Chapter 9

CASH ANALYSIS

TABLE OF CONTENTS

Chapter 9

CASH ANALYSIS

Examination Objectives

- Determine whether adequate accounting policies, practices, procedures, and internal controls exist for all phases of cash operations
- Determine whether the credit union has established guidelines addressing cash operations within which officials and employees operate
- Determine whether adequate security measures and surety bond coverage exist for cash operations including cash storage, replenishment, deposit activities, and transportation of cash and cash-like items

Associated Risks

Cash operations have various associated risks. Following are the primary risks associated with cash analysis:

- Liquidity risk - the credit union should have sufficient cash to meet member share and loan demand and pay operating expenses;
- Transaction risk - the board should adopt, and management should implement policies and procedures that ensure the accuracy and integrity of data and information regarding the credit union's cash accounts. In conjunction with the review of internal controls, examiners should consider (1) the proper recording of cash transactions, and (2) the volume of cash transactions when evaluating transaction risk;
- Compliance risk - examiners should ensure the credit union has an adequate program in place to properly report cash balances and cash transactions as required by current laws and regulations, including Regulation D, BSA and OFAC; and
- Reputation risk - when evaluating reputation risk, examiners should assess whether the credit union maintains the highest level of integrity and honesty over cash accounting and transactions.

Cash and Cash-Like Items

The following are cash and cash-like accounts established by the credit union's board of directors for specific purposes. The board authorizes the amount for each cash account (petty cash, teller change fund, vault change fund, ATM change fund and bank cash):

- Petty cash - used for making incidental payments and defraying other immaterial expense items;

- Teller change fund - used for processing member transactions; may vary in amount based on temporary, seasonal, and projected demands;

- Vault change fund - replenishes drains on teller change funds; may vary in amount based on temporary, seasonal, and projected demands;

- ATM change fund - provides cash for proprietary ATMs to process member ATM transactions; may vary in amount based on temporary, seasonal, and projected demands. Occasionally, credit unions assign ATMs "teller numbers" and include the funds in the teller change fund general ledger account. If so, each ATM on the system should have an identifying number to allow for an audit trail of cash differences by individual ATM;

- Bank cash - (1) includes cash in banks, savings banks, savings and loans, etc.; (2) usually replenishes vault, teller, and ATM change funds; (3) covers loan disbursements, expense disbursements, payroll, and share withdrawals; and (4) usually is a non-interest bearing account or one that earns only a nominal rate. Credit unions should maintain bank cash at reasonable levels or at minimum compensating balance requirements to limit fee assessments;

- Money orders, travelers checks, postage, theater/amusement park tickets - sold by credit unions as a service to the members; represent negotiable monetary instruments that can easily convert to cash; not normally recorded in the general ledger or reflected on the Statement of Financial Condition; and

- Other negotiable instruments - rarely encountered negotiable monetary instruments; warrant review when the examiner identifies them during the course of an examination.

Red Flags

Examiners should watch for the following "red flags", which can alert them to diversion or manipulation of cash by management or staff:

- Accounting/Reconciliations:
  - Ongoing recordkeeping problems;
  - Cash and bank reconciliations not completed, in arrears, or with fluctuating out of balance amounts;
  - Excessive teller overages or shortages, either in number or amount;
  - IOU's in teller or vault cash;
  - Numerous erasures, corrections, whiteouts, line-outs;
  - Numerous voided or third party checks;
  - Numerous stale dated outstanding checks;
  - Numerous stale dated reconciling items;
  - Lump sum postings not conducive to good audit trail;
  - Checks or transactions receipts missing or out of sequence;
  - Timeliness of deposits not in accordance with Bylaw requirements;
  - Bank account activity and/or bank account balances (or share draft clearings/total share draft balances) exceed realistic needs on any single day;
  - Excessive number of depository accounts providing potential for kiting; and
  - Excessive cash/assets ratio (indicates either poor cash management or possibly fraud.)

- Management:
  - Overly dominant manager;
  - Manager or key employee involvement in gambling;
  - Regular vacations not taken, always working late hours;
  - Nepotism;
  - Other forms of insider abuse or preferential treatment;
  - Limited personnel not conducive to segregation of duties;
  - Lack of adequate segregation of duties when the credit union has adequate staff;

- Failure to provide, or delays in providing, standard reports, records, and/or documents;
- Records maintained at home or in inappropriate location;
- Management or staff provide copies of documents rather than originals;
- Inactive supervisory committee;
- Lack of, unacceptable, or non-independent audit or verification;
- Inadequate internal controls and information systems (IS) controls;
- No internal review of override/non-financial reports;
- Bank account frequently overdrawn;
- High volume of excessive transactions;
- Use of borrowed funds in spite of large cash balances;
- Extravagant management or employee lifestyle relative to salary; and
- Lack of a fraud policy.

- Other:
  - Low return on assets or on various asset categories; and
  - Payment of above market dividends to attract deposits

Expanded Review Procedures

The depth of review necessary for each cash account will vary within a credit union and from one credit union to another. The most critical element for determining the degree of variance and the necessary depth of review is the examiner's professional judgment, experience and risk perception. Examiners can obtain assistance in assigning the level of risk by reviewing the appendix to the Risk-Focused Program chapter. The remainder of this chapter includes additional procedures that the examiner may implement when warranted.

Petty Cash Review

Although the petty cash fund authorization is generally immaterial, in cases where examiners note problems they may decide to review the fund to determine that:

- The balance of this fund does not exceed the authorized amount;
- Management has physically segregated it from other cash funds and provides accountability by limiting access;

- Valid receipts or signed cash vouchers evidence payments from the fund, and the sum of the fund, receipts, and vouchers total to the authorized amount;
- Management replenishes the fund in a timely manner and records the proper expense categories at least monthly;
- Management approves any changes in the fund's balance; and
- The supervisory committee or other independent party periodically verifies the fund.

Teller Change Fund Review

Depending on transaction volume and temporary, seasonal, and projected demands, teller change funds can represent a substantial portion of cash inventory. Examiners' scrutiny of teller fund operations may include a review of the following:

- Master Log maintained by the head teller or operations manager;
- At least two days of individual, signed, end-of-day, teller cash counts including related daily work transaction vouchers. If a teller is off work on the day of the verification, examiners must obtain the prior working day's end-of-day teller cash count and related transaction vouchers;
- At least two days of system-generated individual teller summary transaction activity reports that reflect the system's beginning and ending cash balances, check transactions, and cash transactions;
- Teller change fund general ledger detail; and
- Log of Bait Money, including denominations, and serial numbers assigned to each individual teller.

