



paymentAccess

HTTP Integration API

Implementation Guide

Version 3.0.6

Revised: 6/25/09

1627 W. Main Street

Bozeman, MT 59715

(800)-305-1534

www.paymentAccess.com



Notice of Proprietary Information

Information contained herein is subject to change without notice and does not constitute a commitment on the part of paymentAccess, Inc. (**PAYMENTACCESS**). Except for use by customers for obtaining **PAYMENTACCESS** products and services, no part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the express written permission of **PAYMENTACCESS**. Any unauthorized duplication is in violation of U.S. copyright and other laws, and can result in severe monetary and criminal damages.

Applicability

This document is intended to provide information on the use of the paymentAccess HTTP API and the format for using the service.

Customer Support

Support Line: (800) 305-1534

Support Fax Line: (888) 431-4698

E-mail Address: support@gotobilling.com

Table of Contents

Notice of Proprietary Information	2
Applicability.....	2
Customer Support	2
Document History	1
Overview	2
Purpose	2
Notes about the Merchant IDs and PINs.....	2
Use of the x_payment_account_ID field.....	2
Data Types Conventions	3
Transaction Fields	4
MERCHANT LOGIN	4
CUSTOMER INFORMATION.....	5
TRANSACTION INFORMATION	6
TRANSACTION INFORMATION – ACH.....	9
TRANSACTION INFORMATION – Credit Card.....	10
GATEWAY RESPONSE API.....	12
Non-Rely Response.....	12
Example Non-Relay Response Data:.....	13
Relayed Response	14
<i>Example Relay Response Data:.....</i>	<i>14</i>
<i>Example Non-Relay Response Data with ACH Verification Decline message:.....</i>	<i>14</i>
Debug and Test Card Information	14
APPENDIX A – Transaction Types.....	15
Credit Card Transaction Types	15
ACH Transaction Types	15
APPENDIX B – ACH Payment Types	16
ACH Payment Types.....	16
<i>WRITTEN.....</i>	<i>16</i>
<i>WEB.....</i>	<i>16</i>
<i>TEL.....</i>	<i>19</i>
<i>ARC.....</i>	<i>20</i>
<i>RCK.....</i>	<i>23</i>
APPENDIX C – Development Resources	26
Validate Bank ABA (Routing) Numbers.....	26
<i>Language: Javascript.....</i>	<i>26</i>
<i>Language: PHP.....</i>	<i>27</i>

General Credit Card Validation	27
<i>MOD 10 Check Digit</i>	27
<i>Card Prefix Check</i>	28
<i>Card Length Check</i>	28

Document History

Revision	Date	Changes	Name
2.0-2.0.1		Added x_relay_url (p.4), x_relay_type (p.4), and x_debug (p.4) Gateway request fields. Updated x_customer_id field description (p.4).	Jed Danner
2.0.1-3.0		Added x_ach_verification	Jed Danner
3.0.1		Added x_occurrence_type and x_occurrence_number, for submitting recurring transactions	Jed Danner
3.0.2		Added transaction type 'RM'	Jed Danner
3.0.3	11/20/08	Changed url from www.gotobilling.com to secure.gotobilling.com	David Durick
3.0.4	2/13/09	ip_address is server address; extra description on check verification and responses; Explanation on responses for transactions; changed time for VOIDS from 5:30am to 10pmET; Not using BC and BS business designations; added fields x_source_description and x_module_description	David Durick
3.0.5	6/16/09	Added more Debug capability with specific card numbers giving specific responses. A Reference ID for a particular payment account can now be passed x_payment_account_id	David Durick
3.0.6	6/25/09	Added additional information about the use of the x_payment_account_id in the overview section	David Durick

Overview

Purpose

The Gateway Submission API defines the type of information that may be sent to the gateway. When transmitting data to the gateway, information should be posted to <https://secure.gotobilling.com/os/system/gateway/transact.php>.

PAYMENTACCESS recognizes and processes both GET and POST methods. The interface between the ISP and **PAYMENTACCESS** is the standard HTTP/1.0 (or HTTP/1.1) protocol using Secure Sockets Layer (SSL) encryption.

Transactions are broken up into delimited fields. A transaction is transmitted either in the request header for the GET method, or following the request headers for the POST method.

Notes about the Merchant IDs and PINs

1. Merchant IDs (also called Merchant-IDs) and PINs are issued by PaymentAccess upon approval of a merchant's account application. These are sensitive fields that must remain confidential. Under *no* circumstances should the contents of these fields be available to the shopper, either on-screen or through a browser's View/Source command. Instead, they should be filled in by the merchant's web application prior to forwarding to **PAYMENTACCESS**.
2. Merchants must be approved in advance to submit electronic check credit transactions. Once approved, specific conditions apply.

Use of the x_payment_account_ID field

The Purpose of the x_payment_account_ID field is to allow a “one-time” sending of the Credit Card number or the Route and Account number (for an ACH transaction) and then be able to reference it in the future without needing to send the card number or account number again. This allows an application to be developed where it does not have to store these sensitive numbers but instead paymentAccess is the only place these numbers are stored securely. A future transaction may be as simple as needing to process a credit card refund or an ACH credit. This can now be accomplished if the associated x_payment_account_ID from the original transaction is sent. Therefore, the application must keep a database of x_payment_account_ID's for all transactions sent if future transactions using this field are to be performed. The following are the basic points regarding using this feature:

1. Initially the payment account information (CC Number, ACH Account) can be sent along with the x_payment_account_id.
2. The account can then be accessed in the future simply by passing the x_payment_account_id for the desired account. The individual account information is not needed.

