WEB Entry Originators
Security Certification
Requirements

Dear WEB Entries Originator,

Please review the Audit Requirements, complete the audit, then fax or email the certificate and website screen shots to our Compliance Department. Fax: 888.313.7842

Provide a screen shot of your web page that shows the user identity authentication method used. This screen should show where the consumer enters either a login and password, account number, PIN, or social security number to authenticate their identity to protect against unauthorized access.

The NACHA Operating Rules of 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. 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 Receiver's financial information is protected by security practices and procedures that ensure that the financial information that 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 more frequently due to the rapid change of technology and security risks, especially where WEB entry origination is involved.

WEB Entry Audit Components

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 nonetheless recommended by NACHA as sound business practices.)

1. Physical Security (to protect against theft, tampering and damage)

1) Critical network, server, and telecommunications equipment should be placed in physically secure locations that permit access only to authorized personnel.
2) Insure any banking information, including, but not limited to, an Entry, Entry Data, a routing number, an account number, and a PIN or other identification symbol transmitted via an Unsecured Electronic Network, have prior to the key entry and through transmission of any banking information 1) encrypted the banking information using a security technology that, at minimum, is equivalent to 128-bit RC4 encryption technology, or 2) transmitted or received the banking information via a secure session utilizing security technology that provides a level of security that, at a minimum, is equivalent to 128-bit RC4 encryption technology.
3) Firewalls must be fully deployed with secured processes for access.
4) Firewalls must protect websites from inappropriate and unauthorized access.
5) Disaster recovery plans must be developed and reviewed periodically.

2. Personnel and Access Controls (to protect against unauthorized access and use)

1) A formal set of security polices and procedures must be developed that clearly outline the corporate rules governing access to sensitive financial data.
2) 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.
3) Relevant employees must be educated on information security and company practices and their individual responsibilities.
4) Methods of authentication to verify the identity of each Receiver (i.e. passwords, PINs, etc.) have been put in place and are completed prior to access.
5) 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 that they are accompanied by an employee at all times.
    - Restrict access from external networks to authenticated users (i.e. by password or login codes).
    - Ensure that one person acting alone cannot circumvent safeguards (i.e. dual control procedures are in place).

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

1) All Receiver (customer) financial information should be kept behind firewalls and in an area inaccessible from the internet.
2) A data retention schedule should be developed that covers policies on how to handle the data from time of capture to destruction.
3) Retention schedules should be monitored to ensure that they are being met.
4) Receiver (customer) information should only be stored permanently if it is required by law, regulation, rule or a governing organization.
5) Data should not be stored longer than necessary.
6) Distribution of Receiver (customer) data should be limited, with procedures and controls in place governing organization.
7) The need for distributing Receiver (customer) data should be reviewed, and all distribution is verified and approved.
8) Receiver (customer) data sent across networks must be encrypted.
9) Use and regularly update anti-virus software.
10) Regularly test security systems and processes.

Attached you will find an Audit Certification Form. This certification states that you have completed an audit of compliance with the provisions of the ACH rules in accordance with the above listed key rule provisions of the *2014 NACHA Rules & Guidelines, Section Two, Subsection 2.5.17*.

If you should have any questions regarding the NACHA Audit Guideline for WEB entries, please contact us at 888.313.7842 or by email at compliance@securepaymentsystems.com.

Thank you,

Compliance & Risk Management Team
Secure Payment Systems