The entries on the Master Log should balance to the individual and aggregate, end-of-day, teller cash counts. The individual teller cash counts should balance to the ending cash balance on the system-generated teller summary reports. The total ending cash balances for all tellers should balance to the amount of the overall change fund appropriated to teller change funds in the general ledger.

Individual, end-of-day, teller cash counts should balance with the next day's beginning cash on the system-generated teller summary reports. Some data processing systems allow manual input of beginning cash balances. This weakness could disguise or postpone recognition of an out-of-balance condition or shortage. If the credit union cannot modify its computer system, management can mitigate concerns about this weakness by rotating teller drawers among tellers on a surprise basis.

Examiners and auditors routinely perform month-end examinations and audits; however, examiners do not perform cash counts. Management or supervisory committee personnel should periodically perform surprise cash counts.

Examiners should consider the following if they decide to review teller change funds:

- The amount set up in the teller change fund does not exceed the maximum established by the board of directors, the individual teller change funds do not exceed the amounts established by management, and the board has established reasonable total change funds;

- The credit union adheres to management's established maximum teller drawer limitations and maximum teller transaction limitations. Tellers sell their excess teller drawer cash to the vault change fund during days of high transaction activity;

- Supervisory committee, internal audit department, or other appropriate personnel perform periodic random audits of teller change funds;

- The credit union has procedures in place to immediately remove terminating tellers' access to cash operations and to audit, seal or close, vacationing tellers' drawers on their last work day;

- Management restricts tellers, both by policy and computer authority, from processing transactions on their own accounts, accounts of family members, or accounts of other relatives;

- Management restricts tellers' computer authority, in terms of access levels, and has controls in place to identify teller transactions by unique teller stamps, teller codes, or ID numbers;

- Management instructs employees to keep confidential their teller log-on IDs and passwords and periodically changes IDs and passwords;

- The computer has an activated time-out feature that requires tellers who are away from their stations for an extended period of time to sign-on again. If the credit union has not activated the time-out feature, tellers should sign-off when away from their stations for an extended period of time;

- Tellers lock their drawers when away from their stations and secure their funds in the vault overnight;

- Management restricts a teller's access to an individually assigned drawer and uses dual controls to prevent unauthorized access to teller drawers;

- The credit union clears any checks accepted in processing member transactions daily and prohibits tellers from holding cash items (checks, IOU's, drafts, etc.) as part of their change fund balance;

- Debit or credit memos signed by both parties evidence cash purchases from and cash sales to the vault change fund. Credit unions should prohibit cash purchases and sales between tellers;

- The credit union maintains a clear audit trail by promptly and accurately recording to the general ledger all cash activity, including teller differences. Supervisory personnel should regularly review the cash transactions records;

- The credit union provides transaction receipts to members for all transactions;

- The credit union does not have a "slush fund" built over time by overages that a staff member could use to conceal shortages;

- The credit union adequately segregates "bait money" to prevent teller usage;

- Management maintains dual control access to night depository funds and mail deposits, and requires the presence of both persons when removing, processing, and logging the contents;

- Teller change fund policies, practices, procedures, controls, and balancing procedures provide for adequate safeguards over teller operations and accountability; and

- Amounts in tellers' drawers do not exceed surety limits, if surety specifies limits.

If examiners encounter significant weaknesses as a result of the cash review, they may request a controlled random or total teller drawer count or perform a review of individual teller transaction reports.

Vault Change Fund Review

The vault change fund generally represents the largest portion of cash inventory and may fluctuate from time to time depending on anticipated transaction volume, temporary, seasonal, and projected demands. Because of the volume and fluctuation, the credit union should internally balance the vault change fund daily. If examiners review the vault change fund, they should consider that management has instituted the following:

- Master Log, listing end-of-day vault cash balances, maintained by head teller or operations manager;

- End-of-day vault change fund counts signed by head teller or operations manager;

- Vault change fund general ledger detail;

- Reasonableness of the amount maintained in the fund (including the teller change fund) for the needs of the credit union;

- Adherence to maximum vault change fund limitations established by the board of directors, which should correspond to limits established by the bylaws and any applicable surety limits;

- Periodic audits of the vault change fund by the supervisory committee, internal audit department, or appropriate personnel;

- Restricted access to the vault change fund for accountability, both by policy and vault combination or key distribution;

- Required dual control for opening and counting vault change fund replenishments, and signed bank debit memos evidencing the replenishments. Ideally, management should maintain a cash shipment log, and the timing of cash shipments should vary to reduce recognition of an identifiable pattern;

- Restriction of computer access levels for persons having access to the vault change fund. Examiners should review the employee transaction access limitation report to determine adequacy of the credit union's controls in this area;

- Maintenance of a clear audit trail by promptly and accurately recording to the general ledger all vault change fund activity, regardless of whether the fund is fixed or floating. Staff should record and promptly resolve any cash differences;

- Two-part debit or credit memos signed by both parties evidence cash purchases from and cash sales to the vault change fund. Examiners should trace a few transactions;

- Implementation of procedures to prevent an employee responsible for both vault cash and a teller cash drawer from commingling the funds; and

- Adequate safeguards and accountability over vault cash operations provided by vault change fund policies, practices, procedures, controls, and balancing procedures.

ATM Change Fund Review

The credit union must internally balance the ATM change fund daily, recognizing, however, that it cannot perform a true balancing until it replenishes the ATM and verifies the remaining cash, records deposits, and records withdrawals to machine output reports or audit tapes.

If examiners review the ATM change fund, they could ensure the ATM audit tape totals, adjusted for reconciling items, balance to the general ledger ATM change fund balance. Examiners can verify randomly selected individual reconciling items to source documentation, ATM detail tape, or general ledger detail.

During this review process, the examiner could also determine that:

- Management maintains dual control for opening, counting, replenishing, and balancing ATMs;
- Management maintains ATM deposits under dual control with both responsible employees present during opening, listing, and processing of machines and envelopes;
- Management prohibits personnel having custody of member access cards from having access to personal identification numbers;
- Management properly segregates duties involving the balancing of individual ATMs and balancing of system totals;
- Supervisory committee, internal audit department, or other appropriate personnel periodically audits the ATM change fund;
- Management assigns an employee having no duties nor authorizations in the teller or ATM areas of operation responsibility for captured ATM cards; and
- ATM change fund policies, practices, procedures, controls, and balancing procedures provide for adequate safeguards over ATM cash operations and accountability.

If the credit union owns several ATMs, these machines can hold a substantial amount of cash. Some credit unions (usually those maintaining large cash reserves) contract with outside parties, such as armored car services, to replenish and service their ATMs. The credit union should have agreements in place with bonded third parties. The supervisory committee, or other appropriate personnel, must periodically audit and verify these cash reserves, per specifications of surety.

