiated. Corporate applications, where the Originator and Receiver have entered into a trading partner agreement, could require more intricate agreements than consumer applications because the application could include the processing of payment related data or because the application necessitates the transfer of large dollars.

Authorization Requirements for Consumer Applications

Included within this section are sample Authorization Agreements for Direct Deposits (Credits) and Direct Payments (Debits) in consumer applications.

The following general direction is offered to promote accuracy and standardization for authorization requirements:

Account numbers and routing numbers must be accurately stated.

Originators may use the on-us field of the MICR line of checks and sharedrafts to obtain the account number for ACH transactions. Originators should also look on the face of a check or sharedraft for the routing information. Some financial institutions may print the Routing Number and account number used for ACH purposes on the face of the document if the information on the MICR line is not appropriate for ACH activity. In addition, some financial institutions may provide their customers with another source document that indicates the account number to be used for ACH entries.

In an effort to help ensure the proper routing and processing of ACH transactions, Originators should consider the implementation of practices and procedures that will enable them to verify the accuracy of routing numbers prior to the transmission of entries into
the ACH Network. Originators must be aware that, in certain circumstances, such as with TEL entries and WEB entries, the NACHA Operating Rules specifically require an Originator to establish commercially reasonable procedures to verify that routing numbers are valid. While not specifically required by the NACHA Operating Rules, Originators are also encouraged to establish procedures to verify that account number structures are valid.

* The consumer must date and either sign or similarly authenticate a written authorization.

* When the authorization is directed to a demand deposit account or a savings account, the authorizer(s) should so indicate. NOW accounts and sharedraft accounts are transaction accounts within the broad category of demand accounts. The authorizer(s) will also need to indicate when the authorization relates to entries directed to a loan account.

* The company identification number is agreed upon by the originating company and the ODFI. It is common practice to use one of the ANSI standard identifiers indicating what type of number is used. The ANSI standard identifiers are: “1” (indicating an IRS number); “3” (indicating a DUNS number); or “9” (indicating a user-assigned number).

* The individual ID number is the number assigned by an Originator for internal control: Social Security number, employee number, customer billing number, or customer internal account number. No more than 15 characters of identification can be used for this purpose. (Spaces and dashes are included in the count of 15.)

* The Originator must obtain authorization for both consumer credit and debit entries. An exception to the credit authorization requirement occurs when both the Originator and Receiver are natural persons.

### Credits

Authorizations for credit entries may be provided by the consumer in writing, or they may be provided orally or by other non-written means.

### Debits

All debits to consumer accounts must be authorized by the consumer via a writing that is signed or similarly authenticated by the consumer, with the exception of ARC entries, RCK entries, and TEL entries.

Originators of debit entries to consumer accounts must ensure compliance with the following criteria to ensure proper authorization of consumer debits under the NACHA Operating Rules:

**Copy of Authorization** - With the exception of ARC entries, TEL entries, and RCK entries, the Originator must send to the consumer written authorization. This authorization may be sent by mail, fax, or Internet/on-line network, or it may be provided to the consumer in-person. For both paper and telephone alternatives, the consumer has a paper authorization in his possession, which he should retain as his copy of the authorization. The consumer can also request an additional hard copy of the authorization from the Originator. For the Internet/on-line 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 the authorization if requested to do so.

For TEL entries, the consumer's authorization may be obtained orally via the telephone for Single Entry 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. If requested to do so, the Originator must be able to provide the consumer with a copy of the written notice or tape recording.

For ARC entries and RCK entries, authorization consists of notice from the Originator to the consumer and the receipt of the consumer's source document (for ARC entries) or item (for RCK entries) by the Originator.

**Minimum Information Requirements** - The authorization must be readily identifiable as an ACH debit authorization and must clearly and conspicuously state its terms. With the exception of POP entries, TEL entries, and Single Entry WEB entries, the writing must specify that the Receiver may revoke the authorization only by notifying the Originator in the manner specified on the authorization form.

For TEL entries, where the consumer's authorization is obtained orally via the telephone, the authorization must be readily identifiable as an authorization and must clearly state its terms. The following minimum information must be included as part of the authorization:

- the date on or after which the ACH debit to the Receiver's account will occur;
- the amount of the transaction;
- the Receiver's name;
- a telephone number for Receiver inquiries that is answered during normal business hours;
- the date of the Receiver's oral authorization; and
WEB ACH Primer

- a statement by the Originator that the authorization obtained from the Receiver is for a Single Entry ACH debit.

