ACH Security Framework Notice & Self-Assessment

This ACH Security Framework Notice (this "Notice") has been sent to you as the designated owner or authorized representative of your company under your company's ACH Origination Agreement with BAC Community Bank (the "Bank").

Effective September 20, 2013, the NACHA Operating Rules (the "Rules") implemented the "ACH Security Framework." The ACH Security Framework requires that originators in the ACH network establish a data security framework to protect certain non-public information that they hold. As an originator using the Bank's ACH network, you are required to follow the Rules, including the requirements of the ACH Security Framework.

The ACH Security Framework requires all originators to establish and maintain security policies, procedures, and systems related to the initiation, processing, and storage of entries that are 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. "Protected Information" means non-public personal information, including financial information, of a natural person used to create, or contained within an entry and any related addenda records.

Compliance with the Rules is your responsibility under your ACH agreement with the Bank. Attached please find a self-assessment questionnaire designed to help you assess compliance with this amendment. These questions are intended to assist you in determining what your security practices are so that you may identify areas that may need to be updated or improved in order to comply with the ACH Security Framework requirements.

If you have any questions pertaining to this form or your obligations under the ACH Security Framework, please contact our Customer Service Department by calling 877-226-5820 or by emailing: customer.service@bankbac.com

ACH DATA SECURITY SELF-ASSESSMENT FOR ORIGINATORS

1. **What types of ACH related information does your company store?**
   (Mark all that apply)
   NACHA Rules require that all non-public information is protected. NACHA Rules and other regulations contain different retention periods for various documents. For example, authorization forms containing account information need to be stored safely for two (2) years after the last transaction is initiated. Your storage of documents should be in conformance with NACHA Rules and all applicable regulations.
   - ☐ Authorization forms
   - ☐ Checks used as part of authorizations (including voided checks)
   - ☐ Emails 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)
   Limiting access to non-public information, such as account information for your employees, vendors, and customers helps protect data.
   - ☐ Home office of employees
   - ☐ Removable media sources (i.e. Flash drives, CDs, Backup tapes/drives)
   - ☐ Company website
   - ☐ Outsourced technology service provider location/server
   - ☐ File cabinets
   - ☐ Desk drawers
   - ☐ Binders
   - ☐ Work PC/Laptop
   - ☐ Mobile device

3. **Who at your company has access to ACH related information?**
   (Mark all that apply)
   Restricting information on a need-to-know basis is another measure to protect non-public information.
   - ☐ All employees, including any temporary workers
   - ☐ Only those with ACH related job duties
   - ☐ Managers/principals of the company
   - ☐ 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)
Securing documents, such as authorization forms, is another measure to protect private information.

- ☐ Locked storage space (file cabinet, drawer)
- ☐ Locked storage for backup drives or other removable media
- ☐ Key inventory to ensure limited staff access to sensitive information
- ☐ Clean desk policy
- ☐ 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)
Limiting access to applications, such as ACH Origination or other applications for check writing and reconciliation, and establishing user id and password policies helps define roles and builds protection of sensitive information.

- ☐ Unique User IDs for each employee
- ☐ Password controls:
  - ☐ "Strong" password requirements (length, character requirements, etc.)
  - ☐ Secure storage of passwords, including ensuring they are not posted at workstation
  - ☐ Required changes of passwords after _____ days (insert number)
  - ☐ Lockout of user account after _____ invalid attempts (insert number)
  - ☐ 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 email
- ☐ Firewall for office network
- ☐ Secure email 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?**
   Helping employees understand why it is necessary to develop practices that protect sensitive information held by the business also helps them.
   - ☐ Yes
   - ☐ No

   If yes, are the following topics included?
   (Mark all that apply)
   - ☐ Password security
   - ☐ Social engineering (e.g. phishing via email or phone)
   - ☐ Acceptable use policies for internet and email
   - ☐ 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?**
   Overseeing the work of outside service providers, especially those with access to systems containing sensitive company information, is another measure in protecting non-public information.
   - ☐ 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. **How do you keep track of when documents can or should be destroyed?**
   Developing a system to secure sensitive information and routinely destroy it when the retention period expires is another way to protect non-public, private information.

_____

_____

_____

9. **How do you destroy physical information?**

_____

_____

_____

10. 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.)

_____

_____

_____

11. Do you have a plan of how to respond if there is a data breach at your company (physical or digital)?

Building an action plan provides clear direction if a data breach occurs, or if you suspect a data breach. A plan made in advance will help you respond quickly and contact all those affected.

☐ **Yes**

☐ **No**

If yes, have you included steps to contact the following parties as needed?
(Mark all that apply)

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