Bank Account Review

Examiners may verify the most recent month-end bank reconcilement and review at least one other randomly selected month-end bank reconcilement. When credit unions use a corporate credit union for their primary banking purposes, examiners apply the same review procedures to the corporate account reconcilement. Examiners may verify and review at least the following:

- Bank reconcilements for (1) the most recent month-end, (2) the randomly selected month-end, (3) the reconciliation preceding the most recent month-end, and (4) the reconciliation preceding the randomly selected month-end. Examiners need these four bank reconcilements to verify outstanding items and adjustments for the two months' reviews selected;

- Original bank statements correspond with the reconcilements chosen for verification and review, and the current month's original bank statement, if available. If examiners do not have the current month's bank statement available and if they note unusual activity, they may decide to order a cut-off bank statement;

- Outstanding check registers and canceled checks correspond with the reconcilements chosen for verification and review. When the bank truncates the credit union's checks, examiners may substitute voucher copies for canceled checks. Examiners should trace a few checks to the general ledger and bank statement to ensure the checks agree with the amount on the reconcilement;

- Bank stamped original deposit receipts and original bank debit and credit memos correspond with the reconcilements chosen for verification and review;

- Original corporate account statements correspond with the reconcilements chosen for verification and review;

- List of authorized signers on the bank accounts (trace to board authorizations); and

- Bank accounts general ledger detail.

If examiners review bank account reconcilements and statements, they may include the following steps:

- Tracing the book balances to the general ledger and reconciliation of bank statement balances to the bank statements;

- Footing the credit union's bank reconcilements and corresponding outstanding check registers;

- Tracing all reconciling items to source documents, and to statement or general ledger details;

- Verifying that previous month's outstanding checks cleared on the month of review's bank statement for the amount shown on the previous month's outstanding check register;

- Reviewing aging of reconciling items, non-sufficient funds (NSF) items, and outstanding checks. Generally, credit unions should appropriately clear items older than 90 days unless staff is researching them or settling a dispute (i.e., staff should not clear such aged items to another suspense-type general ledger account rather than resolving the problem);

- Reviewing management aging report detailing suspense-type general ledger accounts to ensure proper monitoring and clearing;

- Verifying that the previous month's deposits-in-transit cleared the month of review's bank statement for the amount shown on the previous month's reconciliation. Tracing the most recent month's deposits-in-transit as shown on the reconciliation to bank stamped deposit receipts or current month's bank statement, if available. Credit unions should make deposits promptly as specified in the *FCU Bylaws*. If necessary, the deposit-in-transit review may include a random review of receipts to deposits. Staff should not clear deposits-in-transit to another receivable-type general ledger account;

- Reviewing the origin and destination of a random sample of wire transfers provided on the bank statements and verifying that the credit union posted these wire transfers to the general ledger or

carried them as reconciling items. While the destination of wire transfers is generally the corporate account, examiners should trace destinations to other than the corporate account to source documentation from the originator;

- Determining the credit union adequately controls non-FEDWIRE transfers. Sound controls require that the originating bank or institution confirm the transfer with appropriate personnel not responsible for initiating the transfer;

- Reviewing canceled and outstanding checks for unusual payees, unusual dollar amounts, or unauthorized signatures;

- Verifying that staff properly marks voided checks "VOID", and crosses or cuts out the signature portion of the voided check or, more importantly, punches the MICR line;

- Determining the reasonableness of the volume of bank account activity and average bank account balance in relation to the credit union's asset size, volume and amount of member transactions, and compensating balance requirements;

- Determining that the supervisory committee, internal audit department, or other appropriate personnel periodically audits bank account reconcilements; and

- Reviewing that bank account reconciliation policies, practices, procedures, and controls provide for timely reconcilements, adequate safeguards over the bank account, and accountability. Credit unions should complete reconcilements by the due date of the financial statements as specified in the bylaws.

If the bank or corporate account reconcilements are more than 60 days in arrears, examiners should reach agreement with the credit union to bring the reconcilements current, usually within 30 days. If the reconcilements are six or more months in arrears, the credit union is deemed to have serious and persistent recordkeeping problems (per §715.12 of the *NCUA Rules and Regulations*) requiring the credit union to hire an outside, independent auditor to perform an opinion audit. When reconcilements are seriously in arrears, the examiner may

perform a simplified bank reconciliation to determine how close the bank balance is to the book balance and verifying, to the extent possible, outstanding checks and deposits-in-transit.

When the credit union has not properly reconciled accounts or properly researched and corrected adjusting entries, examiners should follow-up to determine that the credit union makes the needed corrections. Examiners should discuss the necessary level of supervision with the supervisory examiner.

Credit Bank Account Balance

Examiners should not criticize credit unions for having a credit balance in the cash account when the credit union has not overdrawn the bank account. Likewise, examiners should not criticize credit unions for overdrawing the bank account infrequently, if the credit union has a written agreement with the bank indicating the bank's willingness to honor checks drawn by the credit union, even though the credit union may not yet have sufficient funds deposited. Examiners should review the costs credit unions must pay when they overdraw their bank account; the costs may be higher than if they had borrowed the funds.

Conversely, if the credit union regularly overdraws its bank account and has no written agreement, it should increase the account balance accordingly. Additionally, if the credit union frequently overdraws its account, with or without a written agreement, examiners should analyze the effect on liquidity and operating costs. Frequent overdraws could indicate liquidity risk, transaction risk, and reputation risk.

Sweep Accounts

Some banks offer a "sweep account" feature to their customers, which allows the bank to sweep some or all of the balance of the credit union's bank account into some form of overnight marketable securities. Using this feature, the credit union can often improve earnings on its bank account. However, the credit union generally bears all of the market risk liability inherent in the sweep transaction.

If examiners identify sweep account arrangements that warrant review, they should determine that (1) a written agreement exists between the bank and credit union, (2) the agreement should coincide with the

credit union's investment policies and practices, (3) the credit union has an acceptable market risk liability, (4) the bank records the sweep transactions in the credit union's name, and (5) the bank sweeps the credit union's cash into investment securities permissible for credit unions.

Treasurer's Drafts

Treasurer's drafts are drafts that a credit union issues against itself and uses in the same way it would use a checking account at a bank. The credit union does not establish a share draft account for itself. It merely issues drafts that it promises to honor when properly presented. The treasurer's draft is an alternative to the bank checking account and allows the credit union to use the float to its advantage.

