# ACH Security Framework Self-Assessment Worksheet

## Policies and Procedures

Identify the policies and procedures that have been developed or amended to comply with the Security Framework requirements

<table>
<thead>
<tr>
<th>Policy</th>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT/IS Policy</strong></td>
<td>Does the company have an IT/IS team or department?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>Is there a data security policy in place by this team/department?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td><strong>Privacy Policy</strong></td>
<td>Does the company have a privacy policy regarding protected information as described in the security framework rule?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td><strong>Clean Desk Policy</strong></td>
<td>Does the company have a clean desk policy? Example: Removing all business and client sensitive information from desktop and securely storing.</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td><strong>Online Banking Policy</strong></td>
<td>Does the company have an online banking policy? Example: Only accessing business account information, including ACH services, on a computer that is specified for business use only.</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td><strong>Data Breach Policy</strong></td>
<td>Does the company have a Data Breach Policy?</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Describe the policy in place to prevent information from being accessed by an unauthorized user:

Describe the policy in place should secure information be compromised or information accessed by an unauthorized user:

## Handling ACH Protected Information

Identify how Protected Information is collected – Paper Documents

<table>
<thead>
<tr>
<th>Information</th>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACH Authorization forms</strong></td>
<td>Are ACH Authorization forms collected and retained as necessary for all debit or credit transactions?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td><strong>ACH Return and Correction</strong></td>
<td>Are ACH Return and Correction notifications printed from the secure email sent by Chemical Bank?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td><strong>Data Reports</strong></td>
<td>Are additional Data Reports in paper format retained?</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Describe how the confidentiality and integrity of Protected Information is stored until destruction:
### Identify how Protected Information is collected – electronic formats: password protected, encrypted or masked

- Does the company accept ACH internet initiated authorizations?  □ Yes □ No
- Does the company accept ACH telephone authorizations?  □ Yes □ No
- Does the company accept ACH mobile authorizations?  □ Yes □ No

If applicable, describe how the confidentiality and integrity of Protected Information is encrypted, masked, or protected when collected by the ways described above:

### Destroying ACH Protected Information

#### Identify how Protected Information is destroyed and disposed of in a secure manner

- Does the company have a policy in place for destruction of paper documents?  □ Yes □ No

Describe the policy in place for disposal or destruction of paper documents, including the time frame in which they are stored before destruction:

- Does the company have a policy in place for destruction of electronically formatted information?  □ Yes □ No

Describe the policy in place for disposal or destruction of electronically formatted ACH information, including the time frame in which they are retained before destruction. *Example: data erased, disks destroyed:*

### Moving ACH Protected Information

#### Identify how Protected Information is moved, secured, and transmitted

- Does the company have a secure, specified computer ONLY used for business purposes?  □ Desktop □ Laptop □ Yes □ No
- Does the company access the secure site “Business eBanking” by mobile device?  □ Yes □ No
- Does the company access the secure site “Business eBanking” by remote access.  □ Yes □ No
## ACH Security Framework Self-Assessment Worksheet

### Identify how devices are secured
- Are automatic or scheduled updates for each device completed on a regular basis? Including Anti-Virus, Anti-Malware, Anti-spyware, and/or encryption software.  
  - Yes ☐  No ☐

### Identify everyone who has approved access to Protected Information
- Are all authorized users provided with their own user name, password, and token (if applicable)?
  - Yes ☐  No ☐

- Does any authorized user share their log-in information with another, unauthorized employee?
  - Yes ☐  No ☐

### Securing ACH Protected Information
#### Identify effective password conventions
Describe the policy in place for effective password conventions. Example: never using default passwords, strong passwords, or phrases unique to each user including specific length and character type, not sharing passwords, frequency changed, password activated screensavers.

