

## ACH GUIDE

Materials needed: ACH policies (Audit and general), the last two ACH audits, the ACH contract with the Federal Reserve Bank or Third-Party Service Provider, audit verification and financial information on any Third-Party Service Provider, security settings (Operator Reports) for the processing method the FI has chosen, Originator contracts and any reviews of Originator financial information and exposure limits, and any ACH contingency/disaster recovery plans.

### ACH PARTICIPATION

<p>ACH items can be received/processed in several different ways, including directly from the Federal Reserve Bank (an ACH Operator) or via Third-Party Service Providers such as Autosolution for the Web from Bankers' Bank or Shazam, Inc. If the bank is an ODFI and RDFI it is possible two different Third-Party Service Providers may be used.</p>	1.	<p>How does the financial institution conduct ACH transactions?</p>
<p>All banks must be an RDFI. Being an ODFI is a choice of the FI and places additional requirements and responsibilities on the bank.</p>	2.	<p>Is the financial institution a Receiving Depository Financial Institution (RDFI) only or does it participate as an Originating Depository Financial Institution (ODFI) as well?</p>

### POLICIES

<p>An ACH audit policy appears to be required per NACHA rules. A sample audit policy is included in the audit workprogram and it appears to cover all necessary items. Banks can just input the necessary information in this policy and meet the requirement. If the FI formulates its own audit policy, it would need to address the listed areas. <b>If a third party conducts the audit, it would be sufficient for the bank to simply have a section in the ACH policy that notes who will do the audit and that it will be done using NACHA guidelines, who will review it, when it will be completed, and how deficiencies will be corrected.</b></p>	1.	<p>If the financial institution conducts its own ACH audit, has it adopted an ACH audit policy that address the following:</p>
<p>Required.</p>	a.	<p>Implementation and frequency, noting that the audit shall be conducted by December 1 of each calendar year?</p>
<p>Required.</p>	b.	<p>Scope?</p>
<p>Optional/Suggested.</p>	c.	<p>Sources for completing the ACH audit?</p>
<p>Required.</p>	d.	<p>Description of audit functions?</p>

Optional.	e.	A review of potential changes to ACH Rules and any other pertinent reference to ensure continued compliance and identify new requirements that may demand additional training and communication?
Required. Should note if verification of compliance will be performed through (1) interviews with key personnel, (2) reviews of the timing and content of required disclosures and, where applicable (3) tests of specific transaction activities to identify possible compliance exceptions.	f.	Procedures?
Required.	g.	Management review method?
Optional.	h.	Compliance with requirements of internal ACH policies?
Per correspondence with Shazam, Inc., all banks should have written ACH policies/procedures in addition to the required ACH audit policy. Shazam, Inc. does not provide suggested ACH guidelines to banks since banks deploy a variety of ACH processes and procedures unique to their mode of operations. However, in discussions with personnel at Shazam, they indicated the following minimum policy recommendations were appropriate.	2.	In addition to the audit policy (if necessary), has the financial institution adopted a general ACH policy that addresses the following:
	a.	A description of the particular ACH activities undertaken by the FI and any processing methods?
	b.	The security and controls that are in place to assure the integrity of the ACH activities?
	c.	Record retention?
Areas addressed could include physical and logical access controls in the data entry area, data center, and items processing operations as well as separation of duties and dual control procedures.	d.	Internal controls?
	e.	If the audit is conducted by a third party, a notation of such as well as review procedures?