Credit unions establish treasurer's drafts by using a clearing account at the payable-through bank. The drafts, issued for loan disbursements, share withdrawals, and expense disbursements, clear in the same manner as the members' share drafts. As the payable-through bank receives the drafts, it pays them from the credit union's clearing account at the payable-through bank.

Official Check Programs

"Official check" programs (e.g., Travelers Express, American Express) often appeal to smaller credit unions that do not have their own checking account at a bank, although other credit unions may also use this service. Each day the credit union writes drafts payable through a bank. At the end of the day the credit union wires the total of the drafts written to the official check company.

The credit union earns income on the float and once a month the official check company sends the credit union a list of draft items not cleared (the outstanding check list for the month.) This program does not eliminate the cash reconcilement function. While NCUA does not prohibit this program, default by the official check company could negatively affect the credit union's financial condition and reputation.

On-Us Share Draft Accounts

Frequently, larger credit unions use in-house share draft accounts for processing loan disbursements, share withdrawals, expense disbursements, and even payroll. The process is similar to that of

Treasurer's drafts, but the credit union uses a share draft account rather than a treasurer's draft payable account. The on-us share draft accounts serve as an alternative to the bank checking account and allow the credit union to use the float to its advantage.

Examiners can identify these share draft accounts through (1) inquiries with management, (2) review of canceled and outstanding drafts, and (3) review of zero balance or overdrawn share draft reports. Account numbers of such accounts generally begin with "9's". These are actually liabilities and not share accounts. If a credit union uses on-us share draft accounts, it can inflate or deflate actual total share account amounts, which could affect the capitalization deposit.

At any given month-end, the balance remaining in these share draft accounts actually represents outstanding drafts. The examiner could determine that the credit union appropriately accounts for and controls such accounts, and that it closes any remaining balance in these share draft accounts to the related liability account before finalizing month-end financial statements.

Money Orders and Travelers Checks

If examiners review money orders and travelers checks, which are generally off-balance sheet consignment items, they could determine whether the following exists:

- The credit union has adequate policies, practices, and controls to safeguard these negotiable monetary instruments and provide for accountability over the reserve supply and working supply;

- The supervisory committee or other appropriate personnel periodically reconciles the money orders and travelers checks;

- Management maintains the inventory of money orders and travelers checks at reasonable levels as governed by membership demand. If the agreement also requires surety limits, the examiners should review compliance with those limits;

- The credit union opens, counts, and records the shipments of money orders and traveler's checks under dual control;

- The credit union maintains records of serial numbers of money orders and traveler's checks held in the reserve supply and teller working supply;

- The credit union stores the reserve inventory and working supply inventory in the vault during non business hours;

- The credit union posts sales fees to the appropriate income accounts daily;

- The credit union sends sales remittances to the issuer promptly; and

- The credit union destroys money orders and travelers checks, if necessary, under dual control and appropriately logs this activity on a destruction log signed by both parties.

If the review of money orders or travelers checks discloses significant procedural deficiencies, or if staff has not completed current reconcilements, the examiner should observe staff performing an inventory during the examination. As part of this inventory procedure, the examiner should ask the credit union to request from the issuer a listing of money orders and travelers checks issued, but not yet paid. The examiner's inventory should balance with issuer's inventory. The examiner must reach agreement with the credit union to resolve any discrepancies between the two inventories.

Other Negotiable Items

Other negotiable items include, but may not be limited to, postage stamps and theater and amusement park tickets.

Credit unions frequently sell postage stamps, theater tickets, and amusement park tickets. If examiners review postage stamps, theater tickets, and amusement park tickets, they should ensure that the credit union performs inventories at least quarterly and has adequate internal control procedures.

Excessive Transactions

Examiners may incorporate reviews of specialized information systems reports, such as the "Excessive Transaction Report", into their

evaluation of cash operations in automated credit unions. The credit union can change the parameters on the Excessive Transactions Report, but usually sets them to display transactions over $10,000. While the $10,000 parameter is actually for Bank Secrecy Act (BSA) compliance purposes, review of this report may reveal unusual or excessively high transaction volume, which would necessitate further investigation. Refer to the Bank Secrecy Act chapter.

Federal Reserve's Payment System Risk Program

With any payment system, a sending institution may not be able to settle its obligations within a specified time. All FEDWIRE transfers are final and irrevocable when the Federal Reserve Bank (FRB) sends notice of the payment to the receiving institution. Therefore, the receiving institution can pass collected funds immediately to its customer and will bear no risk if the sending institution fails. If the sending institution has insufficient funds in its reserve account at the time the payment order occurs, it incurs a "daylight overdraft." If the sending institution fails that day, before bringing its reserve account into balance, the FRB absorbs the loss.

Systemic risk means the risk that a system participant's failure to settle its net debit position will affect others. The major objective of the FRB's policy statement is to reduce the risk of a settlement failure. The policy statement seeks to achieve this goal by reducing the level of daylight overdrafts and by encouraging institutions to exercise better control over the remaining credit exposure through voluntary adoption of a "cross-system sender debit cap". This cap represents the maximum net debit a depository institution may incur at any one time on all of the large dollar wire transfer systems. It further limits the amount by which an institution's outgoing wire transfers may exceed the value of the transfers received across all systems.

Under the policy statement, the FRB encourages depository institutions to establish their net debit cap based on a self-assessment of three criteria:

(1) Creditworthiness;
(2) Operational controls, policies, and procedures; and
(3) Credit policies and procedures.

Based on the depository institution's evaluation of its strength in these three areas, the FRB determines an overall assessment of the institution. When a depository institution establishes its sender net debit cap, the FRB expects the institution to maintain supporting documentation, a back-up file of its self-assessment, and evidence of its board of directors' review and approval of the cap selected. Appendix 9A, Wire Transfers, provides additional information.

Fraud Detection

If examiners discover fraud or a shortage, they should document the fraud or shortage as completely as possible and notify the supervisory examiner. With supervisory examiner concurrence, the examiner should notify the board of directors and the supervisory committee and request completion of the Suspicious Activity Report (SAR). The examiner will encourage the officials to, at a minimum, (1) suspend the personnel involved with pay, (2) control the access of personnel involved to the credit union, (3) fill the operational void caused by the suspension, (4) contract to perform a fraud audit, (4) notify surety, and (5) file a bond claim after all facts are known.

Ultimately, NCUA must decide the likelihood of pursuing prohibition actions against dishonest individuals. The examiner should seek input for this decision from the supervisory examiner, regional office, and, if necessary, the Office of General Counsel. Should conviction of a crime result for an individual, NCUA usually can obtain a prohibition more easily.