3. If any account information is passed with an existing `x_payment_account_id`. That account information will be updated to match the information given.
4. The `x_payment_account_id` should be unique. Technically it only has to be unique per Customer ID (`x_customer_id`) but it might be easier to design if it is unique across the entire Merchant ID (`merchant_id`) so there's no duplication at all. One suggestion would be to have the `x_payment_account_id` be the `x_customer_id`+(some value) where the value could be the date in YYYYMMDD format. This would facilitate easier research if needed and would likely be easier to implement than other numbering schemes. Especially since the `x_customer_id` must be unique across the Merchant ID.
IMPORTANT NOTE: Validation for the uniqueness of this field will be added in the future, however it is not currently live.

When using the `x_payment_account_id` to reference an existing credit card on file, the following credit card fields are not needed as they will already be on file in `paymentAccess` when the original transaction was sent:

`x_cc_type`
`x_cc_name`
`x_cc_number`
`x_cc_exp`

For ACH transactions, the following fields will not be needed since they will be on file:

`x_ach_route`
`x_ach_account`
`x_ach_account_type`

Data Types Conventions

Modifier	Definition
a	Alpha characters [a-z, A-Z]
n	Numeric digits [0-9]
s	Special characters [-_:@&+##\$/'=-~^]

Transaction Fields

Field	Required	Max Length	Description
MERCHANT LOGIN			
merchant_id	Required	n. 6	Merchant ID assigned by PaymentAccess
merchant_pin	Required	an. 20	Merchant Pin associated with the Merchant ID. Assigned by PaymentAccess
ip_address	Required	an. 12	This field is to allow PAYMENTACCESS to research fraud attempts. It contains the IP address of the originator of the transaction. It is the IP address of the server sending the transaction to PaymentAccess, not the IP address of the end customer entering the transaction.
x_relay_url	Optional	an. ..	Contains the URL to which the gateway will post the response. Include http:// or https://. When set the gateway response will automatically be sent via HTTP POST to this location.

x_relay_type	Optional	a. 7	Indicates the type of action of the response. When ACTIVE is set the browser will automatically be sent to the location specified with x_relay_url. When PASSIVE is set the browser will not be redirected, but the response will be sent to the location specified with x_relay_url via HTTP POST. This is set to default to PASSIVE
x_debug	Optional	n. 1	When set to 1 (numerical one) transactions will be sent in test mode. A response will be given for the transaction, but no processing will occur. Default: 0 (zero).
CUSTOMER INFORMATION			
x_customer_id	Required	an 32	A unique customer Identification number set by the merchant.
x_company	Conditional	an 32	The company associated with the billing address. Either first name & last name, or company name must be given.
x_last_name	Conditional	an 32	The last name of the customer associated with the billing address. Either first name & last name, or company name must be given.
x_first_name	Conditional	an 32	The first name of the customer associated with the billing address. Either first name & last name, or company name must be given.
x_address1	Optional	an 32	The address associated with the billing address

Transaction Fields

x_address2	Optional	an 32	Continuation address associated with the billing address
x_city	Optional	a 40	The city associated with the billing address
x_state	Optional	a 2	The state associated with the billing address. The state is formatted using the two letter post abbreviation. Example: FL
x_zip	Optional	ns 10	The zip code associated with the billing address
x_phone	Optional	n 10	The phone number of the customer associated with the billing address. Does not contain any dashes – ex. 2223334444
x_email	Optional	ans 50	The email of the customer associated with the billing address.
TRANSACTION INFORMATION			
x_transaction_type	Required	2	<p>This field identifies the type of transaction being submitted. Valid transaction types are:</p> <p>Credit Card Type:</p> <ul style="list-style-type: none"> • AS – Authorize Only • DS – Capture Only (Force) • ES – Authorize & Capture • CR – Credit/Refund • VO – Void <p>ACH Transactions:</p> <ul style="list-style-type: none"> • DH (Electronic Check Debit) • DC (Electronic Check Credit) <p>Delete Pending Transactions:</p> <ul style="list-style-type: none"> • RM

x_invoice_id	Required	an 32	<p>Unique transaction ID field specified by the merchant. Also used in determining duplicate submissions.</p> <p>For transaction type 'RM' this can be set to a specific id to remove a single transaction, or can be set to 'ALL' to remove all transactions currently pending for the given customer id.</p>
x_amount	Required	n 10	<p>Amount to be charged or credited. Amount may be formatted with or without a decimal. If no decimal is given two (2) decimal places are assumed (1.00 = 100).</p>
x_process_date	Optional	n 8	<p>Date on which the transaction is to be processed. If no date is given, the transaction will default to the date it is submitted on.</p> <p>Format: YYYYMMDD</p>
x_invoice_file	Optional		<p>File containing information to be sent to customer via email when the transaction is processed.</p>
x_payment_account_id	Optional	an 20	<p>1) Initially the payment account information (CC Number, ACH Account) can be sent along with the x_payment_account_id.</p> <p>2) The account can then be accessed in the future simply by passing the x_payment_account_id for the desired account. The individual account information is not needed.</p> <p>3) If any account information is passed with an existing x_payment_account_id. That account information will be updated to match the information given.</p> <p>The x_payment_account_id should be unique. Validation will be added for this, however it is not currently live.</p>

