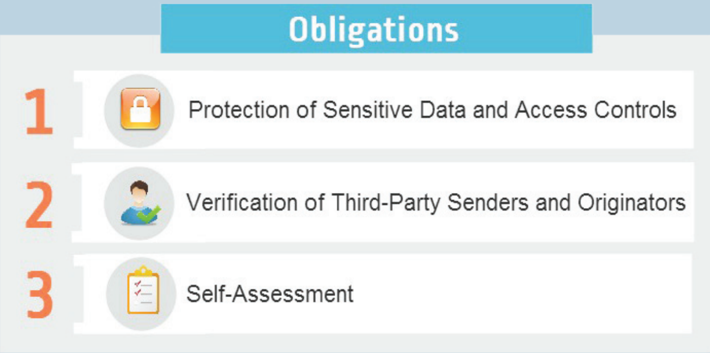
INFOSIGHT

Bringing the future of IT into focus

ACH Security Framework Compliance and Training Solution



Obligations

1 Protection of Sensitive Data and Access Controls

2 Verification of Third-Party Senders and Originators

3 Self-Assessment

In September 2013, NACHA amended the ACH Rules, creating a Security Framework designed to protect the security and integrity of ACH data. These rules became effective on March 21, 2014. The ACH Security Framework establishes minimum data security obligations for ACH Network participants to protect ACH data within their control.

To **ensure and simplify** compliance, InfoSight offers a comprehensive security and compliance solution that exceeds the key components of the new obligations.

Our solution provides the following tools:

1. Training Course for Originators and Third Party Senders

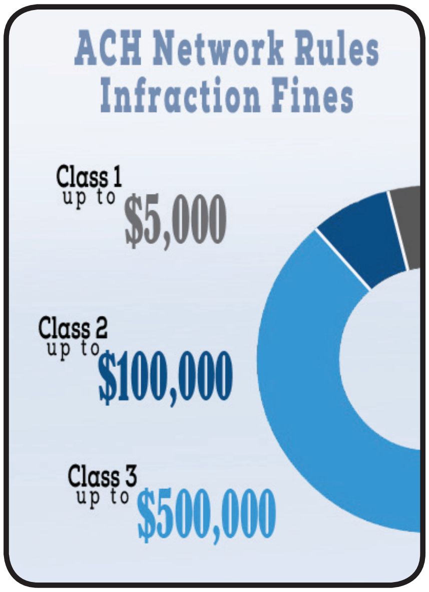
Provide Originators and Third Party Senders the knowledge they need to protect information assets achieve compliance with NACHA guidelines. Beginning with the basics about payments, students will learn about ACH operations and security, related risk factors, preventing fraud, handling of ACH information, and what is expected of them as far as rules and regulations and the required for their policies and procedures.

2. Training Course for ODFIs

This course provides ODFIs with an understanding of the ACH Security Framework Rule and its guidelines regarding internal policies, procedures and the day-to-day processing of ACH entries. Participants will learn about the rights and responsibilities of ODFI's, prerequisites to origination and general warranties and indemnifications. The 2012 FFIEC Authentication guidance for Internet Banking is also discussed.

3. ACH checklist for Originators

Provide Originators with the necessary tools to attain ACH Security Framework compliance. Upon completion of the checklist, originators will be able to determine whether or not their existing practices comply with the ACH Security Framework Rule. The checklist focuses on the key areas of storage, transfer and destruction of ACH Protected Information (PI).



4. Self-Assessment for ODFIs

Verify that the ODFI has established, implemented, and updated the data security policies, procedures, and systems required by the ACH Security Framework.". Additionally, verify the ODFI has conducted a risk assessment and has implemented a risk management program. Record retention, properly executed agreements, notices and encryption are covered.

5. ACH Activity Status Report for Board of Directors

Use this checklist to get organized and easily obtain Board approval for your ACH compliance obligations. The checklist includes activities regarding general rules, ACH Security Framework Rules and the DFI's relationship with Originators.