Alternative Examination Procedures for Small Credit Unions

Internal control limitations, primarily the lack of segregation of duties due to limited staff, can exist for many smaller credit unions. When examining non-complex smaller credit unions, examiners may substitute the following review procedures, which may adequately address their internal control concerns in the cash area:

- Observe staff count all cash in the presence of a credit union official or manager, and determine that the count balances to the corresponding general ledger accounts;

- Determine that the reconcilements balance for two month-ends since the previous examination, and documentation exists for

reconciling items (e.g., deposit slips for outstanding deposits.) Examiners may randomly select one month and confirm clearing of reconciling items within reasonable time frames, but the second month should be the most recent month-end bank reconcilement. Review "stale" outstanding checks and outstanding adjustments over 30 days old;

- "Flip" checks. Select a representative month, look at canceled checks for unusual activity (e.g., payee and check signer are the same person, unusual endorsements, etc.);

- Perform receipts and disbursements test for two months since the previous examination. Examiners may randomly select one month, but the second should be the month prior to the current examination. The testing includes reconciling total debits and credits of the general ledger with the total of debits and credits shown on the bank statements. If the receipts and disbursements test results in differences that need further review, the reconciliation of receipts with deposits may pinpoint the differences; and

- Verify that the credit union makes deposits intact and within timeframes consistent with the FCU Bylaws.

If examiners perform this type review, they should document their review.

Receipt and Disbursement Test

The purpose of the receipts and disbursements test is to quickly determine whether or not cash receipts and disbursements posted to the credit union's books tie out to the actual receipts and disbursements on the bank statement. This test will help identify falsified deposits and checks, month-end lapped deposits, and several other areas of cash manipulation; however, examiner's judgment is needed to determine the cause of the problem.

Receipts Test

1) Place the total of the receipts from the general ledger in a cell on the computer or in the memory of a calculator;
2) Total the deposits on the current bank statement;

3) Subtract the outstanding deposits from the previous month as shown on the bank statement, since this represents activity from the previous month. Also, verify that the prior month's deposits appear intact on the current bank statement;
4) Add the outstanding deposits for the current month;
5) Subtract the total of the current month's outstanding deposits (Step 4) from the stored total of general ledger receipts (Step 1):

- If the answer is zero (i.e., the receipts equal the deposits), no apparent problems exist;
- If they are not equal, determine the source of the difference. Small differences often represent re-deposited, non-sufficient funds (NSF) checks. Examiners should look for credit and debit memos and determine how they affect the statement. Larger differences may require the examiner to check the deposits back individually to determine if an error occurred (see reconciliation of receipts with deposits).

Disbursements Test

The procedures are similar to those for the receipts test, except they involve checks written and cleared instead of deposits. Again, if the test does not zero out, determine the reason for the difference. Reasons may include NSF checks, service charges, check printing fees, or other reconciling items. Examiners may find it necessary to prove out the daily totals by running tapes of each day's checks when they cannot readily determine the differences or when they suspect fraud.

Examiners should be able to perform these tests quickly to uncover posting or other problems. They may develop spreadsheets to speed the work and allow the computer to do the calculating.

Reconciliation of Receipts with Deposits

Examiners may choose the test check of tracing or reconciliation of receipts, as recorded in the credit union's books (or tellers' cash received summaries, if not posted), with deposits recorded by the bank. Examiners may use this test check in situations where the receipts and disbursements test indicates problems that require further research. This test also supports and ties in the cash count and the bank reconcilement.

The reconciliation of receipts with deposits documents that the credit union makes bank deposits intact (i.e., the deposits include the exact amount of one or more day's receipts) and deposits them in the bank within the time limitations set forth in the bylaws. Additionally, this test determines that the credit union does not summarize receipts of more than one day on the same cash received summary. (The credit union should prepare a cash received summary each day and attach it to that day's individual teller cash received summaries.)

Examiners could trace funds received from entries on the credit union's books (or tellers' cash received summaries, if not posted) to evidence of deposits in the bank. The suggested minimum period starts with the beginning of the month prior to the month in which the examination takes place and runs through the day of the cash count. The purpose of this test check is to furnish the examiner with a reasonable appraisal of the credit union's practices with respect to depositing of funds received.

Workpapers and References

- Workpapers
  - Red Flag Questionnaire
  - Cash Internal Control Questionnaire
  - Money Order and Travelers Checks Questionnaire
  - ATM Questionnaire
- References
  - *NCUA Rules and Regulations* – 715.12
  - *FCU Bylaws* – 12/87 – XV,1.
  - *FCU Bylaws* – 10/99 – XIII, 1.

WIRE TRANSFERS - APPENDIX 9 A

Overview

An electronic funds transfer (EFT) is any transfer of funds initiated through an electronic terminal, telephonic instrument, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account. Credit unions primarily use wire transfers to transfer their own funds (e.g., for investments or payment of expenses) from one institution to another. However, credit unions also transfer members' funds upon request.

The majority of credit unions wire funds by calling their corporate credit union (or correspondent bank) and instructing the corporate to (1) access the credit union's settlement account at the corporate to fund a wire transfer, (2) forward the funds and the wire instructions to the Federal Reserve, and (3) post the transaction to the credit union's settlement account at the corporate.

Credit unions that have an Internet-based request system may also submit requests for wire transfers to the corporate credit union or correspondent bank electronically. Many larger natural person credit unions directly access the FEDLINE system (or telephone the Federal Reserve directly) and conduct their own transfers. (FEDLINE, the personal computer-based electronic delivery system by which credit unions access the Federal Reserve System's on-line services and information, provides settlement services, cash services, and a means to transfer funds and securities between institutions.)

In any case, all credit unions offering wire transfers must abide by written security policies and procedures that consistently promote safe and accurate transactions. Credit unions can limit their liability and risk of loss by using recommended security procedures, referred in UCC Article 4A as "commercially reasonable security procedures" (e.g., recorded telephone lines, codes, passwords, personal identification numbers (PINs), encryption, etc.) These procedures help assure the authenticity and correctness of payment orders, and apply to telephone, personal computer, or other electronic transmission of the orders to the credit union.

Transaction Security

Credit union officials must write and adhere to transaction security policies. Examiners should review the written policies and determine their appropriateness for the credit union's size and number of employees. Examiners should also request the list of employees authorized to initiate wire transfers and review it to ensure the credit union keeps it current.

Proper controls depend on accountability (including accurate recordkeeping and sufficient documentation) and adequate separation of duties, which small credit unions having few employees can find a particular challenge. Nonetheless, all credit unions involved in wire transfers should carefully develop and strictly adhere to good internal controls.