Authentication of Authorization - With the exception of ARC entries, RCK entries, and TEL entries, the written authorization must be signed or similarly authenticated by the consumer. Figure 4 (Guidelines for Similarly Authenticated) outlines acceptable alternatives for authenticating the consumer's authorization.

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.), which defines electronic records and electronic signatures. Electronic records include contracts or other records created, generated, sent, communicated, received, or stored by electronic means. Electronic signatures include, but are not limited to, digital signatures and security codes.

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. It is important to note that the authorization and the authentication of that authorization must occur simultaneously. It is not considered acceptable authentication to have identified a consumer at the time of logging on to a website and then later consider that log-in an authentication for purposes of authorizing an ACH debit. Nor is it considered acceptable to authenticate an authorization simply by a click-through process.

Retention of Authorization - The signed or similarly authenticated authorization must be retained by the Originator for a period of two years following the termination or revocation of the authorization. In the case of a paper authorization that has been signed by the consumer, the Originator must retain either the original or a microfilm-equivalent copy of the signed authorization. In the case of an authentication made via telephone, the Internet, or other on-line network, the Originator must retain a copy of the authorization and a recorded record of the authentication. For TEL entries, the Originator must retain a copy of the tape recorded authorization or a copy of the written notice confirming the authorization for a period of two years from the date of the authorization. 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.

Multiple, Non-Recurring Debits

For multiple but non-recurring debits, where the amount and time frame for the initiation of the debits may vary (for example, occasional catalog purchases from the same merchant or occasional purchases of securities with a broker), Originators need not obtain a written authorization for each debit entry, provided they have obtained a written authorization up front which establishes a relationship between the Originator and Receiver (consumer) for this type of activity.

Notice of Change in Amount/Change in Debiting Date for Recurring Debits

For recurring debits, when the debit amount varies, specific requirements apply. If a preauthorized debit transfer varies from a previous transfer relating to the same authorization or from a fixed preauthorized amount, the Originator must send the Receiver written notification of the amount and scheduled date of the transfer at least ten (10) 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; or, 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.

In an application in which the Originator changes the date on or after which a recurring debit entry is scheduled to be debited to a Receiver's account, the Originator must send the Receiver written notification of the new date on which the entry will be debited 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.

Consumer Information

Originators must ensure that the consumer is completely aware of the nature of the product or service that he or she is purchasing. The rights provided to the consumer in questioning electronic funds transfer activity to his account are very liberal. Failure to understand the nature of the product or service that is being sold could result in the return of the ACH debit to the Originator.

Information Requirements

The Originator, upon request, must present a copy of the customer's authorization to an ODFI for 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.
Revocation of Authorization

A Receiver wishing to cancel or revoke his or her authorization must do so directly with the Originator under the terms and conditions set forth in the authorization agreement. A consumer may inform its RDFI that it has revoked an authorization, thereby causing an entry to be returned to the Originator. Before an RDFI may return an entry for “Authorization Revoked by Customer” (return reason code R07), the RDFI must obtain from the Receiver a written statement under penalty of perjury, in which the Receiver states that the authorization for the debit entry has been revoked directly with the Originator. (Note: At its discretion, the RDFI can still choose to require that an affidavit be signed.) The Originator may request that its ODFI obtain a copy of the written statement under penalty of perjury from the RDFI when appropriate. A written request for a copy of the written statement under penalty of perjury must be received by the RDFI within one year of the date on which the adjustment entry was initiated by the RDFI. The RDFI is required to provide a copy of the written statement under penalty of perjury within sixty days after receiving the ODFI’s written request for the copy. (A sample written statement under penalty of perjury may be found in the chapter concerning Receiving Depository Financial Institutions in Section II of these Guidelines.) Originators may not reinitiate entries returned for authorization revoked and should be prepared to contact the Receiver regarding those entries. (Note: POP entries, TEL entries, and Single Entry WEB Entries may not be returned by an RDFI as “Authorization Revoked.” Because these transactions are one-time payments where the Originator will generally process the transaction immediately after the purchase is complete, the Receiver is precluded from revoking authorization for the transaction. The Receiver does, however, retain his right to place a stop payment order on such transactions and to request the return of any unauthorized entry.)

Unauthorized/Improper Consumer Debits

Originators can expect the return of entries that are not properly authorized. An unauthorized debit entry is an entry in which:

the written authorization requirements have not been followed; a transaction was initiated in an amount greater than that authorized by the Receiver; or a transaction was initiated for settlement earlier than authorized by the Receiver.