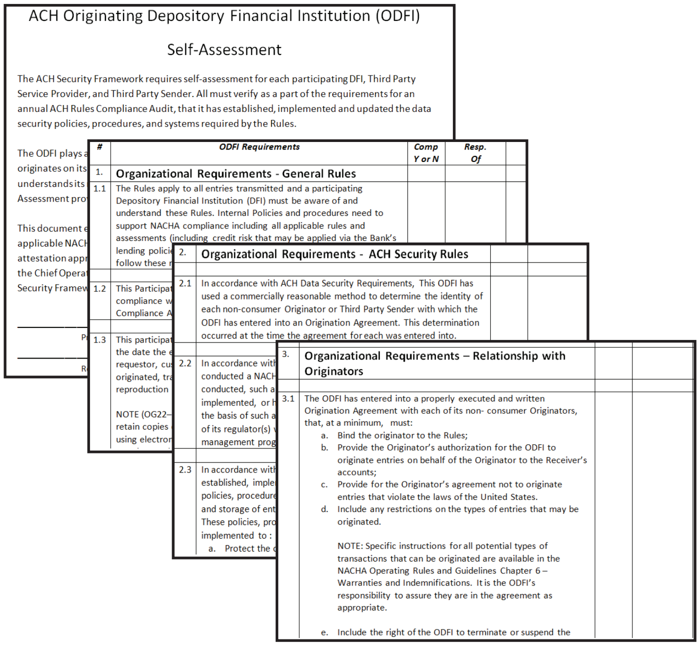
www.infosightinc.com 877-557-9703 (Outside FL) 305-828-1003 info@infosightinc.com

INFOSIGHT

Bringing the future of IT into focus

Don't face compliance issues alone. To learn how InfoSight can help you ensure continuous compliance with internal policy and regulatory mandates, call or visit us today.

Self-Assessment for ODFIs



ACH Originating Depository Financial Institution (ODFI)

Self-Assessment

The ACH Security Framework requires self-assessment for each participating DFI, Third Party Service Provider, and Third Party Sender. All must verify as a part of the requirements for an annual ACH Rules Compliance Audit, that it has established, implemented and updated the data security policies, procedures, and systems required by the Rules.

The ODFI plays a
originates on its
understands its
Assessment pro

This document e
applicable NACH
attestation appr
the Chief Operat
Security Framew

P

R

#	ODFI Requirements	Comp Y or N	Resp. Of	
1.	**Organizational Requirements - General Rules**			
1.1	The Rules apply to all entries transmitted and a participating Depository Financial Institution (DFI) must be aware of and understand these Rules. Internal Policies and procedures need to support NACHA compliance including all applicable rules and assessments (including credit risk that may be applied via the Bank's lending polici follow these r			
1.2	This Participat compliance w Compliance A			
1.3	This participat the date the e requestor, cu originated, tra reproduction NOTE (OG22– retain copies using electron			

2.	**Organizational Requirements - ACH Security Rules**		
2.1	In accordance with ACH Data Security Requirements, This ODFI has used a commercially reasonable method to determine the identity of each non-consumer Originator or Third Party Sender with which the ODFI has entered into an Origination Agreement. This determination occurred at the time the agreement for each was entered into.		
2.2	In accordance with conducted a NACH conducted, such a implemented, or h the basis of such a of its regulator(s) management prog		
2.3	In accordance with established, imple policies, procedure and storage of ent These policies, pro implemented to : a. Protect the		