Most corporates, correspondent banks, Federal Reserve or FEDLINE terminals mandate that credit union employees authorized to send funds by wire identify themselves by passwords, PINs, or test keys.

The credit union should require frequent changing of passwords, depending on the volume of wire activity (e.g., credit unions should change FEDLINE passwords every 30 days and members' passwords at least semiannually.) Credit unions that require regular changing of passwords reduce the risk of an unauthorized user gaining access to a member's account.

The examiner should determine that the credit union properly controls the system of assigning and communicating passwords, and that it promptly acts on suspected compromises of this security by canceling the password and assigning a new one. Examiners should walk through the wire transfer procedure with the credit union staff. Following are examples of controls that credit unions should enact:

- Assign a unique password to each user. Sharing passwords increases the potential to compromise control and accountability;

- Discourage users from selecting easily remembered passwords (e.g., initials, family member's name), or ones that rotate in a pattern, by using PINs or test keys;

- Ensure confidential and secure communication of newly-selected passwords, PINs, or test keys between the credit union and employees authorized to perform wire transfers;

- Instruct employees to close files, turn computer screens from the view of other employees, and refrain from discussing confidential information, including passwords; and

- Control access to the system, passwords, and any backup software when storing passwords on a shared electronic system such as a local area network (LAN.)

Requests for Wire Transfers

To positively identify members, credit unions should require members requesting a wire transfer of any amount to complete and sign a standard authorization form. However, many members make requests for emergencies when the member cannot come to the credit union. In these cases, the credit union should attempt to identify the member over the phone and establish a limit for the amount it will wire under these conditions. Requesting account numbers, social security numbers, or birth dates does not meet minimum security standards for wire transfers. Information not easily accessible to someone other than the member requesting the wire is acceptable (e.g., mother's maiden name, password, etc.) Written procedures should establish a maximum limit (i.e., an amount the credit union has determined it could lose in an unauthorized wire - usually $2,000-$3,000) for wires requested by telephone.

For members regularly requesting telephone wire transfers, the credit union should establish passwords or PINs which it changes routinely. In addition, regular users should sign formal wire transfer agreements that fix responsibility between the parties. The credit union should maintain the agreements on file.

The credit union needs to document wire requests. It must understand that a FAX does not comprise a legal document. Phone calls, unless made on recorded lines, are also difficult to prove; therefore, the credit union should consider installing a telephone recording system on phone lines used for wire transfer calls. At a minimum, the credit union should call back the member to verify authorization of the wire

transfer and record on the wire form the date, time, and initials of the person receiving the request and the person performing the callbacks.

Various credit union departments making wire requests for investments or payment of expenses should record those requests on standard request forms after obtaining approval from individuals authorized to make investments or pay expenses.

Methods of Sending Wire Transfers

Most credit unions wiring through their corporate or a correspondent bank call the institution and request the transfer or submit the request for transfer using a product such as U.S. Central Credit Union's Open Door system or another institution's browser-based transaction program. Authorized users state or enter their passwords or PINs and make or enter the request.

Corporate staff should read back a telephone request order to the requesting credit union for accuracy and may confirm the request by a telephone callback. For Internet based programs, the corporate will probably employ automated checks for accuracy; but may confirm the request through a telephone callback.

Corporate staff should ensure the caller has authority to make the request, and that the requested amount falls within the caller's authority. Most often the credit union's responsibility includes assigning authority to request wires to specific employees and assigning a maximum dollar limit on each employee's authority. The corporate then verifies the caller's authorities to a listing provided by the credit union.

Passwords and callbacks have different purposes and should not substitute for each other. Passwords allow a user into the system, while callbacks confirm the order's source and authenticity. Credit union management may not always recognize this distinction.

Less common (and inappropriate) methods of requesting wire transfers include telegram, telex, and FAX. The ease of compromising the security of these transactions provides each with a great potential for fraud. The examiner should take exception to a credit union's use of any of these methods.

Assuming the credit union has adequate security and proper controls, examiners should not take exception to other forms of electronic transfer, such as Western Union wire terminals, or alternative software such as U.S. Central Credit Union's Open Door product or other browser-based wire request programs.

Pre-Authorized (Card) Wires

Credit unions establish many repetitive wire transfers (e.g., regular or periodic transfers of credit union funds to an investment account at another institution.) For these repetitive wire transfers, the wiring instructions remain the same except for the dollar amount.

The receiving institution (usually the corporate or Federal Reserve) often establishes pre-authorized (card) transfers by creating a template screen in the FEDLINE terminal or within the browser-based transaction program. Then, when the credit union calls in or submits a wire request via the Internet, the caller or person entering the request only gives or enters a password or PIN number and states the need for, or enters, a wire for a certain dollar amount in the credit union's account at "ABC Bank." The caller does not have to give an account number or the bank's ABA number, which results in a more efficient transaction.

The examiner should review the security procedures for establishing, changing, or deleting the credit union's template screen on the FEDLINE terminal or within any browser-based wire request programs. Adequate accountability and control requires a written and confirmed request to establish, change, or delete a pre-authorized template. Additionally, someone other than the operators performing the "initiation" and "verification" functions on the terminal should establish or edit the template screens.

FEDLINE Terminal

A credit union having its own FEDLINE terminal must institute additional controls and security measures beyond those required for accessing the FEDLINE through a corporate or correspondent bank.

Funds transfer messages sent over the FEDLINE terminal must go through two processes before transmission. Initiation involves entering the message into the terminal, while verification requires re-entry into

Sample FEDLINE User Access Report

Local Administration MM/DD/YYYY 14:09:03L 2/C19

MC-F6

User-ID:_____ Name:_____

Password:_____ Verify password:_____

Current states: A Password last changed on:_____ re-try cnt:_____

An 'X' designates what function category a user is allowed to access with an application. No 'X's imply non-restricted functions only.

	Application Code	Function categories					
		Inq.	E/U	V/T	A. Supv.	Supv.	Mngr.
1							
2							
3							
4							
5							
7							
8							
9							

Sample Miscellaneous Security Settings Report

Misc. Security Settings Local Administration MM/DD/YYYY 9:37:58L 6.38

LOCAL ADMINISTRATION ACCESS OPTIONS

User's ID will be suspended after	3	consecutive bad password attempts
User must change password every	45	days
Verification rule	N	(use < F6 > Key)
Override & Release rule	N	(use < F6 > Key)
User-ID will be signed-off after	15	minutes of inactivity

Illustration 9A-1

the terminal of all or part of the message. The security options on the system allow the credit union to decide exactly which data fields within the message it will re-enter. After staff completes the verification process, the FEDLINE terminal automatically transmits the message and transfers the funds.

