ACH Security Framework Checklist

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.

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

The recommendations within are best practices to ensure the security and safeguarding of your system while also adhering to the NACHA guidelines for ACH origination. American National Bank strongly encourages all ACH Originators to adhere to these best practices. Failure to follow these best practices may open your company to additional risks in which you will be liable.

Security Checklist:

Originators

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?

3. Does the policy include ACH activities listed below?

Credit files – payroll, pensions, corporate-to-corporate payments, tax payments, vendor payments.
Debit files – payments, cash concentration, purchases, and donations.

Electronic Device Protection

1. Is antivirus, antimalware/spyware programs installed, kept current and ran regularly on all devices? ☐Yes ☐No
2. Are all devices kept current on Operating System Patches? ☐Yes ☐No
3. Does your system administrator allow remote access to devices? ☐Yes ☐No
4. Does your network share drives? If so, is access granted on an "as needed basis? ☐Yes ☐No

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 To Third-Parties for processing • Via secure online website • Via secure mail 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 Protected Information?	• 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?	• Shredded	• Data erased • Wiped

Other Considerations and Best Practices

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
	  • Specify length and character type
	  ○ Minimum of 8 characters, a mixture of both uppercase and lowercase, including numbers and letters and at least one special character is encouraged.
	  ○ Specify how password should be kept secure (Passwords should never be written down anywhere.
	• Do not share password with co-workers
	• Change password frequently (Most common frequencies are every 30, 60 or 90 days)
	• 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 • Key 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, email and mail • 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