SAMPLES

AUTHORIZATION AGREEMENT FOR DIRECT DEPOSITS (ACH CREDITS)

Company Name_________________________________________ ID
Number________________________________________________
I (we) hereby authorize _______________________________________________________, hereinafter called COMPANY, to initiate credit entries to my (our) Checking Account / Savings Account (select one) indicated below at the depository financial institution named below, hereafter called DEPOSITORY, and to credit the same to such account. I (we) acknowledge that the origination of ACH transactions to my (our) account must comply with the provisions of U.S. law.

Depository Name_________________________________________
Branch__________________________________________________
City______________________________________________________ State_______________
Zip__________________________
Routing Account Number_____________________________________
Number_____________________________________________________
This authorization is to remain in full force and effect until COMPANY has received written notification from me (or either of us) of its termination in such time and in such manner as to afford COMPANY and DEPOSITORY a reasonable opportunity to act on it.

Name(s)________________________________________________ ID
Number_____________________________________________ (Please Print)
Date__________________________________________________
Signature________________________________________________

NOTE: WRITTEN CREDIT AUTHORIZATIONS MUST PROVIDE THAT THE RECEIVER MAY REVOKE THE AUTHORIZATION ONLY BY NOTIFYING THE ORIGINATOR IN THE MANNER SPECIFIED IN THE AUTHORIZATION.
AUTHORIZATION AGREEMENT FOR DIRECT PAYMENTS (ACH DEBITS)

Company Name________________________________________________________ ID
Number______________________________________________________________

I (we) hereby authorize _______________________________________________________, hereinafter called COMPANY, to initiate debit entries to my (our) Checking Account / Savings Account (select one) indicated below at the depository financial institution named below, hereafter called DEPOSITORY, and to debit the same to such account. I (we) acknowledge that the origination of ACH transactions to my (our) account must comply with the provisions of U.S. law.

Depository Name________________________________________________________
Branch____________________________________________
City _________________________________________________________ State________________
Zip__________________________
Routing Account Number_______________________________________________________
Number____________________________________________

This authorization is to remain in full force and effect until COMPANY has received written notification from me (or either of us) of its termination in such time and in such manner as to afford COMPANY and DEPOSITORY a reasonable opportunity to act on it.

Name(s)______________________________________________________ ID
Number________________________________________________________ (Please Print)
Date_________________________________________
Signature_____________________________________________________________

NOTE: DEBIT AUTHORIZATIONS MUST PROVIDE THAT THE RECEIVER MAY REVOKE THE AUTHORIZATION ONLY BY NOTIFYING THE ORIGINATOR IN THE MANNER SPECIFIED IN THE AUTHORIZATION.

SECTION IV – SPECIAL TOPICS (EXCERPT)

CHAPTER VI -- INTERNET-INITIATED ENTRIES

A. INTRODUCTION

Internet-Initiated Entries (WEB entries) are used for the origination of debit entries (either recurring or Single Entry) to a consumer’s account pursuant to an authorization that is obtained from the Receiver via the Internet. This SEC Code helps to address unique risk issues inherent to the Internet payment environment through requirements for added security procedures and obligations.

B. BACKGROUND

There are three unique characteristics of the Internet that warranted the development of new NACHA Operating Rules: 1) the anonymity of the Internet creates an environment in which parties are not certain with whom they are doing business, which poses unique opportunities for fraud, 2) the Internet is an open network, which requires special security procedures to be deployed to prevent unauthorized access to consumer financial information, and 3) the sheer number and speed with which payments can be transacted over the Internet, known as volume and velocity.

While it was imperative to incorporate specific security measures for Internet-initiated ACH debits into the NACHA Operating Rules, it was premature to prescribe an overly detailed, rigid set of rules. Technical solutions and business practices to support these payments are still emerging, and 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.)

The current NACHA Operating Rules for WEB entries establish a set of critical requirements necessary to set a minimum amount of protection for WEB entries. Over the long term, additional enhancements to the Rules may be necessary to build upon this foundation.
C. LEGAL FRAMEWORK

WEB entries are subject to the requirements of the NACHA Operating Rules, the Electronic Fund Transfer Act, and Regulation E, as promulgated by the Federal Reserve Board.

