First Interstate Bank

ACH Security Framework Guidance & Sample Checklist

Effective September 20, 2013, the NACHA Operating Rules “ACH Security Framework” amendment requires Participants in the ACH Network to establish a data security framework which meets the following minimum data security obligations:

- Require non-consumer Originators, Participating DFIs, Third-Party Service Providers, and Third-Party Senders to establish, implement, and, as appropriate, update security policies, procedures, and systems related to the initiation, processing, and storage of Entries and resulting Protected Information;

- Require each Participating DFI, Third-Party Service Provider, and Third-Party Sender to verify, as part of its annual ACH Rules Compliance Audit, that it has established, implemented, and updated the data security policies, procedures, and systems required by the Rules; and

- Require an ODFI to use a commercially reasonable method to establish the identity of each non-consumer Originator or Third-Party Sender with which the ODFI enters into an Origination Agreement.

Attached please find a self-assessment questionnaire designed to help your business comply with this amendment. The questions are intended to assist you in determining what your security practices are. Please take the time to answer the questions to help determine if your security practices meet the obligations of the ACH Security Framework Guidance.

Please contact your local Treasury Solutions Representative if you have any questions pertaining to this form or topic.

ACH DATA SECURITY CHECKLIST FOR ORIGINATORS/THIRD-PARTY SENDERS

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)

   □ Emails or other electronic correspondence with entry information

   □ Electronic NACHA formatted files sent to your FI for processing

   □ Paper files or entries sent to your 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)***

   □ 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)***

   □ 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)***

   □ 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)***

□ 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 e-mail

□ 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?**

□ 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. How do you keep track of when documents can or should be destroyed?

____

____

____

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.)**

____

____

____

9. 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

□ Legal counsel

□ Law enforcement

□ Your customers/employees affected

□ Service providers to help clean or repair affected devices

Completed By: ____
(Printed Name) (Title)

Signature: ________________________ Date: __________________