Transaction Fields

x_memo	Optional	ans 255	Description of transaction to be forwarded to the customer.
x_notes	Optional	ans 255	Internal notes to be stored with the transaction.
x_occurrence_type	Optional	an 10	Used for setting up recurring transactions. Available types: <ul style="list-style-type: none"> • week • biweek • month • bimonth • semiannual • annual
x_occurrence_number	Optional	n 3	Specify the number of occurrences for a recurring transaction. If no occurrence number is giving, the default will be set to indefinite until deleted manually.
x_source_description	Optional	an 20	This is to be used by the developer to send the name and version number of the software that is sending the transactions. It's a free form description field to tell GTB the source of the transactions.
x_module_description	Optional	an 20	This field is used by the developer to send the name and version number of a module or plugin that was built using this API. This allows for proper tracking of plugins or modules that may be built and then used in other software applications. The end software application name and version number would be put into the "source_description" field.

TRANSACTION INFORMATION – ACH			
x_ach_payment_type	For ach transactions: Required	a 3	<ul style="list-style-type: none"> • PPD (Prearranged Payment and Deposit Entry). Used to submit prearranged credit and debit transactions such as payroll deposits and periodic bill payments against a consumer's account. • WEB (Internet-Initiated Entry). Used to submit debit entries pursuant to an authorization that has been obtained from the consumer via the Internet. • TEL (Telephone-Initiated Entry). Used to submit transactions pursuant to an oral authorization obtained from the consumer via the telephone. NACHA regulations require that either the session in which the order was taken be recorded, or the consumer be notified in writing prior to initiation. • ARC (Accounts Receivable Entry): Used to submit ACH debits for consumer checks received via the U.S. mail or at a drop-box location for the payment of goods or services. The consumer's source document (e.g. the check) is used to collect the consumer's routing number, account number, check serial number, (in raw MICR format) and the dollar amount for the transaction.
x_ach_route	For ach transactions: Required or Conditional	n 9	Routing number of the bank associated with the customer's bank account. Can send the x_payment_account_id to reference an existing Route and Account.
x_ach_account	For ach transactions: Required or Conditional	n 20	Account number associated with the customer's bank account. Can send the x_payment_account_id to reference an existing Route and Account.

Transaction Fields

x_ach_account_type	For ach transactions: Required Or Conditional	a 2	<p>Personal Accounts</p> <ul style="list-style-type: none"> • PC – Personal Checking • PS – Personal Savings <p>Business Accounts (<i>Business designations currently not in use-they would create CCD transactions vs. PPD</i>)</p> <ul style="list-style-type: none"> • BC – Business Checking • BS – Business Savings <p>Not needed if x_payment_account_id is sent to reference an existing account</p>
x_ach_serial	Conditional	n 10	Check number of the transaction being submitted. Required for Payment Type ARC
x_arc_image	Conditional	an 22	TIF image file associated with ARC transactions
x_ach_verification	Conditional	n 1	Set to 1 to enable.. otherwise default is off. There are two levels of ACH verification but that is set on the Account level at PaymentAccess. If an ACH transaction receives an Authorization the status sent back will be R, if it is Declined, the status will be D.
TRANSACTION INFORMATION – Credit Card			
x_cc_type	For cc transactions: Optional	a 2	<p>Card Types:</p> <ul style="list-style-type: none"> • VS – Visa • MC – MasterCard • AX – Amex • DC – Discover
x_cc_name	For cc transactions: Optional	a 32	Contains the name located on the credit card

x_cc_number	For cc transactions: Required or optional	n 22	Contains the credit card number. Can send the x_payment_account_id to reference an existing Credit card on file.
x_cc_exp	For cc transactions: Required Or optional	n 4	Contains the expiration date for the credit card. Format: MMY Can send the x_payment_account_id to reference an existing Credit card on file
x_cc_cvv	For cc transactions: Optional	n 4	Three or Four digit validation number for the credit card
x_authorization	For cc transactions: Conditional	n 32	Authorization number of a transaction previously authorized by the gateway. This is required for the following transaction types: DS, CR, VO

GATEWAY RESPONSE API

The Gateway Response API defines the type of information that will be sent by the gateway once a transaction has been processed.

Non-Rely Response.

Gateway Responses are delimited by the *PAYMENTACCESS* tags:

```
<ResponseData>
</ResponseData>
```

Tag Name	Description
<status></status>	<p>Transaction Status. Values are:</p> <ul style="list-style-type: none"> • G - Approved • R - Received • D - Declined • C - Cancelled <p>-----</p> <p>Response Statuses for Various Transaction Types: Credit Card: AS (G)</p> <ul style="list-style-type: none"> • AS – Authorize Only (G if approved) • DS – Capture Only • ES – Authorize & Capture (G if approved) • CR – Credit/Refund • VO – Void <p>Future dated transactions always get R on both Credit Card and ACH transactions.</p> <p>When using the ACH Verification option, if an ACH transaction receives an Authorization the status sent back will be R, if it is Declined, the status will be D. An authorization number is supplied and <description> contains detailed response data on Declines.</p>
<order_number></order_number>	<p>A 22-digit code, formatted nnnn-nnnnn-nnnnn, used by PAYMENTACCESS to synchronize and track transactions and orders. It is not used or recognized by the PAYMENTACCESS host computers.</p>
<term_code></term_code>	<p>The reason the PaymentAccess process terminated. Values are:</p> <p>30998 Internal software error. 20999 Missing or invalid Merchant-ID</p>

