# WEB Proof of Authorization Industry Practices

**Contributors: Susan Pandy, *NACHA*; Kerry Sellen, *First Data*; Brad Smith, *EastPay***

A common challenge among ACH Network participants that originate or process WEB ACH consumer debit transactions is determining what information should be collected and retained so that there is adequate proof of authorization in the event that the transaction is challenged. Currently, no common set of requirements exist to guide the industry in establishing common practices or guidelines. A set of common practices is difficult to establish because the ability to prove that a transaction was properly authorized is highly dependent on the attributes of the authorization process and any underlying processes used to validate identity, all of which may vary among institutions, transaction types and operating models. Hence, the authorization process itself is a critical component to understand in determining how a company may demonstrate proof of such authorization. Furthermore, the authorization process cannot be fully understood without also understanding the underlying authentication methods used to support it in verifying the identity of the consumer that is authorizing the transaction. The next section briefly reviews the complementary nature of these two concepts of authorization and authentication and their relationship to supporting proof of a properly obtained authorization.

# Understanding the Importance of Authorization and Authentication for WEB ACH

Authorization occurs when the Originator and the consumer (the Receiver) enter into an agreement to allow the Originator to initiate a debit entry to the consumer's account. Both the *NACHA Operating Rules* and Regulation E (under the Electronic Fund Transfer Act) govern WEB Entries, and it is important that Originators understand the authorization requirements and related responsibilities before they begin initiating WEB Entries to consumer accounts. Please review the most current version of the *NACHA Operating Rules & Guidelines* for detailed information regarding the initiation of WEB Entries. The authorization process for WEB is different from most other types of ACH transactions because it takes place over the Internet or a wireless network, where it can be more difficult for parties to determine with whom they are doing business. For this reason, in addition to the normal warranty that an Entry is properly authorized (Rule 2.4.1.1), the Rules also contain a specific warranty that the Originator has established and implemented commercially reasonable methods of authentication to verify the identity of the Receiver of the WEB Entry (Rule 2.5.17.5(b)). A transaction cannot be considered properly authorized without adequate authentication of the consumer.

The range of available authentication technologies is broad and those technologies vary in complexity. For a review of authentication technologies that are available in the marketplace, please see The Internet Council's eResource "*The Basics of Authentication in the ACH Network*". The level of risk associated with the transaction will dictate the technology that is used and the manner in which it is deployed. Multifactor authentication is an example of one industry utilized method for robust authentication. It uses multiple characteristics to determine a consumer's identity, typically by obtaining and verifying more than one of the following: something the consumer knows (password), plus something the consumer has (a personal computer), something the consumer is (voice or fingerprint), and someplace the consumer is (geolocation).

The industry's increasing use of multifactor authentication was influenced in part by the release of the FFIEC's guidance to financial institutions in the October 2005, *Authentication in an Internet Banking Environment*, and subsequently updated in the 2011 Supplement available at http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf. As indicated in that guidance, however, multifactor authentication is only one of a range of options, including various types of layered security, that may be used by banks to protect against unauthorized transactions. It is important for Originators to understand trends in risk mitigation controls, and referring to this guidance and its current and future updates is a good way to stay abreast of authentication technology trends for the banking industry.

A business using WEB Entries must determine which authorization and authentication methods should be used based on its risk management approach. Properly authorized WEB transactions will result in fewer unauthorized returns and a reduction in losses. This helps mitigate risk for ODFIs and their business customers by minimizing returns and potential violations of the *NACHA Operating Rules*.





# Authorization Considerations for WEB ACH Transactions

### A. ODFI Considerations for Authorization

ODFIs may want to communicate guidelines on what information should be captured for proving authorization in the origination agreement between the ODFI and its corporate originators. ODFIs may also want to consider offering on boarding / counseling services to Originators and providing training to clients where they can specifically address proof of authorization needs for ACH transactions, coupled with a copy of the *NACHA Operating Rules*. The amount of counseling, training and oversight provided to Originators may vary according to the business models and risks posed by different types of Originators.

Additional education can be provided to Originators by using tools such as worksheets that outline all of the NACHA Operating Rules pertaining to the SEC Codes that the Originator will be offering based on its agreement with the ODFI. This worksheet can include sections for special topics, such as the specific requirements for WEB ACH and the capacity to demonstrate proof of authorization. ODFIs may wish to have Originators sign off on the worksheet to provide additional acknowledgment of understanding of the requirements by the Originator outside of existing agreements.

Some ODFIs leverage the return rate threshold as a trigger for a staggered warning process or termination of a client origination relationship. This type of information can also be used to trigger requests for Originators to provide what they are collecting for proof of authorization. However, requests for proof of authorization should not be solely based on triggering events, but should be incorporated into an ODFI's broader risk management strategy.