**EXAMINATIONS AND AUDITS**

<p>Minimum audit requirements can be found in a separate bankexam tab. All audits are done on the honor system. Shazam, Inc. (and probably other entities) provide annual Audit Workbooks that can be purchased for about \$40. Given the time constraints for completion of the ACH workprogram, as well as the lack of formal training to answer the very detailed audit questions, examiners will not complete the audit if it has not been done by the financial institution. Deficiencies should be noted and future compliance strongly encouraged. Documentation supporting the completion of an audit must be provided to the National Association upon request. Financial institutions warrant to the rest of the payments system, via their ACH participation, that they have completed the required audit.</p>	1.	<p>Has the financial institution completed an ACH audit, in accordance with NACHA guidelines and the adopted audit policy, by December 1 of the calendar year?</p>
	2.	<p>Has the financial institution retained documentation supporting completion of the audit for a period of six years?</p>
	3.	<p>Has the audit been conducted under the direction of the audit committee, audit manager, senior level officer, or independent (external) examiner or auditor of the participating FI or third-party service provider?</p>
	4.	<p>Have all deficiencies noted at audits or regulatory examinations either been corrected or are there plans in place to address the noted problems?</p>
	5.	<p>Has the audit committee, board of directors, or an executive officer reviewed the audit findings?</p>
<p>Third-Party Service Providers, such as Shazam, Inc. and Bankers Bank, are also required to meet the annual audit requirement. The results of this audit, or at least of summary thereof, should be provided to the financial institution. Under the rules, FIs warrant that the Third-Party Service Provider has also completed the required audit.</p>	6.	<p>Has the financial institution received and reviewed the audit conducted by any Third-Party Service Providers?</p>

**TRAINING AND PERSONNEL**

<p>Bank personnel should attend some type of training, preferably annually, to keep updated on rule changes and other compliance issues. Many times, ACH training is provided via the web. Note that some larger financial institutions may have an AAP on staff. An individual with the AAP designation has undergone special training and received certification in regards to ACH.</p>	<p>1.</p>	<p>Do operations personnel receive the training necessary to properly conduct and perform ACH duties?</p>
	<p>2.</p>	<p>Are the necessary personnel provided with adequate materials to be kept up to date on ACH rules?</p>

**COMPUTER SECURITY SETTINGS**

<p>Shazam, Inc. does not offer specific recommendations concerning security for the ACH system, stating that each FI has full discretion to determine the levels and degree of risk it wants to assume. The following settings were noted as "best practices" based on collective input from various service providers.</p>	<p>1.</p>	<p>Has the bank established security settings via the computer system used to facilitate ACH transactions (with the ACH Operator or Third Party-Service Provider) that:</p>
<p>The person responsible for establishing operator privileges for ACH processing should be prohibited from creating or transmitting ACH entries.</p>	<p>a.</p>	<p>Segregates Security Administration duties from creation and/or transmission of ACH entries?</p>
<p>This would be for access to the ACH software on the bank's computer. FYI - passwords are also needed to connect with Shazam, Inc. These connection passwords are changed every ninety days (the new password is mailed out to a designated bank officer). This</p>	<p>b.</p>	<p>Requires a password change at least every 90 days?</p>
	<p>c.</p>	<p>Automatically logs off after 20 minutes of non-use?</p>
	<p>d.</p>	<p>Locks out the operator after 3 failed log-on attempts?</p>

**ACH ODFI RESPONSIBILITIES**

<p>Review the contracts authorizing the institution to initiate ACH items for customers and determine if they adequately set forth the responsibilities of the institution and customers. A SAMPLE AGREEMENT IS IN THE RULES MANUAL ON PAGE OG10.</p>	<p>1.</p>	<p>Does the bank have current, dated contracts for ALL Originators that address the following areas:</p>
	<p>a.</p>	<p>The established exposure limit?</p>
	<p>b.</p>	<p>Liabilities and warranties?</p>
<p>The Originator keeps the authorizations. If a customer complains about a transaction (they would probably do this to the FI) the Originator must back up why they said the money should be taken out of the customer's account.</p>	<p>c.</p>	<p>Responsibilities for processing arrangements and record retention requirements?</p>
	<p>d.</p>	<p>Other Originator obligations such as security and audit requirements?</p>
<p>ODFIs are liable and accountable for any violations of the NACHA Operating Rules (which include compliance with U.S. laws) by either the ODFI or the Originator, so it is important to have contracts in place. Adherence to OFAC enforced sanctions is also required. It appears to be important that OFAC be specifically noted as one of the laws that the bank most comply with, and banks should ensure their Originators know exactly what they are required to do to avoid an OFAC infraction. The following excerpt is taken from the June 2006 BSA manual:</p> <p>With respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying that the Originator is not a blocked party and making a good faith effort to determine that the Originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying that the Receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC policies. ODFIs are not responsible for unbatching transactions and ensuring that they do not process transactions in violation of OFAC's regulations if they receive those transactions already batched from their customers. If the ODFI unbatches the transactions it received from its customers, then the ODFI is responsible for screening as though it had done the initial batching.</p> <p>The BSA workprogram contains one specific question regarding ACH and OFAC compliance</p>	<p>2.</p>	<p>Do the agreements include an acknowledgement that the Originator will comply with laws of the United States, particularly noting OFAC compliance, as well as the state(s) where the Originator and bank are located?</p>