	<p>20998 Could not validate Merchant-ID 20997 Invalid server (potential security violation) 20996 Missing transaction type 20995 Invalid transaction type 20994 Reserved 20993 Reserved 20992 Reserved 20991 Reserved 20990 Reserved 20989 Both Card and Check services are turned off 20988 Merchant is not approved for service 20987 Reserved 20986 Reserved 20985 Reserved 20984 Reserved 20983 Reserved 20982 Reserved 20981 Reserved 20980 Reserved 20979 A required transaction field is missing 20978 A required transaction field is invalid/missing 0 Normal Termination</p> <p>On 20979 and 20978 the <description> field will tell what field it is that is missing or invalid.</p>
<tran_amount></tran_amount>	The amount of the transaction. This field should be the same as the field x_amount in the submitted transaction (see above).
<tran_date></tran_date>	Date Stamp of when the transaction was processed. Format: YYYYMMDD
<tran_time></tran_time>	Time Stamp of when the transaction was processed. Format: HHMMSS
<invoice_id></invoice_id>	Echo of merchant submitted Order ID
<auth_code></auth_code>	Reference number identifying the transaction on the gateway
<description></description>	Description of any error or decline returned for the transaction.

Example Non-Relay Response Data:

```
<ResponseData><status>R</status><order_number>122879-20050804-985829</order_number><term_code>0</term_code><tran_amount>12.33</tran_amount><tran_date>20050804</tran_date><tran_time>091121</tran_time><invoice_id>123549854</invoice_id></ResponseData>
```

Relayed Response

A relayed response will contain the same information, but will be formatted in a HTTP REQUEST string. Active being POST and Inactive being GET.

Example Relay Response Data:

```
?status=R&order_number=122879-20050804-985829&term_code=0&tran_amount=12.33&tran_date=20050804&tran_time=091121&invoice_id=123549854
```

THIS EXAMPLE IS UNDER CONTRUCTION:

Example Non-Relay Response Data with ACH Verification Decline message:

```
<ResponseData><status>D</status><order_number>122879-20050804-985829</order_number><term_code>0</term_code><tran_amount>12.33</tran_amount><tran_date>20050804</tran_date><tran_time>091121</tran_time><invoice_id>123549854</invoice_id></ResponseData>
```

Example Declined Verification:

```
<ResponseData>
  <status>D</status>
  <order_number>122879-20081217198384</order_number>
  <term_code>0</term_code>
  <tran_amount>1.01</tran_amount>
  <tran_date>20081217</tran_date>
  <tran_time>131643</tran_time>
  <invoice_id>44444</invoice_id>
  <description>CHEXDIRECT      <br />DECLINE CHECK      <br /> 3 UNPAIDS
  (ALL)<br />UNPAID AMT=    35<br />PHN 800-238-5888<br />EXPRESS RECOVERY<br
  /></description><
/ResponseData>
```

Debug and Test Card Information

We also have some updated debug methods, which will be in the next version of the documentation.

With this, while in debug mode (x_debug=1), you can trigger the gateway to give you an approve, decline or error based on the reset of the information sent over.

Card #s that will return an approval "G"

```
3700000000000002
6011000000000012
40070000000027
5424000000000015
```

Card #s that will return a decline "D"

```
42222222222222
```

All other Card#s return an error "E"

APPENDIX A – Transaction Types

Credit Card Transaction Types

Transaction Type	Description
Authorize & Capture	Transaction of this type will be sent for authorization. The transaction will be automatically picked up for settlement if approved.
Authorize Only	Transactions of this type will validate the credit card for the amount submitted
Capture Only	This is a request to settle a transaction that was not submitted for authorization through the payment gateway
Credit/Refund	Indicates to the gateway that money should flow from the merchant to the customer. Must have a valid transaction Reference Number.
Void	This is an action on a previous transaction and is used to cancel the previous transaction and ensure it does not get sent for settlement. A VOID request must include a validate transaction Reference Number and must be received before 10:00 pm ET which is the standard auto batch out time for most merchants. However, this can vary from merchant to merchant. You will receive D (Decline) status if you cannot VOID.

ACH Transaction Types

Transaction Type	Description
Debit	Debit transactions are used to move money from the customer to the merchant.
Credit	Credit transactions are used to move money from the merchant to the customer.

APPENDIX B – ACH Payment Types

ACH Payment Types

Notes

- The following are rules set forth by NACHA and the Federal Reserve and may be changed or amended by those governing bodies. Updates and amendments to these rules and regulations can be obtained from NACHA and the Federal Reserve Bank.

WRITTEN
<p>Originators of WRITTEN entries must obtain the consumer's authorization prior to initiating a debit entry under this application. Authorization is obtained by gaining written permission from the customer including: the account to be debited, the dates that the customer's authorization is valid, and the customer's signature.</p>
WEB
<p>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.</p> <p>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.</p> <p>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.</p>

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 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.

* 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.

