

ACH SECURITY FRAMEWORK CHECKLIST

2014 NACHA OPERATING RULES & GUIDELINES

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. What types of ACH data is collected, stored, transmitted and destroyed?

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?

2. Has a security information/privacy policy or procedures been established for your business?

Yes

No

3. Does the policy include ACH activities listed below?

Examples: **Credit files** – payroll, pensions, corporate-to-corporate payments, tax payments, vendor payments. **Debits files** – payments, cash concentration, purchases, donations

Yes

No

Handling ACH Protected Information

	PAPER DOCUMENTS	ELECTRONIC FORMATS – PASSWORD PROTECTED, ENCRYPTED OR MASKED
How is Protected Information collected?	<ul style="list-style-type: none"> • Authorization forms • Corporate Trade agreements • Applications • Origination Agreements • Set-Up/On-Boarding documents 	<ul style="list-style-type: none"> • Internet Initiated authorizations • Telephone / IRV / VRU authorizations • Mobile authorizations
Where is Protected Information stored?	<ul style="list-style-type: none"> • Locked cabinets or drawers 	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Via Online Banking • Via Secure File Transmission – FTPS • Hand-delivery of CD or USB drive To Third-Parties for processing <ul style="list-style-type: none"> • 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?	<ul style="list-style-type: none"> • Desktops • Laptops • Remote Access 	<ul style="list-style-type: none"> • Mobile Devices • CD or USB drives
Are devices secured?	<ul style="list-style-type: none"> • Up-to-date anti-virus • Anti-malware/spyware • Encryption software 	
Who has approved access to Protected Information?	<ul style="list-style-type: none"> • Employees • ODFI • Third-Parties 	

Destroying ACH Protected Information

	PAPER DOCUMENTS	ELECTRONIC FORMATS – PASSWORD PROTECTED, ENCRYPTED OR MASKED
Is Protected Information destroyed in a secure manner?	<ul style="list-style-type: none"> • Shredded 	<ul style="list-style-type: none"> • Data erased • Wiped

Other Considerations:

Minimize or destroy information that is not needed.		
Use effective passwords	<ul style="list-style-type: none"> • Never use default password • Use strong password or password phrase that is unique to each user <ul style="list-style-type: none"> ▪ 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 	
Block Potential Intruders	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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](#)
- NACHA
 - [NACHA joins Better Business Bureau \(BBB\) in “Data Security- Made Simple” National Education](#)
 - [General Computer & Email Security Tips](#)
 - [Understand & Reporting Phishing / Email Scams](#)
- Federal Trade Commission
 - [Practical tips for business on creating and implementing a plan for safeguarding personal information](#)
- Federal Communications Commission
 - [Ten Cybersecurity Strategies for Small Business](#)