- Are passwords stored in a secure location?  
  - Yes ☐  No ☐

- Are tokens stored in a separate secure location from passwords (if applicable?)  
  - Yes ☐  No ☐

### Identify how potential intruders are blocked from accessing Protected Information
- Does the company restrict use of computers for business purposes only?  
  - Yes ☐  No ☐

- Does the company restrict use of wireless networks when accessing or transmitting Protected Information?  
  - Yes ☐  No ☐

- Does the company limit or disable unnecessary workstation ports/services/devices?  
  - Yes ☐  No ☐

- Does the company install updates as soon as they are published?  
  - Yes ☐  No ☐

- Does the company log off computer or device when not in use?  
  - Yes ☐  No ☐

### Identify how access is restricted
- Does the company limit the number of locations where Protected Information is stored?  
  - Yes ☐  No ☐

- Are paper records in a locked location?  
  - Yes ☐  No ☐

- Does the company limit employee access to Protected Information, including imaged reports, storage, server rooms, etc.?  
  - Yes ☐  No ☐
## ACH Security Framework Self-Assessment Worksheet

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the company encrypt or mask electronic Protected Information?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the company prohibit storage of Protected Information on a portable or USB device?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the company established an Internet Acceptable Usage Policy?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Describe the Internet Acceptable Usage Policy in place:

Identify how staff is trained for data protection security

Describe the policy and procedure in place to educate staff including the security policy, potential security breaches, clean desk policy and phishing scams via emails and phone calls.

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can documented proof be provided of employee training?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Completed by:

_______________________________________   _____________________________________
Authorized Signer                    Title

_________________________________ ________________________________
Date                                Business Name
The ACH Security Framework amendment creates a framework within the ACH Operating Rules aimed at protecting the security and integrity of certain ACH data throughout its lifecycle. The Security Framework establishes minimum data security obligations for companies and Third Party Providers to protect ACH data within their purview.

The changes to the NACHA Operating Rules related to the ACH Security Framework provisions are noted below. Please contact us, or refer to your copy of the NACHA operating Rules CD if you would like a copy of any of the modified rules.

- **Article One, Subsection 1.2.2 (Audits of Rules Compliance)** – modified to correct language related to Third-Party Senders for consistency throughout the Rules.
- **Article One, Subsection 1.6 (Security Requirements)** – new subsection incorporates general ACH Security Requirements into the NACHA Operating Rules.
- **Article Two, Subsection 2.2.1 (ODFI Verification of Originator or Third-Party Sender Identity)** – new subsection creates an obligation for the ODFI to use a commercially reasonable method to establish the identity of each Originator or Third-Party Sender.
- **Article Two, Subsection 2.4.1.8 (ODFI has Verified the Identity of Originator or Third-Party Sender That Uses an Unsecured Electronic Network Dishonor of Return by ODFI)** – this subsection is removed from the Rules.
- **Article Eight, Section 8.67 (Protected Information)** – adds a definition for the new term “Protected Information.”
- **Appendix Eight, Part 8.2 (Audit Requirements for All Participating DFIs)** – adds a new item “p” that requires annual ACH Rules Compliance Audits to include a verification that the covered ACH participants (i.e., Participating DFIs, Third-Party Service Providers, and Third-Party Senders) have established, implemented and updated (as appropriate) the security policies, procedures, and systems as required by the Security Requirements provisions.
- **Appendix Eight, Part 8.4 (Audit Requirements for ODFIs)** – modifies item “i” for consistency with the new subsection 2.2.1.

**Resources:**
- Better Business Bureau
  - Data Security – Made Simple
- NACHA
  - Sound Business Practices
  - [https://www.nacha.org/risk/sound-business-practices](https://www.nacha.org/risk/sound-business-practices)
  - Understand & Reporting Phishing / Email Scams
  - [https://www.nacha.org/for-consumers](https://www.nacha.org/for-consumers)
- Federal Trade Commission
  - Protecting personal information
- Federal Communications Commission
  - Ten Cybersecurity Strategies for Small Business
ACH Security Framework Compliance Certificate

Company Name: _______________________________________

I, the undersigned and authorized signer for the Company, do hereby certify that we have received the ACH Security Framework rule and understand our obligations, and are complying with the rule requirements.

_________________________________________________________________

Company Authorized Signer

_________________________________________________________________

Name

_________________________________________________________________

Date