TEL

A TEL entry may be transmitted only in circumstances in which (1) there is an existing relationship between the Originator and the consumer, or (2) there is not an existing relationship between the Originator and the consumer, but the consumer has initiated the telephone call to the Originator. A TEL entry may not be used by an Originator when there is no existing relationship between the Originator and the consumer, and the company has initiated the telephone call. The Originator and the consumer are considered to have an existing relationship when either (1) there is a written agreement in place between the Originator and the consumer for the provision of goods or services (e.g., the consumer has an insurance policy with the Originator), or (2) the consumer has purchased goods or services from the Originator within the past two years. For purposes of these Rules, an affiliate of an Originator that has an existing relationship with a Receiver is not deemed to have such an existing relationship with the Receiver with respect to TEL entries.

As with other ACH entries, Originators of TEL entries must obtain the consumer's explicit authorization prior to initiating a debit entry to a consumer's account. Unlike other debit entries to a consumer's account, however, Originators need not provide the consumer with a written authorization for the consumer to sign or similarly authenticate. Instead, the Originator may obtain the consumer's authorization for a TEL entry orally via the telephone. Originators of TEL entries are obligated either to tape record the consumer's oral authorization or to provide, in advance of the Settlement Date of the entry, written notice to the consumer that confirms the oral authorization. The following specific information must be included in the authorization:

- * the date on or after which the consumer's account will be debited;
- * the amount of the debit entry to the consumer's account;
- * the consumer's name;
- * a telephone number that is available to the consumer and answered during normal business hours for customer inquiries;
- * the date of the consumer's oral authorization; and
- * a statement by the Originator that the authorization obtained from the Receiver will be used to originate an ACH debit entry to the consumer's account.

For an oral authorization obtained over the telephone to be valid, the Originator must (1) state clearly during the telephone conversation that the consumer is authorizing an ACH debit entry to his account, and (2) express the terms of the authorization in a clear manner. The Originator

must retain either the original or a duplicate tape recording of the consumer's oral authorization or a copy of the written notice confirming the consumer's oral authorization for two years from the date of the authorization. At the request of the ODFI, the Originator must provide a copy of the consumer's authorization.

An Originator that chooses the option to provide the consumer with written notice confirming the consumer's oral authorization must disclose to the consumer during the telephone call the method by which such notice will be provided. The written notice must include, at a minimum, the six pieces of information required to be disclosed during the telephone call, as described above. Originators should understand that the term "provide" is intended to mean that the Originator has utilized a medium (e.g., U.S. mail, fax, or other mail delivery method) to send the written notice to the consumer. (Note: Any written notice or disclosure required by the NACHA Operating Rules may be provided in electronic form, including e-mail. This includes the notice for TEL. Please note, however, that state and federal laws may require consumer consent before using electronic notices/disclosures.) The term "provide" does not imply receipt of such notice by the consumer. Originators must understand that, when written notice is used to confirm the authorization, the consumer must be afforded the right to contact the Originator, using the telephone number provided, to correct any erroneous information contained within the notice.

An Originator using a voice response unit (VRU) to capture a consumer's authorization for a TEL entry must understand that key-entry responses by the consumer to input data and to respond to questions does not qualify as an oral authorization. A VRU may be used by the consumer to key enter data and to respond to questions, provided that the actual authorization by the consumer is provided orally.

RISK MANAGEMENT

In an effort to minimize the risk related to Telephone - Initiated Entries, in which the identity of the consumer and the consumer's assent to the authorization cannot be assured by a written authorization, the NACHA Operating Rules require Originators to implement a number of specific risk management procedures relating to TEL entries: * Verification of Identity of Receiver.

Originators of TEL entries are required to utilize commercially reasonable procedures to verify the identity of the consumer. Originators will need to establish a commercially reasonable method (e.g., use of a directory, database, etc.) to verify the consumer's name, address, and telephone number. The Originator is also advised to further verify the Receiver's identity by verifying pertinent information with the Receiver (e.g., past buying history, mother's maiden name, Caller ID information, etc.).

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 business. 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. The determination of commercial reasonableness is based on the situation of each Originator with respect to a number of factors including the size, type, and frequency of entries typically transmitted by the Originator, the alternatives available to the Originator, and procedures in general use by similarly situated Originators. Whether an Originator has fulfilled its obligations to perform in a commercially reasonable

ARC

Obligations of Originators of ARC Entries

Accounts Receivable Entries - An Accounts Receivable (ARC) Entry is a Single Entry ACH debit used by Originators to convert a consumer check that is received via the U.S. mail or at a dropbox location for the payment of goods or services. For the ARC application, the consumer's check is viewed solely as source document, from which the consumer's routing number, account number, check serial number, and dollar amount for the transaction are captured for use in the ACH debit entry.

Capture of MICR Information During initial processing of an ARC entry, the Originator may not key-enter the routing number, account number, or check serial number from the Receiver's source document. An Originator may, however, key-enter such information to correct errors relating to MICR misreads, misencoding, or processing rejects.

ARC entries are subject to the requirements of the NACHA Operating Rules, the Electronic Fund Transfer Act, and the Federal Reserve Board's Regulation E. The ARC entry is a single entry debit to a consumer's account, initiated by an Originator for purchases or payments that are made by mailing a check (used as a source document) to the Originator via the U.S. mail or by placing the check in a dropbox. The Originator is required to use a reading device to capture the MICR line (routing number, account number, and check serial number) of the source document (check) but may key enter the amount of the transaction. This application requires the Originator to provide, prior to the receipt of each check, notice to the consumer that receipt of his check will be authorization for the check to be used as a source document for an ACH debit transaction to the Receiver's account at his financial institution. Used only as a source document, the check will not enter into the check collection process, nor will it constitute an access device as defined by Regulation E.