D. DEFINITIONS

1. WEB ENTRY

A WEB entry is defined as a debit entry to a Consumer Account initiated by an Originator pursuant to an authorization that is obtained from the Receiver via the Internet. There are two components of the definition that are important to address:

* the WEB Standard Entry Class (SEC) code is only appropriate to use when initiating debit entries that have been authorized by the Receiver via the Internet. An authorization that was obtained from the Receiver in person, through the mail or over the telephone in order to effect an Internet payment is not to be initiated as a WEB transaction. These transactions should use the appropriate SEC code as defined by the NACHA Operating Rules. For example, if a Receiver authorizes a monthly debit to his or her account for a bill payment service via paper in writing, but goes to the biller's website to verify the amount of the bill each month, this transaction would constitute a PPD entry rather than a WEB entry; and

* the WEB SEC code cannot be used to initiate credit entries except for reversals of WEB debit entries.

It is important to note that for transactions that involve some use of the Internet but are not defined as WEB transactions (such as the example cited above), Originators are encouraged to incorporate the security and risk management principles of the WEB rules, as applicable. For example, it would still be advisable for the Originator to authenticate the Receiver, deploy a secure Internet session using 128 bit SSL encryption, and conduct a security audit to ensure the Receiver's data is stored securely.

2. COMMERCIALLY REASONABLE

For all WEB entries, each Originator is obligated to ensure that certain aspects of a transaction have been handled in a commercially reasonable manner. In addition, each ODFI warrants that the Originator has handled those aspects of a transaction in a commercially reasonable manner. Those aspects of the transaction include commercially reasonable fraudulent transaction detection systems, security technology to establish a secure Internet session, and procedures to verify the validity of the RDFI's routing number.

A commercially reasonable system, technology, practice, or procedure is one that corresponds to commonly accepted commercial practices among commonly situated Originators conducting similar types of transactions. In other words, the concept of commercial reasonableness means that an Originator, given the facts of a specific transaction, acted in a way that other similar Originators would have acted. Whether an Originator has fulfilled its obligations to perform in a commercially reasonable manner will be determined based on an evaluation of the circumstances, including a weighing of the cost to the Originator to employ a particular technology or procedure against the level of protection it affords to the Originator and other ACH participants. Accordingly, what constitutes a commercially reasonable system, technology, practice or procedure may change over time. For example, as new technology becomes available or costs of certain technologies or procedures decrease, new standards of commercial reasonableness may evolve. Therefore, Originators and ODFIs need to work together to ensure continued compliance.

The person challenging the use of a particular system, technology, practice or procedure has the burden of establishing that the system, technology, practice or procedure employed by the Originator was not commercially reasonable.

3. SINGLE-ENTRY v. RECURRING

The WEB Standard Entry Class Code applies to both recurring and Single-Entry Internet-initiated payments. In the case of WEB entries, a Single-Entry payment means a one-time transfer of funds initiated by an Originator in accordance with the Receiver's authorization for a single ACH debit to the Receiver's account. One example of a Single-Entry WEB transaction would be a consumer purchase of a book online.

For purposes of WEB entries, a recurring payment is: 1) an entry that has been set up to occur, based on the Receiver's authorization obtained via the Internet, at regular intervals without any additional intervention of the consumer (i.e., a monthly debit to the consumer's account for a mortgage payment); or 2) multiple entries, based on an authorization provided by the consumer establishing a relationship with the Originator for a specific type of activity, that are originated each time upon the specific instructions of the consumer (i.e., an instruction to a broker to purchase or sell securities).

There are two primary reasons why a distinction has been made between recurring and Single-Entry WEB transactions. First, Single-Entry payments have the potential to be more risky because the Originator and Receiver often do not have a prior relationship established, which makes robust authentication more difficult and the possibility of fraud and exception processing higher. For example, a one-time purchase of a diamond is thought to be more susceptible to fraud than a recurring payment for a telephone bill. While all of this is subjective and depends highly on each unique transaction, it is important for both Originators and
WEB ACH Primer

ODFIs to be able to recognize these payments in order to monitor them separately for risk management purposes if they so choose.

Second, one permissible reason for returning a WEB entry and the stop payment requirements for WEB entries are different for Single-Entry and recurring payments. Originators are not required to include within the authorization language for a Single-Entry WEB entry the method by which the consumer can revoke his authorization for the transaction. (Note: This revocation language is required to be included in authorizations for all recurring payments, including recurring WEB entries.) This is because these are one-time payments and the Receiver will most likely not have the opportunity to revoke the authorization before the transaction is processed. Accordingly, RDFIs are prohibited from returning Single-Entry WEB entries based on a consumer's claim that his authorization has been revoked (i.e., using Return Reason Code R07).

