

This section is intended to determine the adequacy of controls over the ACH environment. The examiner must review compliance with established policy, the effectiveness of contingency/recovery planning and assess the soundness of physical and internal controls. The reviews of work flows and control points will ensure that adequate control procedures have been established to maintain the accuracy and integrity of the data. The procedures are created so that they may be implemented separately as part of either the IS or safety and soundness examinations. The examiner should document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

## **Tier I**

### **AUTOMATED CLEARING HOUSE (ACH)**

1. Determine the nature and characteristics of the system/network in use by:
  - a. Identifying the source of ACH activities.
  - b. Determining whether customers are performing their own input or the financial institution is using third party servicers or multiple ACH operators.
  - c. Identifying both the hardware and software being used in-house to support these ACH activities.
2. Review policies and procedures in place to monitor customer balances for credit payments (e.g., payrolls) to ensure that payments are made against collected funds or established credit limits, and that payments in excess of established credit limits are properly authorized.
3. Determine if deposits resulting from ACH transmitted debits on other accounts are treated as uncollected funds until the institution has reasonable assurance that the debits have been paid by the institution on which they were drawn. Also, if drawings against uncollected funds are monitored to ensure they are within established guidelines.
4. Review a sample of contracts authorizing the institution to perform ACH activities for customers to determine if they adequately set forth responsibilities of the institution and the customer, primarily as they relate to the following rules established by NACHA:

- a. Is the institution operating within established ACH operating rules and regulations?
  - b. Are agreements in effect for all ACH customers (incoming and outgoing) that set forth the responsibilities of the institution and customers and do the agreements include the rules of the ACH; funding arrangements (outgoing); Expedited Funds Availability Act (FRB Reg. CC); and UCC4A (credit transfer only)?
5. Have ACH activities been considered in the institution's overall insurance program?
  6. If third-party processors are employed to perform any major services related to ACH activities, are annual financial statements received and reviewed; and are reports covering audits of the processors periodically obtained and reviewed?
  7. Compare the last executed internal audit procedures covering ACH operations to the related questions detailed in Tier II of these procedures, and determine whether they meet or exceed Tier II coverage.
  8. Review a sufficient sample of supporting audit workpapers necessary to confirm that they support the execution of procedures established in step 7.
  9. Review all audit reports related to the ACH and determine the current status of any exceptions noted in the audit report.
  10. Procedures included in Tier II that are not sufficiently covered under steps 7 and 8, are to be implemented as part of this examination. (Note: To the extent coverage is clearly satisfactory and current, audit procedures and workpapers also may be used to address steps 1 to 4.)

## **CONCLUSIONS**

11. Review the results of work performed in this chapter and in the chapters for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers

should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

12. Discuss with management:
  - a. Violations of law, rulings, regulations, or significant internal control deficiencies.
  - b. Recommended corrective action for deficiencies cited.
  - c. Management's proposed actions for correcting deficiencies.
13. Assign rating. (see Chapter 5 for additional information.)
14. Prepare an index of workpapers for this section of the workprogram.
15. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.
16. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

**Examiner | Date**  
\_\_\_\_\_

**Reviewer's Initials**

## Tier II

### ACCOUNTING AND PROCESSING

1. Is a log maintained of the ACH payments received from and delivered to each customer?
  - a. Are all payments received, balanced to the aggregate of payments sent to an ACH operator?
  - b. Are all payments received from an ACH operator balanced to the aggregate of payments delivered to customers?
2. Are all general ledger accounts related to ACH reconciled on a timely basis?
3. Are reconcilements and exception items regularly reviewed by supervisory personnel?
4. Are daily activity and pending files with the ACH operator reconciled daily?
5. If applicable, is activity with third-party processors preparing ACH transaction files reconciled daily?
6. Are holdover transactions adequately controlled?
7. Are individual outgoing batches reconciled before being merged with other ACH transactions?
8. Are separate accounts used to control holdovers, adjustments, return items, rejects, etc. and are they periodically reconciled?
9. Is a separate investigation unit in place to control customer inquiries, return items, rejected/unposted items, differences, etc., and do they periodically generate reports of outstanding items and aging for management?
10. Does management adequately track exceptions to credit limit policies and legal contracts?
11. Are exception reports (e.g., rejects, return items, and aging of open items) receiving appropriate attention?
12. Is an adequate separation of duties maintained throughout the ACH process including origination, data entry, adjustments, internal reconcilement, preparation of general ledger entries, posting to

customers accounts, investigations, and reconciliation with ACH operators?