Eligible Items The Originator can accept a check as a source document to initiate an ARC entry only if it has been sent through the U.S. mail or delivered to a dropbox. To be used as a source document for this type of transaction, the check or sharedraft must: (1) contain a pre-printed serial number, (2) be drawn on a consumer account, and (3) be completed and signed by the consumer.

Checks that may not be used as source documents for ARC entries include:

- corporate checks
- third-party checks
- demand drafts and third-party drafts that do not contain the signature of the Receiver
- credit card checks
- obligations of a financial institution (e.g. cashier's checks, money orders, etc.)
- checks drawn on the Treasury of the United States, a Federal Reserve Bank, or a Federal Home Loan Bank
- checks drawn on a state or local government
- checks payable in a medium other than United States currency.

Authorization/Notification Requirements

Originators are required to provide notice to the Receiver, prior to the receipt of each source document that will be used as the basis for the origination of an ARC entry, that receipt of the Receiver's check will be deemed to be the Receiver's authorization for an ACH debit entry to the Receiver's account. the check will be used solely as a source document for capturing the Receiver's routing number, account number, check serial number, and dollar amount of the entry. The provision of the notice by the Originator to the consumer and the receipt of the source document together constitute authorization of the ARC entry.

Reinitiation of ARC Entries Originators must be aware that the NACHA Operating Rules restrict

the number of times that any entry, including ARC entries, returned for insufficient or uncollected funds may be reinitiated to no more than two times following the return of the original entry. An Originator must remedy the reason for the return of an ARC entry returned for any other reason before reinitiating the transaction. Originators must ensure that they have established policies and procedures to comply with these rules governing reinitiation of ARC entries.

Retention of Source Document Each Originator of ARC entries must retain an image, microfilm, or other copy of the front and back of the consumer's source document for a period of two years from the Settlement Date of the entry. The ODFI must send a copy of the front and back of the source document to the RDFI within 10 banking days of receipt of a written request by the RDFI within two years of the Settlement Date of the entry. The original source document to which the ARC entry relates must be destroyed by the Originator within fourteen days of the Settlement Date of the entry. This requirement is to protect against the risk that, by error, the source document might subsequently be entered into the check processing system for payment as a check.

Sample Notification and Statement Language

Notification Language Below is sample language that may be used by Originators to assist them in developing notifications for authorizations for ARC entries. The ARC application requires the Originator to provide notice to the consumer, prior to the receipt of his check, that receipt of his check will be authorization for the check to be used as a source document for an ACH debit transaction to the consumer's account at his financial institution. The provision of the notice by the Originator to the consumer and the receipt of the source document by the Originator together constitute authorization for the ARC entry.

Originators should be aware that, although the NACHA Operating Rules do not prescribe specific notification language, each notification must comply with the requirements of the NACHA Operating Rules, which require that the notice clearly and conspicuously state that the receipt of the source document will authorize an ACH debit to the Receiver's account in accordance with the terms of the source document.

SAMPLE NOTICE FOR ARC ENTRIES

By sending your check, please be aware that you are authorizing [ABC Company] to use information on your check to make a one-time electronic debit from your account at the financial institution indicated on your check. This electronic debit will be for the amount of your check; no additional amount will be added to the amount.⁵[If we cannot collect your electronic payment, we will issue a draft against your account.]⁶If you do not have sufficient funds in your account, a fee of \$ will be debited electronically from your account.⁶Please contact the Billing Department at [(555) 123-4567] to learn about other payment options if you prefer not to have your check used in this way.

⁵ If the originator is not able to collect the amount owed within the ACH Network, and chooses to collect the amount owed through another payment mechanism, they should consult with their legal counsel for any language requirements for any state or federal laws.

⁶To collect additional fees or service charges through the ACH Network, an Originator must follow the authorization requirements within the NACHA Operating Rules but must also include language in the notice to be compliant with Regulation E.

Statement Information The NACHA Operating Rules require the RDFI to send or make available to the consumer specific information relating to each ACH entry to the consumer's account. Below is a sample of how the ARC entry could appear on a consumer's periodic statement.

01/15/02	\$199.92	ABC Mortgage	MORTGAGE	1202
----------	----------	--------------	----------	------

The first field is the posting date, followed by the amount of the ARC entry, Company Name, Company Entry Description, and the Check Serial Number.

RCK

Legal Framework Re-presented Check Entries (RCK entries) are subject to applicable NACHA Operating Rules, the Uniform Commercial Code, and Federal Reserve Regulation CC. These entries are not, however, subject to the Electronic Funds Transfer Act or Regulation E. The legal framework for Re-presented Check Entries is premised on the fact that the origin of each re-presented check entry is a paper check that has been dishonored. Transfers of funds that were originated by a check, draft, or similar paper instrument are specifically excluded from coverage under the EFTA (15 U.S.C. 1693a(6)) and Regulation E (12 C.F.R. 205.3(c)(1)). Accordingly, if a Re-presented Check Entry is treated as a check transaction for purposes of the EFTA and Regulation E, it follows that the UCC and Regulation CC should continue to be the bodies of law that govern the rights and responsibilities of the parties involved with that payment, even though it has been converted to electronic form.