Likewise, to ensure that a consumer has the ability to place a stop payment order on a Single-Entry WEB entry, the NACHA Operating Rules allow a consumer 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. In contrast, for a recurring payment, the consumer has the right to place a stop payment only as long as they request the stop payment at least three days prior to the scheduled settlement date of the entry.

E. OBLIGATIONS OF ORIGINATORS

1. AGREEMENTS WITH ODFIs

Originators choosing to utilize the ACH Network for initiating 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 WEB transactions and should define any specific processing obligations relating to such transactions. For example, the NACHA Operating Rules require ODFIs to set specific exposure limits for WEB transactions for each Originator, and the agreements may need to be modified to address those limits. For more information on agreements, refer to the ODFIs chapter within Section II of these Guidelines.

2. AUTHORIZATION REQUIREMENTS

Originators of WEB entries must obtain the consumer'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 NACHA Operating Rules, which require that the authorization be (1) in a writing that is signed or similarly authenticated by the Receiver, (2) be readily identifiable as an ACH debit authorization, (3) clearly and conspicuously state its terms, and (4) must (for recurring payments only) provide the Receiver with a method to revoke their authorization by notifying the Originator in the manner prescribed.

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

The NACHA Operating Rules include the use of a digital signature or code to similarly authenticate a written authorization. This does not exclude other methods of similarly authenticating an authorization, such as a shared secret, etc. To satisfy the requirements of the NACHA Operating Rules, the authentication method chosen must not only identify the consumer but also must demonstrate the consumer's assent to the authorization. The Federal Reserve Board, in its Official Staff Commentary to Regulation E, has clarified that the similarly authenticated standard permits signed, written authorizations to be provided electronically, and that such 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.), which defines electronic records (as contracts or other records created, generated, sent, communicated, received, or stored by electronic means) and electronic signatures. Electronic signatures include, but are not limited to, digital signatures and security codes.

3. RISK MANAGEMENT

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

* Fraudulent Transaction Detection Systems

The best way in which Originators can minimize the potential for fraudulent ACH transactions is by employing fraudulent transaction detection systems to identify the Receiver before accepting ACH debit authorizations. In order to meet the requirement, the fraudulent transaction detection system must authenticate the identity of the Receiver. Systems that track payment history, behavior, and purchase type, while recommended, do not meet the requirement unless they are used in...
WEB ACH Primer

conjunction with a method of authentication.

Fraudulent transaction detection systems employ different methodologies and offer different features at varying costs. The choice of which particular fraudulent transaction detection system is appropriate for a particular Originator is generally a decision to be made by the Originator. When considering which fraudulent transaction detection system to deploy, Originators should determine whether their WEB entry transactions will be primarily conducted with existing customers, new customers or both.

Existing customers can usually be authenticated by shared secrets between the customer and the Originator, such as a designated PIN, password or previous transaction history. This is because there is an established relationship between existing customers and the Originator. However, there is no standard authentication process that is being used online to identify and authenticate unknown individuals on the Internet. Therefore it is the Originator's responsibility to choose an appropriate solution that will minimize the potential for fraudulent transactions. Some factors to consider in selecting an authentication method that is commercially reasonable include transaction amount, type of goods offered, new or existing customer, and method of delivery. However, a fraudulent transaction detection system must be deployed no matter how small the transaction amount or type. It will never be considered commercially reasonable to have done nothing. Similarly, assigning a password 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. Since Originators are responsible for fraudulent ACH transactions, it is to their benefit to incorporate an adequate amount of authentication into their online ACH payment process.

* Verification of Routing Numbers

Many WEB entries will be Single-Entry payments, and Receivers will frequently enter their routing numbers manually using a keyboard. For these reasons, exception processing related to WEB entries may increase. To minimize exception processing related to 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 consumer enters the routing number correctly and that it is a valid RDFI routing number for ACH transactions. Although the NACHA Operating Rules do not require Originators to verify the validity of Receiver account number structures, it is strongly recommended that they employ procedures to do so. Some of the methods discussed below are appropriate to help verify the validity of both routing numbers and account number structures.

Verifying the validity of routing numbers can be accomplished as either 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.