3.	**Organizational Requirements – Relationship with Originators**		
3.1	The ODFI has entered into a properly executed and written Origination Agreement with each of its non- consumer Originators, that, at a minimum, must: a. Bind the originator to the Rules; b. Provide the Originator's authorization for the ODFI to originate entries on behalf of the Originator to the Receiver's accounts; c. Provide for the Originator's agreement not to originate entries that violate the laws of the United States. d. Include any restrictions on the types of entries that may be originated. NOTE: Specific instructions for all potential types of transactions that can be originated are available in the NACHA Operating Rules and Guidelines Chapter 6 – Warranties and Indemnifications. It is the ODFI's responsibility to assure they are in the agreement as appropriate. e. Include the right of the ODFI to terminate or suspend the		

Training Course for ODFIs

NACHA ACH SECURITY FRAMEWORK
TRAINING COURSE FOR ODFIS:

ACH ORIGINATION REQUIREMENTS

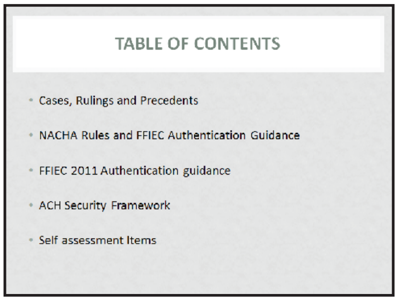
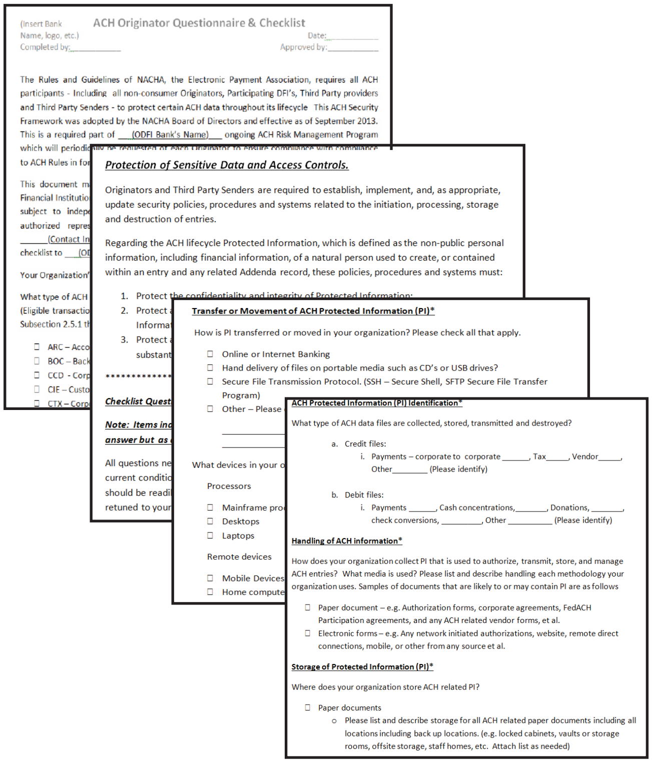


TABLE OF CONTENTS

- Cases, Rulings and Precedents
- NACHA Rules and FFIEC Authentication Guidance
- FFIEC 2011 Authentication guidance
- ACH Security Framework
- Self assessment Items

ACH Checklist for Originators



(Insert Bank Name, logo, etc.)

ACH Originator Questionnaire & Checklist

Completed by:____________

Date:____________

Approved by:____________

The Rules and Guidelines of NACHA, the Electronic Payment Association, requires all ACH participants - Including all non-consumer Originators, Participating DFI's, Third Party providers and Third Party Senders - to protect certain ACH data throughout its lifecycle This ACH Security Framework was adopted by the NACHA Board of Directors and effective as of September 2013. This is a required part of ___(ODFI Bank's Name)___ ongoing ACH Risk Management Program which will periodically be requested of each Originator to ensure compliance with compliance to ACH Rules in for

This document m
Financial Institutio
subject to indepe
authorized repres
______(Contact In
checklist to ___(OD

Your Organization'

What type of ACH
(Eligible transactio
Subsection 2.5.1 th

- ☐ ARC – Acco
- ☐ BOC – Back
- ☐ CCD - Corp
- ☐ CIE – Custo
- ☐ CTX – Corp

Protection of Sensitive Data and Access Controls.