Eligible Items A Re-presented Check Entry is considered to be a presentment notice for purposes of Revised Article 4 of the Uniform Commercial Code (1990 Official Text). To that end, the receipt of a Re-presented Check Entry constitutes presentment of the item in accordance with Article 4-110, and the return of the Re-presented Check Entry constitutes notice of dishonor or non-payment of the item in accordance with Article 4-301. The provisions of the NACHA Operating Rules that are applicable to Re-presented Check Entries are in accordance with the Commentary provisions set forth in 12 C.F.R. Part 229.37 of Federal Reserve Regulation CC.

To be eligible to be transmitted as an RCK entry, an item must:

- * be an item within the meaning of Revised Article 4 of the Uniform Commercial Code (1990 Official Text);
- * be a negotiable demand draft drawn on or payable through or at a participating DFI, other than Federal Reserve Bank or Federal Home Loan Bank;
- * contain a pre-printed serial number;
- * be in an amount less than \$2,500;
- * indicate on the face of the document that it was returned for insufficient or uncollected funds;
- * be dated less than 180 days from the date the entry is transmitted to the RDFI;
- * be drawn on a consumer account; and
- * must have been previously presented (a) no more than twice in paper form, if the entry is an initial RCK entry; or (b) no more than once in paper form and no more than once as an RCK entry, if the entry is a reinitiated RCK entry.

Items that are ineligible for transmission as RCK entries include, but are not limited to:

- * non-cash items (as defined by Section 229.2(u) of Federal Reserve Regulation CC);
- * drafts drawn on the Treasury of the United States, a Federal Reserve Bank, or a Federal Home Loan Bank;
- * drafts drawn on a state or local government that are not payable through or at a Participating DFI;
- * United States Postal Service money orders;
- * items payable in a medium other than United States currency;
- * items that are third-party items (e.g., the payee endorses a check over to a third party who also endorses the check); and
- * demand drafts and third-party drafts that do not contain the signature of the Receiver (e.g.,

the drawer does not sign a check but authorizes another party to debit his account via a draft).

OBLIGATIONS OF ORIGINATORS

NOTICE REQUIREMENT An RCK entry is authorized by the consumer through the provision by the Originator of a notice to the check writer and the subsequent receipt of the consumer's check by the Originator. Originators of RCK entries must provide notice to the check writer, prior to receiving the item to which the RCK entry relates, informing the check writer that his returned check may be collected electronically if the check is returned for insufficient or uncollected funds. The manner in which the Originator provides notice to the check writer is not prescribed by the NACHA Operating Rules. However, the notice must clearly and conspicuously state the terms of the Re-presented Check Entry policy. It is recommended that notice provided at the point-of-sale be clearly displayed on a sign at the point-of-sale, and that notice provided by a billing firm (i.e., utility company or credit card company which issues a bill for payment) be clearly displayed on or with the monthly billing statement.

Originators should be aware that, to protect both the check writer and the RDFI, a check writer will be able to sign a written statement under penalty of perjury and be recredited for the amount of the entry if the required notification by the Originator is not provided. The RDFI, in turn, will be able to return the RCK entry by transmitting the return entry to its ACH Operator by its deposit deadline for the return 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 RCK entry.

RESTRICTIVE ENDORSEMENTS Any restrictive endorsement (e.g., "For Deposit Only") placed on the item by the Originator or its agent is void or ineffective when the item is presented as a re-presented check entry.

COLLECTION FEES Re-presented Check Entries may be originated only for the face amount of the check. No collection fees may be added to the amount of the item when it is transmitted as an ACH entry.

An Originator desiring to use the ACH Network to collect a service fee must originate a separate PPD, TEL, or WEB debit entry to the consumer's account and must follow all rules governing the specific transaction used, including having first obtained the consumer's authorization for such an entry in the manner specified by the NACHA Operating Rules.

Some Originators may desire to place an authorization stamp on the check being used for the payment of goods or services in order to collect a returned check fee in the event that the check is returned for insufficient or uncollected funds. In order for this practice to be compliant with the NACHA Operating Rules, the following requirements must be met:

- * An authorization placed on the check must be signed (not initialed). This signature must stand alone, i.e., the authorization language for the ACH debit entry must not be stamped in close proximity to the maker's signature on the check. The signature must clearly relate to the authorization language itself.
- * The authorization on the check must be identifiable as an ACH debit authorization and must clearly and conspicuously state its terms (i.e., the print cannot be so small or smeared that a consumer would be unable to easily read the authorization and understand its terms).
- * The authorization on the check must contain information that explains how the consumer may revoke the authorization.
- * The Originator must provide the consumer with an electronic or hard copy of the authorization.
- * The Originator must retain the original or a microfilm (or its equivalent) copy of the authorization for two years from the termination or revocation of the authorization.

Authorization language, if stamped on the back of the check, should be in the endorsement

space provided and not lower on the check. Before stamping the back of a check with anything other than an endorsement, Originators must ensure that they understand and are in compliance with both the NACHA Operating Rules and all regulations that govern the collection of checks.

NUMBER OF PRESENTMENTS Originators may transmit a re-presented check entry no more than twice after the first return of a paper item, and no more than once after the second return of a paper item.