### B. Originator Considerations for Authorization

Although the NACHA Operating Rules require that certain information be included in the consumer's authorization, the Rules do not require that the authorization contain specific language or be in any particular format. The following pieces of information should be included in the authorization:

1. Express authorization language (e.g., "I authorize Company A" to debit my account)
2. Amount of transaction: for recurring transactions this could be the same amount each time or it could be for a range of amounts or amounts that are determined on the basis of specified activity
3. The date(s) and/or frequency of the transaction(s)
4. The consumer's account number
5. The consumer's financial institution's routing number
6. Revocation language (for recurring payments or payments scheduled in advance)

When considering how to prove that a transaction was properly authorized, the Originator should provide documentation that shows transaction details including consumer information and sales documentation to show what goods and/or services were exchanged. For example, some of this documentation can be captured in the form of a screen shot of the authorization language, plus the date and timestamp of the consumer login, and the authorization process that evidenced both the consumer's identity and his assent to the authorization. In effect, capturing these details helps to demonstrate the processes that were used to verify the customer's identity as well as the processes used to support the authorization. [1]

---

[1] See Chapter 48, Internet Initiated / Mobile Entries

### C. Information Retention

The ability for the Originator to accurately and positively demonstrate that an authorization occurred is important. Under the *NACHA Operating Rules*, Originators must retain the original or a copy of each written authorization of a Receiver, or a readily and accurately reproducible Record evidencing any other form of authorization, for two years from the termination or revocation of the authorization (Article II, Subsection 2.3.2.5, p. OR 6) and be able to provide these records to the ODFI upon request. In a situation where the authorization is not physically signed, but rather is "similarly authenticated," such as with a WEB Entry, the Originator must keep a copy of the authorization and a record of the process used to link that authorization to the consumer.

## Common Industry Practices for Capturing Proof of Authorization for WEB ACH

The following section discusses some of the methods that are available for satisfying authentication needs. In order to satisfy authentication requirements, ODFIs may wish to consider utilizing a combination of the following methods based on their overall risk management strategy. NACHA does not endorse any specific technology or approach, as each ODFI must consider which technologies, processes and procedures are most appropriate for managing risk.

Based on information obtained from member Financial Institutions, Originators and Third-Party Service Providers, a combination of the following practices is common:

### A. Consumer/Receiver IP Address Capture/Audit Log

Computers connected to the Internet must speak the "Internet language" called the "Internet Protocol," or simply IP. Each computer is assigned a unique address somewhat similar to a street address or telephone number. Every computer, whether it functions as a website, is being used by a web surfer, is a mail server, and/or is used for any other function, has an IP address so it can communicate across the Internet. Communication is accomplished by sending pieces of information called "packets" that include the IP address of the destination computer. This information can be captured and tracked in order to trace the user and identify anomalies in IP address use, which could trigger investigations of potentially fraudulent transactions. This information can also be used to provide additional information about or confirmation of the authorization process.

### B. Screen Shot Capture

A screen shot capture is a screen shot of the authorization language displayed to the consumer on the Originator's website that captures how the consumer assents to the transaction by such actions as clicking on an "I agree" button or entering some digital code or shared secret. A simple screen shot of the authorization language presented and agreed upon by the consumer does not constitute adequate proof of authorization as it does not establish any link to the accountholder and the authorization. The need is to demonstrate the process by which the consumer authorized the transaction, including the underlying verification/authentication process that links identity to the authorization, such as a digital code, password, shared secret, date and time-stamp of consumer log-in. In addition to documenting the process used to evidence assent to the authorization, the Originator should document the process used to evidence that the authorization was provided by a known consumer.





### C. Date and Time-Stamp of Consumer Login

Maintaining a record and capturing the date and time-stamp of the consumer's login and authorization can be used to audit WEB transactions and provide additional information about or confirmation of the authorization process.

## Recommendations for WEB Proof of Authorization Practices

ODFIs and Third-Party Service Providers should consider, based on their specific circumstances:

- requesting a dummy account from their Originators to log in and view the various screens presented to the consumer to initiate a WEB transaction.
- establishing an education and counseling process for WEB Originators.
- regularly monitoring the WEB transaction activity of Originators for any significant changes in return rates or authorization processes.
- creating examples of terms and conditions language for Originators to display on their websites to consumers.
- developing a checklist of industry practices for authentication.

---

### Appendix A - Sample WEB Authorization Language

****SAMPLE**  Authorization Form  **SAMPLE****

Before getting to the screen where the consumer will give his or her authorization, or on that screen, a method that is compliant with the E-Sign Act that similarly authenticates the consumer must be used. Methods used could include a personal identification number, password, etc. Authentication at the time of sign-on to the website may be adequate authentication for a click-through authorization as part of the same session, however, Originators need to consider if authentication at the time of sign-in is enough to link the account holder to a later authorization should they be required to produce proof of authorization/authentication. In addition to any information the company includes to identify the payment being made, the authorization must include the consumer's assent to the transaction. *This authorization language, and the related screen flow, is only a sample. We strongly recommend that prior to using any authorization or authorization language you receive approval from your legal counsel.*

**Screen 1:**

To pay your (Company Name and type of bill), enter amount below and click the PAY button
Amount: $_____

**Screen 2:**

I authorize _____ (Company Name) hereinafter named COMPANY to initiate a single or __#___ recurring ACH/electronic debit to my account in the amount of $XXX.XX from (can specify either “bank account on record” if account information is retained once it is entered, or provide a space for the entry of account information: checking or savings account, Depository Name, Routing Number and Account Number) on _____(date and/or frequency of debits).

I agree that ACH transactions I authorize comply with all applicable law.

IF THE PAYMENT IS SCHEDULED IN ADVANCE OR THE AUTHORIZATION IS FOR RECURRING DEBITS, INCLUDE THE FOLLOWING:

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

Payments made after X:XX P.M eastern time will be applied as of the next business day.

To complete the payment process, click the “authorize” button. Once payment is authorized, there cannot be any changes or corrections.

It is recommended that you print a copy of this authorization and maintain it for your records.


**Screen 3:**

Thank you for your payment. The confirmation below verifies that you have authorized (Company Name) to initiate an electronic payment from your bank account.

Payment Confirmation Number: XXXXXX

Authorized Payment Amount: XXX.XX

Date Authorized: XX/XX/XXXX

Expected Payment Date; XX/XX/XXXX