MERCHANTS bank of commerce

Cash Management Documentation

ACH and Wire Security Framework
Information and Workbook

Electronic Banking Department
530.722.3940
ebd@mboc.com

Do not include account information when emailing for support

Revised July 2019

Table of Contents

This checklist does not need to be returned to the bank. We are providing it to you for your information as a jumpstart to kicking off your security program for ACH and Wire transactions. We hope you find the information useful.

Security Requirements

Chapter 4 of the NACHA Operating Guidelines addresses ACH Data Security Requirements. Each Originator must establish and implement security policies, procedures and systems related to the initiation, processing and storage of entries.

"Security policies, procedures, and systems related to the initiation, processing, and storage of entries must be designed to:

1) protect the confidentiality and integrity of Protected Information;
2) protect against anticipated threats or hazards to the security or integrity of Protected Information; and
3) protect against unauthorized use of Protected Information that could result in substantial harm to a natural person."

The Rules define Protected Information as the non-public personal information, including financial information, of a natural person used to create, or contained within, an entry and any related addenda record. The definition of Protected Information not only covers financial information, but also includes sensitive non-financial information (such as non-financial account information contained in addenda records for bill payments) that may be incorporated into the entry or any related addenda record. By covering natural persons, the rule on the protection of sensitive data includes consumer information, but not corporate information, which is consistent with existing industry regulations and guidance. However, impacted ACH participants may apply the rule more broadly so that it covers all customers. The security policies, procedures, and systems of ACH participants must include controls on system access that comply with applicable regulatory guidelines. Impacted systems include all of those used by the ACH participant to initiate, process, and store entries. It is expected that security policies are reviewed and approved at a level of responsibility within an organization that is commensurate with the importance of the subject matter; however, the rules on ACH security do not include specific requirements regarding the level of approval of such policies and procedures, thus providing institutions flexibility to accommodate their respective corporate governance structures.

Review Your Business

1) What types of ACH data is collected, stored, transmitted and destroyed? Take inventory of the types of ACH that are part of your business. Are your processes to collect, store, transmit and destroy data in compliance with NACHA rules?

2) Has your company implemented security policies and procedures? ☐ Yes ☐ No
3) Do the security policies and procedures cover ACH activities such as payroll, taxes, payments, donations, etc.? ☐ Yes ☐ No

Handling ACH Protected Information

1) Is protected information collected properly secured?
    a. Paper documents such as authorization forms, applications, origination agreements, onboarding documentation

    b. Electronic formats such as via email, USB drives, cloud storage locations, mobile authorizations? Are emails encrypted? Are PDF documents password protected?

Device Protection

1) Are all devices kept current on Operating System patches? ☐ Yes ☐ No
2) Is antivirus, antimalware/spyware programs installed, kept current and ran regularly on all devices? ☐ Yes ☐ No
3) Does your system administrator allow remote access to devices? ☐ Yes ☐ No
4) Does your network share drives? If so, is access granted on an "as needed" basis? ☐ Yes ☐ No

Destroying Protected Information

1) Are all paper documents shredded after the retention period has expired? ☐ Yes ☐ No
2) Are all electronic devices erased and wiped after the retention period has expired? ☐ Yes ☐ No

Educate Staff

Your first line of defense from the cybersecurity threats is your staff. It is imperative that business owners, management and employees stay current on the latest threats. Keeping security at the

forefront of everyone's mind while staying vigilant will provide a strong defense against threats trying to steal your information.

1) Do you have an education plan in place to train new employees, as well as one to keep current staff updated on keeping your business safe? ☐ Yes ☐ No
2) Are all employees aware of the threats that are disguised to look like legitimate links in emails? ☐ Yes ☐ No
3) Do your employees know that they should not open attachments in email without first confirming with the sender via phone or other means? ☐ Yes ☐ No
4) Are employees changing password frequently for secure websites and not reusing passwords for multiple sites? ☐ Yes ☐ No

Other Resources

- Please ask us for a copy of our Business Online Banking Security Best Practices, if you did not see it in your ACH and/or Wire Annual Review letter.

- You can register for free access to the NACHA Rules at www.nacharulesonline.org.

- Federal Trade Commission
  - Protection Personal Information: A Guide for Business https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business
  - Cybersecurity for Small Business https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

- Better Business Bureau
  - Cybersecurity for Small and Medium Sized Businesses https://www.bbb.org/council/for-businesses/cybersecurity/
  - The 5-Step Approach https://www.bbb.org/council/for-businesses/cybersecurity/the-5-step-approach/
  - Scams and Your Small Business: A Guide for Business https://www.ftc.gov/tips-advice/business-center/guidance/scams-your-small-business-guide-business