* Security of Internet Session

The NACHA Operating Rules for WEB entries require Originators to employ a commercially reasonable security technology which provides a level of security that, at a minimum, is equivalent to 128 bit SSL encryption technology. Currently, 128 bit SSL encryption technology is the standard for financial transactions and is considered commercially reasonable. If technological advancements drive the commercially reasonable standard to change, Originators should comply with the new standard.

Originators should also be aware that the 128 bit SSL encrypted session must begin, at a minimum, at the first point of key entry of Receiver financial information through the transmission of the data to the Originator.

* Audits of Website Security

Data loss or compromise not only hurts the consumer, but also damages the merchant's reputation. Consumer trust is a key factor in building loyalty to merchants. 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 WEB transactions require Originators to conduct an audit at least once a year to ensure that Receivers' financial information is protected by security practices and procedures that ensure that the financial information that the Originator obtains from consumers is protected by security practices that include adequate levels of: 1) physical security to protect against theft, tampering, or damage, 2) personnel and access controls to protect against unauthorized access and use, and 3) network security to ensure secure capture, storage and distribution of financial information. Such an audit must be completed annually.

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 or security seal program that covers these security issues. 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. As long as the audit covers these components, it will meet the requirement.

While the NACHA Operating Rules only require Originators 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 WEB entries also conduct more frequent audits.

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:
  * 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 to these areas and information only when absolutely necessary and ensure they are accompanied by an employee at all times.
  * Restrict access from external networks to authenticated users (i.e. by passwords or login codes).
  * Ensure that one person acting alone cannot circumvent safeguards, i.e. dual control procedures are in place.

Procedures and audit trails need to be established to scrutinize activities of users with access to Receiver information in order to detect anomalies.

(3) Network security to ensure secure capture, storage and distribution

* All Receiver financial information should be kept behind firewalls and in an area inaccessible from the Internet.

* A data retention schedule should be developed that covers the policies on how to handle the data from the time of capture to destruction.

* Retention schedules should be monitored to ensure that they are being met.

* Receiver information should only be stored permanently if it is required by law, regulation, rule, or a governing organization.

* Data should not be stored longer than necessary.

* Distribution of Receiver data should be limited, with procedures and controls in place governing how it is distributed.

* The need for distributing Receiver data should be reviewed, and all distribution is verified and approved.

* Receiver data sent across networks must be encrypted.

* Use and regularly update anti-virus software.

* Regularly test security systems and processes.
EXCERPTS FROM THE 2004 NACHA OPERATING RULES

ARTICLE TWO – ORIGINATION OF ENTRIES EXCERPTS

SECTION 2.1 Prerequisites to Origination

SUBSECTION 2.1.2 Receiver Authorization and Agreement

The Receiver has authorized the Originator to initiate the entry to the Receiver's account. In the case of CBR, CCD, and CTX entries, the Receiver has an agreement with the Originator under which the Receiver has agreed to be bound by these rules as in effect from time to time. In the case of debit entries to a Consumer Account, the authorization must be in writing and signed or similarly authenticated by the consumer. The similarly authenticated standard permits signed, written authorizations to be provided electronically. The 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.), which defines electronic records (as contracts or other records created, generated, sent, communicated, received, or stored by electronic means) and electronic signatures. Electronic signatures include, but are not limited to, digital signatures and security codes. The authorization process must evidence both the consumer's identity and his assent to the authorization. To meet the requirement that an authorization be in writing, an electronic authorization must be able to be displayed on a computer screen or other visual display that enables the consumer to read the communication. The authorization also must be readily identifiable as an authorization, must clearly and conspicuously state its terms, and, for all entries except POP entries and Single-Entry WEB entries, the authorization must provide that the Receiver may revoke the authorization only by notifying the Originator in the manner specified in the authorization. The authorization for ARC Entries consists of a notice meeting the requirements of subsection 2.1.4 (Notification for Accounts Receivable Entries and Re-presented Check Entries) and the receipt of the Receiver's source document. The authorization for RCK entries consists of a notice meeting the requirements of subsection 2.1.4 and the receipt of the item to which the RCK entry relates. In the case of credit entries, the authorization may be provided orally or by other non-written means. Entries subject to subsections 2.1.3 (Exception to Authorization Requirement) and 2.1.5 (Authorization for Telephone-Initiated Entries) are excepted from these Receiver authorization requirements.

SECTION 2.10 Internet-Initiated Entries

SUBSECTION 2.10.1 General Rule

A WEB entry may be transmitted by an Originator pursuant to an authorization that is obtained from the Receiver via the Internet to effect a transfer of funds from a Consumer Account of the Receiver.