RETENTION OF COPY OF ITEM The Originator must retain a copy of the front and back of the item (check) to which the RCK entry relates for seven (7) years from the settlement date of the RCK entry. When requested to do so by the ODFI, the Originator must provide a copy of the front and back of the check to the ODFI for its use or for the use of the RDFI requesting the information. If the check has been finally paid, this must be indicated on the copy.

RETURN OF RE-PRESENTED CHECK ENTRIES Originators should be aware that RCK entries may be returned for a variety of reasons. For the majority of RCK entry returns, the RDFI must transmit the return entry to its ACH Operator by midnight of the second banking day following the banking day of receipt of the RCK entry.

However, Originators should be aware that, for RCK entries for which (1) the Receiver had placed a stop payment order on the item to which the RCK entry relates, (2) the required notice stating the re-presented check entry policy was not provided by the Originator, (3) the check is ineligible, (4) all signatures on the check are not authentic or authorized, or the check has been altered, (5) the amount of the entry was not accurately obtained from the item, or (6) both the RCK entry and the item to which the RCK entry relates have been presented for payment, the RDFI will be able to transmit a return entry to its ACH Operator by its deposit deadline for the return 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 RCK entry. With the exception of returns due to stop payment on the original item, the Receiver is required to provide the RDFI with a written statement under penalty of perjury stating the reason for the return as described above. (Note: For additional information on written statements under penalty of perjury, refer to the RDFIs chapter in Section II of these Guidelines.)

APPENDIX C – Development Resources

Validate Bank ABA (Routing) Numbers

Language: Javascript

```
<script language="javascript">
<!--
function checkABA( aba ) {
    var i, n, t;

    // First, remove any non-numeric characters.
    t = "";
    for (i = 0; i < aba.length; i++) {
        c = parseInt(aba.charAt(i), 10);
        if (c >= 0 && c <= 9)
            t = t + c;
    }

    // Check the length, it should be nine digits.
    if (t.length != 9) {
        alert("Invalid Routing Number"); // Testing Purposes, You may remove
        return false;
    }

    // Now run through each digit and calculate the total.
    n = 0;
    for (i = 0; i < t.length; i += 3) {
        n += parseInt(t.charAt(i), 10) * 3
        + parseInt(t.charAt(i + 1), 10) * 7
        + parseInt(t.charAt(i + 2), 10);
    }

    // If the resulting sum is an even multiple of ten (but not zero),
    // the aba routing number is good.
    if (n != 0 && n % 10 == 0) {
        alert("Your Routing Number is Valid!"); // Testing Purposes, You may remove
        return true;
    } else {
        alert("Invalid Routing Number!"); // Testing Purposes, You may remove
        return false;
    }
}
-->
</script>
```

Example:

```
<form>
<input type="text" name="bank_aba">
<input type="button" onclick="javascript:checkABA(this.form.bank_aba.value)" value="validate">
</form>
```

Language: PHP

```

<?php
// CHECK FOR VALID ABA NUMBER
function aba_validate($aba)
{
    // First, check for 9 digits and non-numeric characters.
    if (ereg("[0-9]{9}$", $aba))
    {
        $n = 0;
        for ($i = 0; $i < 9; $i += 3)
        {
            $n += (substr($aba,$i,1) * 3)
                + (substr($aba,$i + 1,1) * 7)
                + (substr($aba,$i + 2,1));
        }

        // If the resulting sum is an even multiple of ten (but not zero),
        // the aba routing number is good.

        if ($n != 0 && $n % 10 == 0)
        {
            return(true); // found good aba
        }
        else
        {
            return(false);
        }
    }
    else
    {
        return(false);
    }
}
?>

```

General Credit Card Validation

There are three common edits that catch the greatest majority of bad card

- MOD 10 check digit
- Credit card prefix check
- Credit card length validation

MOD 10 Check Digit

The MOD 10 check digit calculation validates the credit card by calculating the last digit of the card number from all the other numbers in the card.

The last digit of a credit card can be calculated based on a calculation performed upon all the digits preceding it. This operation is called a **MOD 10 check digit**

Example Coding for MOD 10**Language: C**

```
/* The operator for mod in 'C' is % */
```

```
long mod10 (card,card_len-1) /* module 10 check digit function */
char *card; /* credit card number */
short card_len /* card length */
{
register int count; /* a counter */
register int weight; /* weight to apply to digit being checked*/
register int sum; /* sum of weights */
register int digit; /* digit being checked*/
long mod;
weight=2;
sum =0;
/* compute the sum */
for (count = card_len - 1; count >=0; count = count -1)
{
digit = weight * (card[count] - '0');
/* add both the tens digit and the ones digit to the sum */
sum = sum + (digit / 10) + (digit % 10);
if (weight ==2)
weight = 1;
else
weight = 2;
}
/* subtract the ones digit of the sum from 10 and return the ones digit of that
result */
mod = (10 - sum%10) % 10;
return (mod)
}
```

Card Prefix Check

The prefix check is the comparison of the first few digits of each card number to a list of known prefixes.

American Express / Optima	37, 34
Carte Blanche	389
Diners Club	30, 36, 381 - 388
Discover (Novus)	60110, 60112, 60113,60114, 60119
JCB	3528 – 3589
MasterCard	51 – 55
Visa	4

Card Length Check

The number of digits for each card is constant, allowing a validation to be performed by verifying the number of digits for each card number.

American Express / Optima	15
Carte Blanche	14
Diners Club	14
Discover (Novus)	16
JCB	16
MasterCard	16
Visa	13 or16