RPA Risk & Compliance Committee
ACH Security Framework Workgroup
Checklists for ACH Security Framework

2013 NACHA OPERATING RULES & GUIDELINES
Supplement #2-2012, effective September 20, 2013

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 [*and Third-Party 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.

Security Checklist for Corporates:
Originators, Third-Party Service Providers and Third-Party Senders

1. Has a security information/privacy policy or procedures been established for your business?
    - Does it include ACH activities that are listed below?
2. What types of ACH data is collected, stored, transmitted and destroyed?
    - Examples:
        - Credit files – payroll, pensions, corporate-to-corporate payments, tax payments, vendor payments
        - Debits files – payments, cash concentration, purchases, donations
    - *Action Steps:* Take inventory of the types of ACH that is part of your business. How is that ACH data, or Protected Information, collected, stored, transmitted and destroyed?

RPA Risk & Compliance Committee
ACH Security Framework Workgroup
Checklists for ACH Security Framework

Handling ACH Protected Information		
	Paper Documents	**Electronic formats – password protected, encrypted or masked**
How is Protected Information collected?	• Authorization forms • Corporate Trade agreements • Applications • Origination Agreements • Set-Up/On-Boarding documents	• Internet Initiated authorizations • Telephone / IRV /VRU authorizations • Mobile authorizations
Where is Protected Information stored?	• Locked cabinets or drawers	• Secure servers, desktops and laptops • USB drives, CDs • Secure online websites or cloud-computing

Moving ACH Protected Information	
How is Protected Information moved, or transmitted, for initiation into the ACH network?	To ODFI: • Via Online Banking • Via Secure File Transmission – FTPS • Hand-delivery of CD or USB drive To Third-Parties for processing • Via secure online website • Via secure email Does the Corporate customer adhere to the Security Procedures for Transmission as established by the ODFI?
What devices are used to access Protected Information?	• Desktops • Laptops • Remote Access • Mobile Devices • CD or USB drives
Are devices secured?	• Up-to-date anti-virus • Anti-malware/spyware • Encryption software
Who has approved access to	• Employees

Protected Information?	• ODFI • Third-Parties

Destroying ACH Protected Information		
	Paper Documents	**Electronic – password protected, encrypted or masked**
Is Protected Information destroyed in a secure manner?	• Shredded	• Data erased • Wiped

Other Considerations	
Minimize or destroy information that is not needed	

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

Block Potential Intruders	• Restrict use of computer for business purposes only • Protect your IT system – anti-virus/spyware software, firewalls • Limit or disable unnecessary workstation ports/services/devices • Automatic log-outs after a certain amount of inactivity • Change all vendor supplied passwords (administrator account in particular) • Encrypt all data when moved and when stored • Install updates as soon as it is published • Log off computer or device when not in

	use
Restrict Access	• Limit the number of locations where Protected Information is stored • Keep paper records in locked cabinet • Limit employee access to Protected Information, including server rooms • Take precaution when mailing Protected Information • Encrypt or mask electronic Protected Information • Do not store Protected Information on portable devices • Transmit Protected Information over the Internet in a secure session • Establish an Internet Acceptable Usage Policy
Educate Staff	• 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

Additional Resources:

Corporates – Originators and Third Parties

- Better Business Bureau –
  - Data Security – Made Simple
    - http://www.bbb.org/data-security/
  - List of Additional Resources for Securing Sensitive Data
    - http://www.bbb.org/data-security/securing-sensitive-data/resources/
- NACHA
  - NACHA joins Better Business Bureau (BBB) in "Data Security- Made Simple" National Education
    - https://www.nacha.org/node/891
  - General Computer & Email Security Tips
    - https://www.nacha.org/c/newresources.cfm/AID/1052

  - Understand & Reporting Phishing / Email Scams
    - https://www.nacha.org/c/newresources.cfm/AID/1047
- Federal Trade Commission
  - Practical tips for business on creating and implementing a plan for safeguarding personal information
    - http://business.ftc.gov/documents/art01-protecting-personal-information-five-steps-business
- Federal Communications Commission
  - Ten Cybersecurity Strategies for Small Business
    - http://www.uschamber.com/sites/default/files/issues/defense/files/10_CYBER_Strategies_for_Small_Biz.pdf

RPA Risk & Compliance Committee
ACH Security Framework Workgroup
Checklists for ACH Security Framework

Security Checklist for DFI	
Risk Assessment and Layered Security Procedures for all ACH data	
Commercially Reasonable Authentication Methods	• Call-backs • Security Tokens • Confirmation authentication via text or email
Internal Policies and Procedures	• Security Policy • Privacy Policy • Clean Desk Policy • Online Banking Policy • ACH Management Policy • Vendor Management Policy
DFI up-to-date on technology, rule and regulatory changes	• BSA/AML • Gramm-Leach-Bliley Act • Know Your Customer Policy – Customer Due Diligence • FFIEC Guidance – Supplement to the Authentication in an Internet Banking Environment • *NACHA Operating Rules & Guidelines* • State Laws

Additional Resources for Depository Financial Institution:

- FFIEC Information Security Program
  - http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program.aspx
- FFIEC Practical Application
  - http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/data-security/practical-application.aspx
- Privacy Act Issues Under Gramm-Leach-Bliley for Consumers
  - http://www.fdic.gov/consumers/consumer/alerts/glba.html
- Privacy Policy
  - http://www.fdic.gov/regulations/examinations/financialprivacy/handbook/
- Better Business Bureau –
  - Data Security – Made Simple
    - http://www.bbb.org/data-security/
  - List of Additional Resources for Securing Sensitive Data
    - http://www.bbb.org/data-security/securing-sensitive-data/resources/

RPA Risk & Compliance Committee
ACH Security Framework Workgroup
Checklists for ACH Security Framework

- NACHA
  - NACHA joins Better Business Bureau (BBB) in "Data Security- Made Simple" National Education
    - https://www.nacha.org/node/891
  - General Computer & Email Security Tips
    - https://www.nacha.org/c/newresources.cfm/AID/1052
  - Understand & Reporting Phishing / Email Scams
    - https://www.nacha.org/c/newresources.cfm/AID/1047
- Federal Trade Commission
  - Practical tips for business on creating and implementing a plan for safeguarding personal information
    - http://business.ftc.gov/documents/art01-protecting-personal-information-five-steps-business
- Federal Communications Commission
  - Ten Cybersecurity Strategies for Small Business
    - http://www.uschamber.com/sites/default/files/issues/defense/files/10_CYBER_Strategies_for_Small_Biz.pdf