13. Are reference manuals available to data entry personnel? Do manuals address:
  - a. Credit relationships?
  - b. Internal control policies and procedures?
  - c. Operational procedures and controls?
  - d. Data security/customer security issues?
14. Are adjustments (e.g., added payments, stop payments, reroutes, and reversals) to original ACH instructions received in an area that does not have access to the data files?
15. Are assurances made that the individual making the request for an adjustment is authorized (e.g., signature verification and call backs on telephone instructions) and are records maintained (e.g., logs and taping of telephone calls) of individuals making the request?
16. Is it required that master customer profile originations and change requests:
  - a. Are in writing?
  - b. Identify the originating personnel?
  - c. Document supervisory approval?

**FUNDING AND CREDIT**

17. Before releasing payments to an ACH operator, are assurances obtained that sufficient collected funds (e.g., on deposit or prefunded) or credit facilities are available?
18. If prefunding arrangements are in place for customers without credit lines, are funds either blocked (held for disposition) or maintained in separate accounts until the transaction date?
19. If not prefunded, are blocks placed for outgoing payments on deposit accounts; applied as reductions to credit lines; or included in the overall funds transfer monitoring process?

20. Are payments resulting in extensions of credit lines or drawings against uncollected funds properly approved, and is documentation maintained to support the approvals?
21. If third-party processors are employed to process outgoing ACH transactions, are procedures in place to monitor ACH activity and ensure that funds are collected (collected balances, prefunding, credit lines) before the institution settles with the ACH operator?
22. Are ACH debits deposited treated as uncollected funds and are drawings against such funds adequately monitored for debits originated by high-risk customers?
23. Are drawings against uncollected ACH deposits properly approved, and is documentation maintained to support approvals for debits originated by high-risk customers?
24. Is there an internal control risk assessment (per FDICIA 112)?
25. Does management perform a risk assessment of the area in terms of the importance of the function to the overall corporate services function?

## **SECURITY**

26. Is a comprehensive data security system maintained that provides segregation of duties performed via computer terminals, such as data entry, adjustments, and release to the ACH operator?
27. Does the maintenance of the security systems include periodic changes of passwords, protection of password files, non-display of passwords on terminals, and automatic shut-down of terminals not in use?
28. Is data pending release to the ACH operator maintained in an environment that protects the data from unauthorized change?
29. Are telecommunications lines used to receive data from customers and to transmit data to ACH operators encrypted?
30. Are magnetic tapes and/or other data (computer or manual listings) submitted by customers protected from unauthorized access from the time they are

received by the institution until they are entered into the ACH system?

- 31. Is adequate physical security maintained over ACH operating areas?

**CONTINGENCY**

- 32. Has a written contingency plan been developed and tested for partial or complete failure of the system and/or communication lines between the institution, ACH processor, customers, and data center? Is the plan reasonably comprehensive in relation to the volume and importance of ACH activity to the institutions operation? Do the procedures provide for a reasonable recovery period?
- 33. For input reconstruction, are transactions files duplicated or otherwise retained for a minimum of 24 hours?
- 34. Determine if data and program files are adequately retained and backed up at off-premises facilities.
- 35. Determine if the center has established and tested procedures to recover and restore data.
- 36. Determine if the frequency and methods of testing contingency plans are adequate.
- 37. Proceed to procedure 11, Tier 1.

**Examiner | Date**

\_\_\_\_\_

**Reviewer's Initials**