

ACH SELF-AUDIT CHECKLIST FOR ORIGINATORS

1. What types of ACH related information does your company store? **Mark all that apply.**

- Authorization forms
- Checks used as part of authorizations (including voided checks)
- E-mails or other electronic correspondence with entry information
- Electronic NACHA formatted files sent to your FI for processing
- Paper files or entries sent to FI for processing
- Other reports containing entry information from accounting software or other programs

2. Where is information related to ACH entries stored? **Mark all that apply.**

- | | |
|---|---|
| <input type="checkbox"/> Home office of employees | <input type="checkbox"/> File cabinets |
| <input type="checkbox"/> Removable media sources
(i.e. Flash drives, CDs, Backup tapes/drives) | <input type="checkbox"/> Desk drawers |
| <input type="checkbox"/> Company website | <input type="checkbox"/> Binders |
| <input type="checkbox"/> Outsourced technology service provider location/server | <input type="checkbox"/> Work PC/laptop |
| | <input type="checkbox"/> Mobile device |

3. Who at your company has access to ACH related information? **Mark all that apply.**

- | | |
|--|---|
| <input type="checkbox"/> All employees, including any temporary workers | <input type="checkbox"/> Managers/principals of the company |
| <input type="checkbox"/> Only those with ACH related job duties | |
| <input type="checkbox"/> Outside parties (cleaning companies, contractors, etc.) | |

4. Which of the following controls do you have in place for the **physical** security of data? **Mark all that apply.**

- | | |
|--|--|
| <input type="checkbox"/> Locked storage space (file cabinet, drawer) | <input type="checkbox"/> Key inventory to ensure limited staff access to sensitive information |
| <input type="checkbox"/> Locked storage for backup drives or other removable media | <input type="checkbox"/> Clean desk policy |
| | <input type="checkbox"/> Office security systems or alarms |

5. Which of the following controls do you have in place for the **digital** security of data? **Mark all that apply.**

- Unique User IDs for each employee
- Password controls:
 - i. "Strong" password requirements (length, character requirements, etc.)
 - ii. Secure storage of passwords, including ensuring they are not posted at workstation
 - iii. Required changes of passwords after ____ days (insert number)
 - iv. Lockout of user account after ____ invalid attempts (insert number)
 - v. Timeout or automatic locking of workstation after ____ minutes (insert number)
- Restricted access to files on network by job duties
- Designated PC for any internet banking or funds transfer services, such as ACH
- Updated anti-virus and anti-malware programs
- Automatic software patches or upgrades, including operating system updates
- Restrictions on types of internet sites that can be used or usage of company e-mail
- Firewall for office network
- Secure e-mail for communications with customers/employees when sensitive information is being transmitted
- Encrypted or secured customer websites if used for accepting payment requests
- Encryption for laptops or other mobile devices
- "Self-destruct" or "remote clean" ability for lost or stolen mobile devices
- Controls for remote connections to and from the company (e.g. Virtual Private Network [VPN] connection)

6. Are your company's employees provided training on information security? Yes No

If yes, are the following topics included? **Mark all that apply.**

- Password security
- Social engineering (e.g. phishing via e-mail or phone)
- Acceptable use policies for internet and e-mail
- Security of mobile devices/laptops when traveling

7. Do you work with outside service providers to help you with your technology and data security efforts? Yes No

If yes, are the following topics considered before starting a new relationship with a service provider? **Mark all that apply.**

- Research of potential new companies (financial history, references, internet search)
- Contract review regarding data security practices and confidentiality
- How a service provider would notify you of a possible breach and action plan
- Other steps taken to review potential service providers:

8. Do you have access to the ACH rules? Yes No

9. Are your current authorizations readily accessible so if warranted, a copy can be provided within the 10 day timeframe required by the NACHA rules? Yes No N/A

If no, please explain: _____

10. Do you retain all terminated authorizations for two years? Yes No N/A

11. How do you destroy physical information?

How do you destroy digital media sources that contain ACH information? (e.g. hard drives from computers and/or copiers, flash drives, copiers, CDs, backup tapes, etc.)

12. Do you have a plan of how to respond if there is a data breach at your company (physical or digital)? Yes No

If yes, have you included steps to contact the following parties as needed?

- Financial institution
- Law enforcement
- Service providers to help clean or repair affected devices
- Legal counsel
- Your customers/employees affected

Completed By: _____
(Printed Name) (Title) (Company Name)

Signature: _____ Date: _____