The examiner should determine that the credit union requires two different employees to perform the initiation and verification processes on the terminal. Both the credit union's written policies and its established control parameters on the system should require this separation of duties. Examiners should ask the local administrator to screen print the "Miscellaneous Security Settings" for purposes of reviewing the controls. (Illustration 9A-1 contains examples of the FEDLINE User Access Report and Miscellaneous Security Settings screen print.)

Miscellaneous Security Settings

The examiner should have the local administrator screen print the Miscellaneous Securities Settings during the examination. The screen print will show:

- Settings for the Verification Rule;
- The Override and Release Rule;
- The number of bad password attempts allowable before the system suspends a user ID;
- The number of minutes the system allows the FEDLINE terminal to remain unattended before it automatically logs off;
- Whether the system suppresses the keyboard eavesdropping message each time a user enters the FEDLINE; and
- Whether the system prints a full or summary account of deleted transactions during the cycle-date rollover.

Verification Rule

The Miscellaneous Security Settings screen displays the setting of the "verification rule" to N, U, or E. The "N" designator allows the same FEDLINE operator to perform initiation, editing (if needed), and verification functions on the same message. In other words, this designator allows one FEDLINE operator to transmit funds. The "U" designator restricts the FEDLINE operator who last initiated or edited a message from verifying that message. Thus, this designator requires

at least two FEDLINE operators to transmit funds. The "E" designator is the most restrictive. It requires that a FEDLINE operator other than the initiator or the editor perform the verification function.

The "N" designator for the verification rule does not require adequate separation of duties; therefore, it is unacceptable for credit unions. Larger credit unions should set this designator at "E" thus requiring the highest level of separation of duties. However, the examiner may accept a setting of "U" for the verification rule, especially if the credit union has limited staff, and if, in the examiner's judgment, it has other adequate controls.

FEDLINE Functions and Access Levels

A two-character code identifies each application in FEDLINE. The following codes assign access authority to an operator:

**	All Applications
AH	Automated Clearing House
AS	Accounting Services
BA	Book-Entry Securities
CS	Cash Services
CH	Check Services
FT	Funds Transfer
HC	Host Communication
HD	Help Desk
LA	Local Administration
MS	Miscellaneous Support
RA	Local Reserve Account
RR	Reporting and Reserves
SB	Savings Bond
SS	Startup/Shutdown Control
ST	Securities Transfer
TA	Treasury Auction
TT	Treasury Tax and Loan

The following six access levels exist within each application:

- Inquiry
- Entry/Update
- Verify/Transmit

- Assistant Supervisory
- Supervisory
- Managerial

The credit union can assign an employee one or more access levels within an application; they need not be the same for each application. For example, the credit union may give an employee inquiry capability for the Securities Transfer (ST) Application, and managerial capability for the Funds Transfer (FT) Application. Also, the credit union need not assign all six levels of access within each application.

The credit union may choose to customize some local options in accordance with the institution's specific operating environment. These rules apply to the entire FEDLINE system installed on the computer, not to a specific application.

The local access options are:

- Number of invalid password attempts;
- Password expiration interval;
- Key verification requirements;
- Override and release rule;
- Automatic sign-off and time-out intervals;
- Suppression of possible keyboard eavesdropping; and
- Cycle-date rollover print delete option.

Local Administrator

The credit union will designate one or more employees as a local administrator for the FEDLINE terminal. The local administrator may add or delete authorized users and authorized functions of established users. (For example, funds transfer is only one of several functions. Others include securities transfers, ACH transactions, etc.) The local administrator can also select, add, delete, or change an individual's security options.

The local administrator should be an employee who works outside the operational area responsible for the terminal and who the credit union (1) would challenge for trying to gain terminal access routinely, and (2) will not assign any other duties on the FEDLINE terminal. The

examiner may have to make certain allowances for the limited staff in a smaller credit union.

User Profile Report

During the examination, the examiner should identify and ask the local administrator to print out FEDLINE's User Profile Report in the examiner's presence.

The User Profile Report shows all authorized users, the functions each may perform, and the authority level within each authorized function. The examiner should identify all users on this report and determine that the credit union has broad enough authorization levels to allow staff to efficiently carry out their duties and responsibilities, yet sufficiently restricts these authorization levels to ensure sound internal controls.

The examiner should pay particular attention to the following function codes:

- ** (Double asterisk) - Allows the user to perform any function
- LA - Local administrator function
- FT - Funds transfer function
- ST - Securities transfer function

Anyone with the "**" function code can perform any function. The examiner should determine the appropriateness of giving such widespread authority. Two different employees should always perform the initiation and verification functions. However, when possible, NCUA strongly encourages greater separation of duties.

As mentioned earlier, the personnel authorized to perform the LA function should not have authorization to perform any other function. Under certain circumstances, a local administrator could unilaterally set himself up to perform other functions at any time. However, the additional time required to set up the new authorization and the attention that would result from the local administrator being at the terminal, as well as constant internal auditing and monitoring of FEDLINE activity, should deter any unauthorized actions by the local administrator. Internal auditing and monitoring of the FEDLINE

system should include review of user access by someone not involved in the funds transfer process, other than the local administrator.

The FT code designates those employees who may perform funds transfer functions. The examiner should determine that the credit union has assigned this code to the minimum number of employees necessary for efficient operation. No employee outside the funds transfer department should have authorization to perform the FT function at any level higher than "inquiry."

The ST code designates those employees who may perform securities transfers on the FEDLINE terminal. Examiners review the use of this code in conjunction with the examination of the credit union's securities safekeeping program.

User Access Report

The examiner should ask the local administrator to print the User Access Report.

FEDLINE Security Features

- Number of password tries. Every user on the FEDLINE terminal has a personal password that the system requires before an individual can perform any function. The system requires periodic change of personal passwords. The local administrator can set the number of times a user may enter an erroneous password before the system locks out that user's ID. The miscellaneous security settings screen shows this setting.

  The examiner should determine the appropriateness of the number of password-attempts setting. Normally, the credit union setting should allow no more than three bad attempts.

- Override and Release Rule. This setting, which restricts the overriding and releasing of messages, has available the same three options as the verification rule.

- Automatic log-off of unattended FEDLINE terminal. The miscellaneous security settings screen also states the number of minutes that the FEDLINE terminal will stay active before automatically logging off. The local administrator can set this

parameter at any number from 0 to 999. If the local administrator sets this number at other than zero, the terminal will automatically log off after being left unattended for the pre-set number of minutes. If the local administrator sets the number at zero, the terminal will not log off automatically.