SUBSECTION 2.10.2 ODFI Warranties

In addition to the other warranties contained within these rules, each ODFI initiating a WEB entry pursuant to this section 2.10 warrants to each RDFI, ACH Operator, and Association that:

SUBSECTION 2.10.2.1 Fraud Detection Systems

Each Originator for which the ODFI transmits WEB entries has employed a commercially reasonable fraudulent transaction detection system to screen each entry.

SUBSECTION 2.10.2.2 ODFI Exposure Limits

In the case of a WEB entry initiated by an Originator that is not a natural person, the ODFI has (1) utilized a commercially reasonable method to establish the identity of the Originator, (2) established procedures to monitor the credit-worthiness of that Originator on an on-going basis, (3) established an exposure limit for that Originator, (4) implemented procedures to review that exposure limit periodically, and (5) implemented procedures to monitor entries initiated by that Originator relative to its exposure limit across multiple settlement dates.

SUBSECTION 2.10.2.3 Verification of Routing Numbers

Each Originator that originates WEB entries has used commercially reasonable procedures to verify that routing numbers are valid.
WEB ACH Primer

SUBSECTION 2.10.2.4 Security of Internet Session

Each Originator that originates WEB entries has established a secure Internet session with each Receiver utilizing a commercially reasonable security technology providing a level of security that, at a minimum, is equivalent to 128-bit encryption technology prior to the Receiver's key entry and through transmission to the Originator of any banking information, including, but not limited to, the Receiver's routing number, account number, and PIN number or other identification symbol.

SUBSECTION 2.10.2.5 WEB Annual Audit

Each Originator that originates WEB entries shall conduct or have conducted annual audits to ensure that the financial information it obtains from Receivers is protected by security practices and procedures that include, at a minimum, adequate levels of (1) physical security to protect against theft, tampering, or damage, (2) personnel and access controls to protect against unauthorized access and use, and (3) network security to ensure secure capture, storage, and distribution.

SUBSECTION 2.10.2.6 Liability for Breach of Warranty

Each ODFI breaching any of the warranties contained within subsection 2.10.2 (ODFI Warranties) shall indemnify every RDFI, ACH Operator, Association, and any other party covered by the warranty from and against any and all resulting claim, demand, loss, liability, or expense, including attorneys’ fees and costs, resulting directly or indirectly from the breach of these warranties. In addition, in the case of a Consumer Account, the ODFI shall indemnify every RDFI, ACH Operator, Association, and any other party covered by the warranty from and against any and all resulting claim, demand, loss, liability, or expense based on the ground that the failure of the ODFI to comply with any provision of these rules resulted, either directly or indirectly, in the violation by an RDFI of the Federal Electronic Fund Transfer Act or Federal Reserve Board Regulation E.

ARTICLE THREE – OBLIGATIONS OF ORIGINATORS EXCERPTS

SECTION 3.8 Obligations of Originators of Internet- Initiated Entries

SUBSECTION 3.8.1 Fraud Detection Systems

Each Originator originating WEB entries must employ a commercially reasonable fraudulent transaction detection system to screen each entry.

SUBSECTION 3.8.2 Verification of Routing Numbers

Each Originator that originates WEB entries must use commercially reasonable procedures to verify that routing numbers are valid.

SUBSECTION 3.8.3 Security of Internet Session

Each Originator that originates WEB entries must establish a secure Internet session with each Receiver utilizing a commercially reasonable security technology providing a level of security that, at a minimum, is equivalent to 128-bit encryption technology prior to the Receiver's key entry and through transmission to the Originator of any banking information, including, but not limited to, the Receiver's routing number, account number, and personal identification number (PIN) or other identification symbol.

SUBSECTION 3.8.4 WEB Annual Audit

Each Originator that originates WEB entries shall conduct or have conducted annual audits to ensure that the financial information it obtains from Receivers is protected by security practices and procedures that include, at a minimum, adequate levels of (1) physical security to protect against theft, tampering, or damage, (2) personnel and access

