ALERUS

ACH ORIGINATION

WEB VS. PPD PAYMENTS

WEB Payment

A **debit entry originated by a business to debit a consumer** based on an authorization that is communicated, other than by oral communication via a telephone call, from the receiver to the originator **via the internet or wireless network**.

— Nacha Rules Book

If your business is debiting a consumer, and they have delivered their authorization via the internet or wireless network, then the transaction should be processed as a WEB payment.

There are additional responsibilities for originators who are processing WEB payments to ensure the security and accuracy of the transaction information for their consumer clients.

PPD Payment

A **credit or debit originated by a business to/from a consumer's account** based on an authorization from that **consumer**. This can be a standing order or a single-entry authorization from that consumer.

— Nacha Rules Book

If your business is crediting or debiting a consumer, and they have delivered their authorization in writing, in person, or via the mail, then the transaction should be processed as a PPD payment. The key difference from a WEB payment is that the signed authorization is delivered in person or via mail.

FAQ

Am I required to obtain authorization prior to processing a WEB or PPD payment?
In both cases if you are *debiting* a consumer, you must have a documented authorization on file. It is recommended to obtain written authorization for PPD credits; however, this is not required.

What needs to be included in the ACH authorization?
For both WEB and PPD transactions the language can be similar. See the TM Resource Center for sample authorization forms.

The authorization must include:

- Receiver's name
- Amount of the entry(ies) or a reference to the method of determining the amount
- Timing (including start date), number, and/or frequency of entries
- Account to be debited
- Date of the receiver's authorization
- How the receiver may revoke the authorization directly with the originator. This should include the time and manner in which the receiver's communication with the originator must occur, (i.e., how much time the originator needs to be notified in advance to give them reasonable opportunity to act on the revocation request).

Standing Authorization Usage

Type	Receiver's Affirmative Action		
	Written Request	Telephone Call	Internet/Wireless Network[1]
In writing	PPD	PPD or TEL	PPD or WEB
Telephone	TEL	TEL	TEL or WEB
Internet or wireless network	WEB	WEB or TEL	WEB

WEB or PPD Payment Usage Examples

Use Case	WEB or PPD	Reason
Consumer comes into your business and requests to be debited automatically. They complete the form in your office and hand it to your team member for processing.	PPD	"Wet" signature delivered in person
Consumer prints a form from your website, completes the form, signs it, and mails the form to your business for processing.	PPD	"Wet" signature, sent via postal mail
Consumer comes into your business and signs the authorization form using a pin pad.	PPD	Signed and delivered in person
Consumer prints a form from your website, completes the form, signs it, and emails the form to your business for processing. (It is not recommended to deliver sensitive information via email.)	WEB	Submitted via internet/ wireless network
Consumer completes the form and acknowledges your business may debit them based on the criteria outlined in the authorization via your website.	WEB	Submitted via internet/ wireless network
Consumer delivers authorization in person but sends an email or text message to communicate when to initiate the payment (authorization frequency).	PPD	Standing authorization in writing. Payment frequency via internet/ wireless network

WEB Originator Responsibilities

- If using electronic signature, must be compliant with E-SIGN Act[2] for the electronic signature/authorization. Prompt the receiver to print/save a copy of the authorization confirmation.
- Utilize a commercially reasonable method of authorization to verify the person signing into your website to authorize entries is the person they say they are.
- Utilize a commercially reasonable process to verify that the routing number used is valid.
- Utilize a commercially reasonable fraud detection system to screen the WEB debit entries. At minimum, this validation process must be completed for the first use of an account when an account changes. This can be done with prenotes, micro-entries, or an application/API, (e.g., Plaid).
- If requested, originator must be able to provide proof of authorization. For a WEB entry, this will include a screenshot/printout of the authorization language and an audit log showing the steps from user being authenticated to their authorization of entry. Audit log should include date/time stamps, user ID, IP address, transaction details, etc.

[1] Includes Alexa, Skype, website, text message, app.
[2] Electronic Signatures in Global and National Commerce Act.

- Complete an annual WEB debit security audit to verify security practices and procedures for data collection, storage, and retention to ensure adequate levels of:
  - Physical security to protect against theft, tampering, or damage
  - Personnel and access controls to protect against unauthorized access and use
  - Network security to ensure capture storage and distribution

For full details on the Nacha rules, you may purchase a rules book through UMACHA.