PIONEER[SM] | All Together Forward[SM]

ACH DATA SECURITY FRAMEWORK
CORPORATE RESOURCE GUIDE

This ACH Data Security Framework Resource is provided to assist Originators develop a program to comply with the ACH Data Security Framework Rule.

This resource contains the following documents:

- **Corporate ACH Data Security Framework Sample Self-Assessment Worksheet** - The Sample Self-Assessment provides examples of the types of policies, procedures, standards and controls that would identify compliance with the Rule. *The sample self-assessment is to illustrate potential responses only and should not be considered all inclusive.*
- **Corporate ACH Data Security Framework Self-Assessment Worksheet** - Use this document to identify all the means and methods by which the Protected Information is gathered, stored, transmitted, encrypted and destroyed.
- **Additional Corporate Resources-** Links to resources for the corporate users.

Rule Background

2013 NACHA OPERATING RULES Supplement #2-2012

The ACH Data 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 Originators, Third Party Providers and Third Party Senders to protect ACH data within their purview.

SECTION 1.6 *Security Requirements*

Establish, implement and update, as appropriate, policies, procedures and systems with respect to the initiation, processing and storage of ACH Entries that are designed to:

a) Protect the confidentiality and integrity of Protected Information until destruction;
b) Protect against anticipated threats or hazards to the security or integrity of Protected Information until its destruction; and
c) Protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

Policies, procedures and systems must include controls that comply with applicable regulatory guidelines on access to all systems used by such non-consumer Originators or Third-Party Service Providers/Senders to initiate, process and store ACH Entries.

Section 8.67 "Protected Information"

The non-public personal information, including financial information of a natural person used to create, or contained within, an ACH Entry and any related Addenda Record.

CORPORATE ACH DATA SECURITY FRAMEWORK
SAMPLE SELF-ASSESSMENT WORKSHEET

Policies and Procedures	
Identify the policies and procedures that have been developed or amended to comply with the Security Framework requirements:	• Some examples are policies and procedures that address IS/IT security, privacy policies, clean desk policies, internet banking policies/procedures, vendor management policies, device management policies, etc.

Handling ACH Protected Information		
	Paper Documents	**Electronic formats – password protected, encrypted or masked**
Identify how Protected Information is collected:	• Authorization forms • Data reports • NOCs and returns paper reports	• Internet Initiated authorizations • Telephone / IRV /VRU authorizations • Mobile authorizations
Identify how and where Protected Information is stored:	• Locked cabinets or drawers	• Secure servers, desktops and laptops • USB drives, CDs • Secure online websites or cloud-computing

Moving ACH Protected Information	
Identify how Protected Information is moved, secured and transmitted:	To and from your financial institution and/or Third-Parties • Via secure online website • Via secure email • Via dedicated connection
Identify the devices used to access Protected Information:	• Desktops • Laptops • Remote Access • Mobile Devices • CD or USB drives
Identify how devices are secured:	• Up-to-date anti-virus • Anti-malware/spyware • Encryption software
Identify everyone who has approved access to Protected Information:	• Employees • Third-Parties

CORPORATE ACH DATA SECURITY FRAMEWORK
SAMPLE SELF-ASSESSMENT WORKSHEET

Destroying ACH Protected Information		
	Paper Documents	**Electronic – password protected, encrypted or masked**
Define how Protected Information is destroyed and disposed in a secure manner:	• Documented destruction	• Data erased • Disks destroyed

Securing ACH Protected Information	

Identify effective password conventions:	• Never use default password
	• Use strong password or password phrase that is unique to each user
	  ○ Specific length and character type
	  ○ Specify how password should be kept secure
	• Do not share password with co-workers
	• Change password frequently
	• Use password-activated screensavers
	• Safeguard passwords

Identify how potential intruders are blocked from accessing Protected Information:	• Restrict use of computer for business purposes only • Restrict use of wireless networks when accessing or transmitting protected information • Protect your IT system – anti-virus/spyware software, firewalls • Limit or disable unnecessary workstation ports/services/devices • Require automatic log-outs after a certain amount of inactivity • Change all vendor supplied passwords (administrator account in particular) • Encrypt all data during transmission and storage • Install updates as soon as they are published • Log off computer or device when not in use
Identify how access is restricted:	• Limit the number of locations where Protected Information is stored • Keep paper records in locked cabinet • Limit employee access to Protected Information, including imaged reports, cold storage, server rooms, etc. • Take precaution when mailing Protected Information • Encrypt or mask electronic Protected Information • Prohibit storing Protected Information on portable devices • Transmit Protected Information over the Internet in a secure session • Establish an Internet Acceptable Usage Policy
Document staff training:	• Keep Protected Information safe and secure at all times • Mask Protected Information in communications, such as phone calls, emails and snail mails • Make staff aware of security policy • Make staff aware of phishing scams, via emails or phone calls • Notify staff immediately of potential security breach • Establish a Clean Desk policy

CORPORATE ACH DATA SECURITY FRAMEWORK
SELF-ASSESSMENT WORKSHEET

INSTRUCTIONS:

Complete this ACH Data Security Framework Self-Assessment Worksheet to confirm your compliance with the ACH Security Framework requirements. Identify all the means and methods Protected Information is gathered, stored, transmitted, encrypted and destroyed for each category.

Once a comprehensive self-assessment has been conducted, retain the ACH Data Security Framework Self-Assessment Worksheet annually as evidence of compliance for ACH requirement. You may be required to provide a copy of the self-assessment worksheet to your financial institution, ACH auditor or upon request from other auditors.

2013 NACHA OPERATING RULES Supplement #2-2012
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 Originators to protect ACH data within their purview.

SECTION 1.6 *Security Requirements*
Establish, implement, and update, as appropriate, policies, procedures, and systems with respect to the initiation, processing and storage of Entries that are designed to:

a) Protect the confidentiality and integrity of Protected Information until destruction;
b) Protect against anticipated threats or hazards to the security or integrity of Protected Information until its destruction; and
c) Protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

Policies, procedures and systems must include controls that comply with applicable regulatory guidelines on access to all systems used by such non-consumer Originators, Participating DFIs, or Third-Party Service Providers/Senders to initiate, process and store Entries.

Section 8.67 "Protected Information"
The non-public personal information, including financial information, of a natural person used to create, or contained within, and Entry and any related Addenda Record.

CORPORATE ACH DATA 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	

Handling ACH Protected Information		
	Paper Documents	**Electronic formats – password protected, encrypted or masked**
Identify how Protected Information is collected:		
Identify how and where Protected Information is stored:		

Moving ACH Protected Information	
Identify how Protected Information is moved, secured and transmitted:	To ODFI (your financial institution): To Third-Parties (processor, CPA firm, etc.):
Identify the devices used to access Protected Information:	
Identify how devices are secured:	
Identify everyone who has approved access to Protected Information:	

Destroying ACH Protected Information		
	Paper Documents	**Electronic – password protected, encrypted or masked**
Define how Protected Information is destroyed in a secure manner:		

Securing ACH Protected Information	
Identify effective password conventions:	
Identify how potential intruders are blocked from accessing Protected Information:	
Identify how access is restricted:	
Document how staff is educated:	