SECTION 3.10 Record of Authorization

An Originator must retain the original or a microfilm or microfilm-equivalent copy of each authorization of a Receiver for two years from the termination or revocation of the authorization. In the case of TEL entries, the Originator must retain the original or a microfilm or microfilm-equivalent copy of the written notice or the original or a duplicate tape recording of the oral authorization for two years from the date of the authorization. At the request of its ODFI, the Originator must provide the original or copy of the authorization to the ODFI for its use or for the use of an RDFI requesting the information pursuant to subsection 4.1.1 (Right to Information Regarding Entries). This section 3.10 does not apply to SHR or MTE entries if the ODFI and RDFI are parties to an agreement (other than these rules) for the provision of services relating to SHR or MTE entries.
ARTICLE THIRTEEN – DEFINITION OF TERMS

SUBSECTION 13.1.37 "Originator"

means a person that has authorized an ODFI to transmit (1) a credit entry to the account of a Receiver with an RDFI, or, if the Receiver is also the RDFI, to such Receiver, or (2) a debit entry to the Receiver's transaction account or general ledger account with an RDFI, or, if the Receiver is also the RDFI, to such Receiver. Where the context so requires, as in the case of MTE entries, that term also refers to the ODFI.

SUBSECTION 13.1.41 "Person"

means a natural person or an organization.

SUBSECTION 13.1.44 "PPD entry"

means a credit or debit entry (other than an MTE or POS entry) initiated by an organization pursuant to a standing or a single entry authorization from a Receiver to affect a transfer of funds to or from a Consumer Account of the Receiver. "PPD+" is a PPD entry with one addenda record.

SUBSECTION 13.1.48 "Receiver"

means a person that has authorized an Originator to initiate (1) a credit entry to the Receiver's account with an RDFI, or, if the Receiver is also the RDFI, to such Receiver, or (2) a debit entry to the Receiver's transaction account or general ledger account with an RDFI, or, if the Receiver is also the RDFI, to such Receiver. With respect to debit entries, the term "Receiver" shall be deemed to mean all persons whose signatures are required to withdraw funds from an account for purposes of the warranty provisions of subsection 2.2.1 (Warranties).

SUBSECTION 13.1.64 "WEB entry" or "WEB"

means a debit entry initiated by an Originator pursuant to an authorization that is obtained from the Receiver via the Internet to effect a transfer of funds from a Consumer Account of the Receiver.

APPENDIX FIVE – RETURN ENTRIES EXCERPT

SECTION 5.4 Table of Return Reason Codes (cont.)

(Return, Adjustment, Correction, and Acknowledgment of Entries and Entry Information) of these Rules.

R07 Authorization Revoked by Customer (adjustment entries) The RDFI's customer (the Receiver) has revoked the authorization previously provided to the Originator for this particular transaction. The Receiver may request immediate credit from the RDFI for an unauthorized debit. The request must be made in writing within fifteen (15) days after the RDFI sends or makes available to the Receiver information pertaining to that debit entry. The Receiver must also provide the RDFI with a written statement under penalty of perjury that the authorization for the debit entry has been revoked by the Receiver. The RDFI must return the rescinded transaction to its ACH Operator by its deposit deadline for the adjustment entry 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 original entry. This code and related Operating Rule provisions apply to Consumer entries only. (Note: This Return Reason Code may not be used for POP entries, Single-Entry WEB entries, or TEL entries.)

R10 Customer Advises Not Authorized, Notice Not Provided, Improper Source Document, or Amount of Entry Not Accurately Obtained from Source Document (adjustment entries)

* For entries to Consumer Accounts that are not ARC entries, POP entries, or RCK entries, the RDFI has been notified by its customer, the Receiver, that the Originator of a given transaction has not been authorized to debit his account. The Receiver may request immediate credit from the RDFI for an unauthorized debit. The request must be made in writing within fifteen (15) days after the RDFI sends or makes available to the Receiver information pertaining to that debit entry. The Receiver must also provide the RDFI with a written statement under penalty of perjury, pursuant to subsection 7.6.5 (Receiver's Written Statement Under Penalty of Perjury), that the debit entry was not authorized by the Receiver. For purposes of this code and related Operating Rule provisions, a debit entry was not authorized by the Receiver if (1) the authorization requirements of Article Two, subsection 2.1.2 (Receiver Authorization and Agreement) have not been met; (2) the debit entry was initiated in an amount greater than that authorized by the Receiver; or (3) the debit entry was initiated for settlement earlier than authorized by the Receiver. An unauthorized debit entry does not include a debit entry initiated with fraudulent intent by the Receiver or any person acting in concert with the Receiver. The RDFI must return the rescinded transaction to its ACH Operator by its deposit deadline for the
WEB ACH Primer

adjustment entry 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 original entry. This code and related Operating Rule provisions apply to Consumer entries only.