Originators and Third Party Senders are required to establish, implement, and, as appropriate, update security policies, procedures and systems related to the initiation, processing, storage and destruction of entries.

Regarding the ACH lifecycle Protected Information, which is defined as the non-public personal information, including financial information, of a natural person used to create, or contained within an entry and any related Addenda record, these policies, procedures and systems must:

1. Protect the confidentiality and integrity of Protected Information;
2. Protect a
   Informat
3. Protect a
   substant

****

Checklist Quest

Note: Items inc
answer but as

All questions ne
current conditio
should be readi
retuned to your

Transfer or Movement of ACH Protected Information (PI)*

How is PI transferred or moved in your organization? Please check all that apply.

- ☐ Online or Internet Banking
- ☐ Hand delivery of files on portable media such as CD's or USB drives?
- ☐ Secure File Transmission Protocol. (SSH – Secure Shell, SFTP Secure File Transfer Program)
- ☐ Other – Please

____
____

What devices in your o

Processors

- ☐ Mainframe pro
- ☐ Desktops
- ☐ Laptops

Remote devices

- ☐ Mobile Devices
- ☐ Home compute

ACH Protected Information (PI) Identification*

What type of ACH data files are collected, stored, transmitted and destroyed?

a. Credit files:
   i. Payments – corporate to corporate ______, Tax_____, Vendor_____, Other________ (Please identify)

b. Debit files:
   i. Payments ______, Cash concentrations,_______, Donations, _______, check conversions, _________, Other __________ (Please identify)

Handling of ACH information*

How does your organization collect PI that is used to authorize, transmit, store, and manage ACH entries? What media is used? Please list and describe handling each methodology your organization uses. Samples of documents that are likely to or may contain PI are as follows

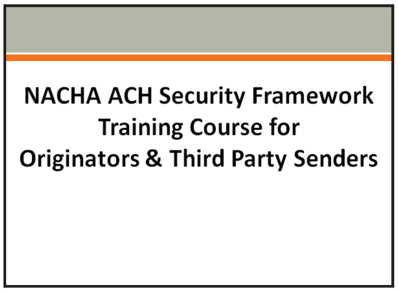
- ☐ Paper document – e.g. Authorization forms, corporate agreements, FedACH Participation agreements, and any ACH related vendor forms, et al.
- ☐ Electronic forms – e.g. Any network initiated authorizations, website, remote direct connections, mobile, or other from any source et al.

Storage of Protected Information (PI)*

Where does your organization store ACH related PI?

- ☐ Paper documents
  - ○ Please list and describe storage for all ACH related paper documents including all locations including back up locations. (e.g. locked cabinets, vaults or storage rooms, offsite storage, staff homes, etc. Attach list as needed)

Training Course for Originators and Third Party Senders



NACHA ACH Security Framework
Training Course for
Originators & Third Party Senders

Course Content

ACH – Automated Clearing House
- ○ Definitions and Authorities for Participants
  - Participants, Rules and Guidance
  - Protected Information (PI)
- ○ Required protections
  - Yours
  - Bank's
  - Compliance interaction with your Bank (DFI)
- ○ Your responsibilities
  - Policies , Procedures, Practices
    - Protected Information (PI) Practices
    - Collection of PI
    - Storage of PI
    - Transfer or Movement of PI
    - Who has approved access to PI
    - Destruction of PI
    - Responsibilities and Accountabilities
- ○ Checklist and Close

www.infosightinc.com 877-557-9703 (Outside FL) 305-828-1003 info@infosightinc.com

INFOSIGHT
Bringing the future of IT into focus

Contact us for more information on how InfoSight can help your organization improve your information security and compliance posture. InfoSight serves hundreds of organizations around the country with innovative managed services and technology solutions to keep organizations secure, resilient, and compliant. Contact us today.