Summary of recent and upcoming NACHA Operating Rule Changes

Micro-Entries (Phase 2)

Effective on March 17, 2023

This change impacts Originators

An Originator of Micro-Entries must conduct commercially reasonable fraud detection on its use of Micro-Entries, including by monitoring of forward and return volumes of Micro-Entries

- The use of commercially reasonable fraud detection is intended to minimize the incidence of fraud schemes that make use of Micro-Entries
- Monitoring forward and return volumes, at a minimum, establishes a baseline of normal activity
- An Originator would not be required to perform an entry-by-entry review

Reminders of responsibilities with current NACHA Rules for Originators

Notification of Change (NOC)

Originators must respond to Notifications of Change by making corrections within six banking days of receipt of the NOC information or prior to initiating another entry to the Receiver's account, whichever is later. (Note: Special requirements apply to NOCs received in response to prenotification entries and to Single Entries. These are discussed in more detail below.)

NOC received in response to a prenotification entry

- An Originator must make all changes contained within an NOC related to a prenotification entry; however, the Originator's timing requirements for action can differ, depending on when the NOC is made available to the ODFI. For a timely NOC (that is, an NOC made available to the Originator's ODFI by the ACH Operator by the opening of business on the second banking day following the prenote's settlement date), the Originator must make the requested changes before transmitting a "live" entry to the Receiver's account. For an untimely NOC (that is, an NOC made available to the ODFI by the ACH Operator after the opening of business on the second banking day following the prenote's settlement date), the Originator must make the requested changes within six banking days of receiving the NOC information from its ODFI or prior to transmitting the next entry, whichever is later

NOC Received in response to a Single Entry

- By definition, a Single Entry is a credit or debit entry based on a Receiver's authorization for a one-time transfer of funds to or from the Receiver's account. No subsequent entries may be originated unless separately authorized by the Receiver via a new authorization. The NACHA Operating Rules, therefore, allow an Originator discretion in determining whether to make the changes requested in any NOC related to an Entry identifiable as a Single Entry. Originator action on NOCs related to entries bearing any of the following SEC Codes is optional, at the Originator's discretion: ARC, BOC, POP, RCK, and XCK Entries, as well as TEL and WEB entries bearing a Single Entry indicator ("S" or "blank" for TEL and "S" for WEB).

Internet Initiated/Mobile Entries (WEB)

Debit WEB entries are used by non-consumer Originators to debit a consumer based on an authorization that is communicated, other than by an oral communication, from the Receiver to the Originator via the Internet or a Wireless Network. Originators of WEB transactions must establish commercially reasonable methods of authentication to:

a. Verify the identity of the Receiver;

b. Detect fraudulent transactions;

c. Establish secure internet sessions; and

d. Procedures to verify the validity of the receiving bank's routing number.

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

The following pieces of information must be included in the authorization:

1. Express authorization language ("I authorize Company A" to debit my account)

2. Amount of transaction:

• for a Single-Entry payment

• for a recurring entry that is for the same amount each interval, or

• for a range of payments

3. The effective date of the transaction

4. The Receiver's account number

5. The Receiver's financial institution's routing number

6. Revocation language

In the event that an Originator must demonstrate proof of a Receiver's authorization for a debit WEB entry, it should provide documentation that provides transaction details including Receiver information and sales documentation to show what goods and/or services were exchanged.

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

Originators of WEB transactions must use Fraudulent Transaction Detection Systems.

Using fraudulent transaction detection systems to screen debit WEB entries reduces the potential for fraudulent ACH transactions. Fraudulent transaction detection systems employ different methodologies and different features at varying costs. The choice of which features should be included in a fraudulent transaction detection system for a particular Originator is generally a decision to be made by the Originator.

Examples of fraudulent transaction detection systems are systems that track payment history, behavior, purchase type, delivery information, etc. Factors to consider when choosing a fraudulent transaction detection system for debit WEB entries include, but are not limited to:

• the number of transactions processed by the Originator,

• the average dollar size of each transaction,

• the typical relationship with the Receiver (existing or new), and

• the type of goods or services being sold.

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

Originators of WEB transactions must conduct an annual data security audit to ensure that Receiver's financial information is protected by security practices and procedures that ensure the financial information the Originator obtains from Receives is protected by commercially reasonable security practices that include adequate levels of:

a. Physical security to protect against theft, tampering, or damage;

b. Administrative, technical, and physical access controls to protect against unauthorized access and use; and

c. Network security to ensure secure capture, transmission, storage, distribution and destruction of financial information.

This audit requirement can be met in several ways. It can be a component of a comprehensive internal or external audit, or it can be an independent audit that uses a commercially reasonable generally accepted security compliance program. An Originator that is already conducting an audit of these practices and procedures for another area of its business is not required to have two separate audits; however, the audit should address adequate levels of data security for the Originator's ACH operations. Possible re-tooling of ACH Originators' fraud detection systems ◦Or implementation of a system for Originators who currently do not perform any fraud detection for WEB debits

Originators of WEB transactions are Required to Verify Routing Numbers.

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

Verifying the validity of routing numbers can be accomplished by:

• a component of a fraudulent transaction detection system,

• through a separate database or directory (either commercial or proprietary), or

• through other methods devised by the Originator, for example manual intervention such as calling the Receiver's financial institution.

Telephone Initiated Entries (TEL)

A TEL is a consumer debit entry that is authorized orally via the telephone. A TEL may only be transmitted in circumstances in which:

a. There is an existing relationship between the Originator and the Receiver; or

b. There is not an existing relationship between the Originator and Receiver, but the Receiver originated the telephone call to the Originator.

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

a. There is a written agreement in place between the Originator and Receiver for the provision of goods or services, or

b. The Receiver has purchased goods or services from the Originator within the last two years.

An Originator of TEL transactions is required to:

a. Establish and implement commercially reasonable procedures to verify the identity of the Receiver.

b. Establish commercially reasonable procedures to verify routing numbers are valid.

Authorization Requirements. Originators of TEL transactions must obtain the Receiver's explicit oral authorization before initiating a debit entry to a consumer's account. For both Single Entry and recurring TEL entries, the Originator must clearly state during the telephone conversation that the consumer is authorizing an ACH debit entry to his account. The Receiver must explicitly express consent. Silence is not express consent. The following are additional authorization requirements:

a. The date on or after which the Receiver's account will be debited;

b. The amount of, or a reference to the method of determining the amount of, the debit entry to the Receiver's account;

c. The Receiver's name or identity;

d. The account to be debited;

e. A telephone number that is available to the Receiver and answered during normal business hours for customer inquiries;

f. The method by which the Receiver can revoke the authorization;

g. The date of the Receiver's oral authorization; and

h. A statement by the Originator that the authorization obtained from the Receiver is for a Single Entry. If the entry is to be recurring, then the timing, number, and/or frequency of the transactions should be outlined.

In addition to these requirements the Originator must comply with all requirements related to telemarketing practices including the Telephone Consumer Protection Act (TCPA) and all updates to these rules as they may be implemented.

Originators of TEL transactions are Required to Verify Routing Numbers.

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

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

Verifying the validity of routing numbers can be accomplished by:

• a component of a fraudulent transaction detection system,

• through a separate database or directory (either commercial or proprietary), or

• through other methods devised by the Originator, for example manual intervention such as calling the Receiver's financial institution.

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

• Debit the Receiver without obtaining the Receiver's authorization for such a transaction;

• Cold call consumers with whom they have no existing relationship and subsequently debit the Receiver; and/or

• Use mail solicitations to instruct the consumer to initiate the telephone call to the Originator and subsequently attempt to sell goods or services using deceptive marketing practices.