<p>Ask the ODFI how NACHA rules are communicated to Originators (i.e. delivery of annual Corporate Rules book, monthly guides, etc.).</p> <p>There is a Corporate Edition of NACHA operating rules that could be provided to businesses--and many ODFIs do this --although many Originators may not actually open the book throughout the year. The ODFI should educate, and simply Originators a book doesn't accomplish that.</p> <p>The ODFI could also type up a memo or FAQ document, updated annually, and highlight the most relevant ACH rules for that Originator. One Originator submitting payroll, for example, should understand the consumer funds availability rule. And another submitting monthly dues billing, for example, should understand the consumer's return rights up to 60 days and subsequently what their own rights are after an item is returned.</p>	3.	<p>Has the ODFI communicated NACHA operating rules and annual rules changes to its Originators?</p>
<p>This could include the submission of periodic financial information. For the origination of credit files, the FI warrants funds availability as the transactions are released to the payment system; reversals are rarely successful. Debit origination files include a 4 day return item risk; granting availability the next day exposes the FI to potential loss.</p>	4.	<p>Has the ODFI established procedures to monitor the creditworthiness of its Originator customers on an ongoing basis?</p>
<p>ODFIs are required by NACHA Operating Rules to establish limits on and monitor their exposure to risk when transmitting entries on behalf of their corporate customers. It is especially important to establish limits for web entries. Exposure limits should be set at a level slightly above what is considered to be "normal" activity. If the Originator should submit a file above the limit established, this should prompt bank personnel to ask additional questions of the Originator to ensure the file is not fraudulent. The risk to the ODFI is a credit risk upon initiating entries until the customer funds the account. For debit entries, the risk is if the bank grants funds availability to the Originator until the debit can no longer be returned by the RDFI. If the transaction is properly authorized, returns must be made no later than the second banking day following settlement. If not properly authorized, FI exposure can be up to 60 days from when it sends a periodic statement to the customer.</p>	5a.	<p>Has the ODFI established ACH exposure limits for Originators that are reviewed periodically and adjusted as needed?</p>
<p>If the exposure limit is exceeded, the transaction should be suspended to make sure there are no fraudulent items in the batch. If necessary, credit officer approval should be received prior to release.</p>	5b.	<p>Are entries initiated by the Originator monitored for compliance to the exposure limit?</p>

