SECURE PAYMENT SYSTEMS Advantage ACH© EZCheck

Clear Form

WEB Entries ACH
Website Security Audit Certification

At SPS we value our customers and would like to thank you for your business. Please note the current NACHA Rules require each WEB entries Originator to conduct an internal or external audit of compliance with provisions of the ACH rules in accordance with the requirements of the 2020 National Automated Clearing House Association ("NACHA") Operating Rules & Guidelines, Section Five, Chapter 48. These audit provisions do not prescribe a specific methodology to be used for the completion of an audit, but identify key rule provisions that should be examined during the audit process. An audit must be conducted by the end of each year by a senior level manager, officer, or an external auditor. **The NACHA Rules require a yearly audit to be conducted.**

Documentation supporting the completion of an audit must be (1) retained for a period of six years from the date of the audit, and (2) provided to the National Association upon Request.

Company Legal Name: DBA Name:

Tax ID Number: Website Address:

Date Audit Completed:
mm/dd/yyyy

Audit firm, examining body or individual conducting the audit:

Name: Contact:

Phone:

Address:

City: State: Zip:

I hereby confirm this company has conducted its Rule Compliance Audit Requirements in accordance with Section Five, Chapter 48, of the 2020 NACHA Rules & Guidelines.

Signed:

Name and Title: Date:
mm/dd/yyyy

Website content copies to be submitted with certification:

□ 1. Customer Service Contact information, including phone number and hours of operation.

□ 2. Screenshots of websites payment process, this should include all screens the customer would see while processing a live payment. Including log in, payment processing, terms and conditions and confirmation page.

□ 3. An example authorization of a web payment, this should include any data your system stores regarding a particular payment in a easily readable form.

Please return both pages of audit and website content to the SPS Compliance Dept. at compliance@securepaymentsystems.com via our secure email link https://securepaymentsystems.secureemailportal.com/ or via Fax to 858.549.1323. If you should have any questions regarding the NACHA Audit Operations Guideline for WEB entries, please call us at 800.313.7842 (extension 327 or 329) or by email at compliance@securepaymentsystems.com.

Save & Print

Annual WEB Audit Checklist

Completion Deadline: ***December 31, 2020*** **Company Name:**

Physical Security:	**Yes**	**No**	**Notes**
1.) Critical Network Server & Telecommunication equipment in secured location with access only to authorized personnel?	○	○	
2.) Firewalls in place to protect website(s) from inappropriate & unauthorized access?	○	○	
3.) Are process and procedures in place for securely administering those firewalls?	○	○	
4.) Disaster recovery plans in place and reviewed periodically?	○	○	

Personnel and Access Controls:	**Yes**	**No**	**Notes**
1.) Security policies and procedures in place clearly outlining the company's policies and the corporate rules governing access to sensitive financial data?	○	○	
2.) New employee hiring procedures include verifying application information and reference checks for those with access to Receiver financial information?	○	○	
3.) Relevant employees educated on, and understand, information security and the company's practices as well as their individual responsibilities?	○	○	
4.) Limited access to secured areas to authorized personnel only?	○	○	
5.) Terminated employees' access has been denied/suspended?	○	○	
6.) Visitors have no access to secure areas and information, and are accompanied by an employee at all times?	○	○	
7.) All access authenticated to any database with sensitive information? (i.e. passwords, token devices, biometrics…)	○	○	
8.) Key-management procedures in place requiring dual control and separation of duties?	○	○	
9.) Procedures and audit trails in place to scrutinize activities of users who have access to the customer's information?	○	○	

Network Security:	**Yes**	**No**	**Notes**
1.) Are firewall configurations installed and maintained, protecting all Receiver financial information, including but not limited to company network, databases and portable electronic devices?	○	○	
2.) Is anti-virus software used and regularly updated?	○	○	
3.) Are all system components updated with the latest vendor-supplied security patch installations and defaults changed?	○	○	
4.) Are data retention schedules in place and do they state the company's policy of how employees are to handle the data from the time it is captured until it is destroyed? (Receiver financial information only stored permanently if required by law or regulation.)	○	○	
5.) Are retention schedules monitored regularly to ensure that they are met? (at a minimum quarterly)	○	○	
6.) Controlled distribution of Receiver financial and personal information and policies & procedures implemented to direct the distribution of sensitive financial information?	○	○	
7.) Data distribution policies & procedures reviewed periodically?	○	○	
8.) Encryption of Receiver data and financial information at all points in the transaction course from transmission to storage? (128-bit RC4 encryption technology or equivalent.)	○	○	
9.) Are security systems and processes tested frequently? (i.e. exposure scans, external and internal penetration testing, intrusion detection, file integrity monitoring.)	○	○	

Save & Print