<p>The best way to receive an ACH file is probably by diskette delivered directly from the Originator to the FI. Bank should check the disk for viruses by opening the antivirus program and telling it to scan to appropriate drive with the disk in it. Per the 2006 ACH Rules, the ALL ACH transactions that involve the exchange or transmission of bank information via an electronic network MUST be either encrypted using a commercially reasonable security technology, for be transmitted via a secure session using a commercially reasonable security technology. IN THIS INSTANCE, COMMERCIALY REASONABLE SECURITY TECHNOLOGY MEANS AT A MINIMUM 128 BIT ENCRYPTION. Note that many of our ACH origination customers still receive a paper document (faxed or hand delivered) containing payroll or billing information from the company. While this might not represent a major security risk from those outside the ODFI, it does give the ODFI much more chance to make a human error resulting in greater liability to them. Examiners could encourage the ODFI to get an electronic file and avoid any data entry.</p>	6.	<p>How does the bank receive files from the Originator? If by e-mail is the data encrypted? If by disk, is it checked for viruses?</p>
<p>If sent via the Internet, files go to a particular spot on the server and certain people have access to the folder to retrieve the files. Security should be in place to secure the files so only the authorized people could access them, for instance using user names and passwords.</p>	7.	<p>If files are sent via the Internet, how does the bank receive them and where are they housed?</p>
<p>If an unscheduled file arrives, it should be cancelled if authorization is not subsequently obtained via a verified callback. Also, as a customer service, the customer should be contacted if a scheduled file does not arrive.</p>	8.	<p>Is a processing calendar (file schedule) maintained on Originators?</p>
<p>Whether or not to perform callbacks to Originators depends somewhat on the ACH procedures that the particular FI has enacted. If, for example, the FI only allows the Originator to deliver the ACH file on a diskette utilizing stringent physical controls procedures, a callback may not be necessary. In contrast, if the FI allows the ACH file to be sent via unencrypted email (a poor security practice), a callback might be very necessary to substantiate the actual sender, the integrity of the data, and other aspects.</p>	9.	<p>Have callbacks or some other form of verification (such as a signed fax) been established to validate the authenticity of an ACH file when received?</p>
	10.	<p>Does management ensure that change requests are in writing (or the equivalent confirmation for on-line activities), identify the originating personnel, document supervisory approval, and are verified by staff unable to make changes?</p>

**ACH ACCOUNTING, PROCESSING, AND GENERAL**

Assess the adequacy of separation of duties throughout the ACH process, including origination, data entry, adjustments, internal reconciliation, preparing general ledger entries, posting to customer accounts, investigations, and reconciliation with ACH operators.	1.	What are dual control and separation of duty procedures for ACH transactions (processing, clearance, and settlement) adequate?
	2.	Are customer deposit account balances for credit payments monitored to ensure payments are made against collected funds or established credit limits?
	3.	Based on the responses to the Technology Questionnaire, are adequate contingency provisions in place?

**THIRD-PARTY SERVICE PROVIDERS**

This section is ONLY to be completed if a Third party performs ACH procession for an Originator.

A Third-Party Service Provider is an organization other than the ACH Operator (Federal Reserve Bank) that performs a function of ACH processing on behalf of the Originator, ODFI, or RDFI. A function of ACH processing could be the act of creating an ACH file on behalf of an Originator or ODFI or acting as a sending point or receiving point on behalf of the ODFI or RDFI, respectively. The organization acting as the Third-Party Service Provider could be a data processing service bureau, correspondent bank, payable through bank, or simply a FI acting on behalf of another FI. The ODFI should request information about the processor's financial condition, operating environment, and security, confidentiality, and accuracy measures.	1.	Do all agreements with any Third-Party Service Providers:
A batch or file that exceeds the credit limit should be brought to the ODFI's attention before the file is deposited so the ODFI can either approve it as an exception or ask that it be held until the next day.	a.	Provide for established credit limits for batches and entire files?
	b.	Ensure senior management is aware of the practice of utilizing a Third-Party Service Provider?

The ODFI's approval of each company should be contingent on the creditworthiness of the company.	c.	Require that the Third-Party Service Provider not begin originating ACH entries for new companies under the ODFI's routing number without prior approval from the ODFI?
	d.	Require that the Third-Party Service Provider notify the ODFI of dollar totals for each file the processor deposits so that the ODFI can reconcile activity and settlement totals on reports from the ACH Operator?
	e.	Address who will be responsible for erroneous entries, who will handle rejects and in what time frame, who will handle returns and notification of change, how customer inquiries will be handled, and what type of audit trail will be provided?
	f.	Require completion of an annual ACH audit and that documentation attesting to such completion be provided to the FI annually?

---

WKSht - ACHGuide (Rev 12/31/06)