If the local administrator sets the time parameter too long, chances increase that one operator may gain access to the terminal while it is still logged on under another operator's user ID, resulting in a loss of accountability.

The examiner should review the unattended FEDLINE terminal setting and determine its appropriateness. Normally, the credit union should set the parameter between one and five minutes.

- Suppress Possible Keyboard Eavesdropping. This setting permits the administrator to turn off the "possible keyboard eavesdropping" message noted each time a user enters FEDLINE.

  The examiner should determine that the administrator has not suppressed the message. The credit union should enact and monitor a control preventing a Terminate and Stay Resident (TSR) program on the terminal to ensure that no one copies various keystrokes.

- Cycle Date Rollover. Before beginning each day's work, a credit union employee must perform a function on the FEDLINE terminal known as the "cycle date rollover," which resets the date on the terminal. The FEDLINE system requires the operator to clear or cancel messages still pending (i.e., initiated but not verified or transmitted) before performing this function. The policies should require canceling and reporting to management any pending messages.

  The security administrator can set the system to print either a full or a summary account of deleted transactions during the cycle-date rollover process. Either report documents pending message problems. While the detailed report contains all the information about the transaction, the summary report shows only limited information about the transaction.

- Update Message Application Attributes. This function allows staff persons with managerial access to customize several control related aspects of outgoing message processing including: verification thresholds, a duplicate reference number edit, and an accountable message transmission limit. Management can establish these verification requirements for the message processing functions at the application level for Funds Transfer, Securities Transfer, Checks, or Treasury Tax and Loan (TT&L) messages. Examiners can determine whether the credit union has set any of these customized features by asking that the staff person with managerial access to the applications screen print the settings on the update message application attributes' screens.

  The credit union can set verification thresholds for accountable and non-accountable messages for which it will impose the verification requirement. If the credit union sets the dollar amount at 0.00, it will verify all messages; whereas, if the credit union sets the dollar amount at 99,999,999,999.99, it will verify no messages. For other settings, it will verify any amount over the amount set. NCUA recommends that the dollar amounts be set at 0.00 to verify all messages.

  The credit union can automatically check for duplicate reference numbers when creating or updating information depending on the numbering of source documents. Good internal controls require activation of this edit check to prevent duplication of numbers. Examiners should determine that the credit union uses a different number on each source document.

  Credit unions can prevent transmission of accountable messages (including those with a verified status) until an authorized operator using the message status override function releases the messages. Credit unions with larger staffs usually activate this additional control; however, credit unions with smaller staffs often set the control at "N" indicating that the system will automatically que verified messages for transmission. Examiner's judgment will determine the adequacy of the setting.

Reconciliation of the FRB Account and Funds Transfers

The credit union should reconcile the number and dollar amounts of funds transferred to the Federal Reserve account balance throughout the day. Periodic reconciliation discourages fraud. Smaller credit unions may reconcile only two or three times during the day; larger credit unions more often. In addition, staff must perform a detailed reconciliation of the Federal Reserve account daily. The individual responsible for reconciling should not otherwise perform funds transfer duties.

Audit Copy of FEDLINE Messages

A FEDLINE printer records messages on the FEDLINE terminal. There are three categories of messages:

- Outgoing transactions;
- Incoming transactions; and
- Miscellaneous messages.

The credit union can have all messages going to the same printer, or direct different categories of messages to different printers. The FEDLINE system assigns a sequence number to each message. Each category has a separate sequential numbering.

In order to establish an audit trail, the credit union should use multiple-part paper on the FEDLINE printer. The credit union should maintain one copy of the messages in continuous form for the entire day, from log-on to log-off. If staff must perforate the paper (e.g., when the box of paper runs out), a supervisor other than a FEDLINE terminal operator should inspect the old and new continuous forms to account for all messages and should initial the beginning and end of each form where the gap occurs. Supervisory review of the entire audit trail for unauthorized attempts to access the system, unauthorized messages, etc., should occur daily. The supervisor should initial the audit trail indicating the review. The credit union must retain daily audit trails through both the next audit and examination periods.

Functions, Applications, and Security Parameters in Browser-Based Systems

Corporate credit unions or other third-parties, including correspondent banks, provide a number of browser-based programs used by credit unions to submit wire transfer requests. Each program has its own defined functions, applications, and security parameters. While each program has differences, the functions, applications, and security parameters should essentially mirror the control features available using Fedline.

A wire transfer made through a corporate credit union or correspondent bank using browser-based software rather than FEDLINE does not change the need for involving two credit union employees in performing the initiation and verification processes. System parameters similar to FEDLINE controls should require this separation of duties. Examiners should ask the browser-based program local administrators to print out a screen similar to the FEDLINE "Miscellaneous Security Settings" screen, showing the availability and activation of a dual control feature. Browser-based programs also generally provide for maximum dollar limits for each user. Usually, examiners can verify the presence of dollar limits by accessing the system's User Authority Reports.

Physical Security

Following are important aspects of physical security:

- Location of the FEDLINE terminal. Ideally, the credit union should locate the FEDLINE terminal in a secured room dedicated solely to wire transfer activities, with only authorized terminal operators and their supervisors having access. However, smaller credit unions having limited space often cannot place the terminal in a secured room. In that case, the credit union should place the terminal in a low traffic area, but within sight of the workstations of all the terminal operators or the operators' supervisor. This reduces the likelihood of unauthorized personnel gaining access to the terminal.

- Number of staff present. The credit union's written wire transfer policies and procedures should require the presence of at least one employee who understands and can operate the FEDLINE terminal and a supervisor whenever the FEDLINE terminal is operational.

- Security of telephone lines. The examiner should determine the security from eavesdropping of the credit union's telephone lines. A breach of security could occur from outside or inside the building. The telephone company bears responsibility for security outside the building; security inside the building rests with the credit union.

  Examiners should evaluate the security of the room containing the credit union's telephone switching panel (i.e., locked with management maintaining the key) and determine that the telephone system does not allow one extension to listen in on another system. An unauthorized person could listen in on a telephone line at this switching panel with the aid of relatively simple equipment. If a repairman needs access to the panel, management should verify the repairman's identification and take necessary precautions to avoid breaches of security any time the panel is unsecured.

- Security of encryption key diskette. The Federal Reserve provides all authorized, licensed users with a diskette containing the encryption key for the FEDLINE terminal. The terminal has a security feature that requires the reload of the encryption key if the credit union moves the terminal. FEDLINE licensing agreements allow maintaining only two copies of the diskette; one copy at the credit union and the other offsite for use during disaster recovery. The credit union should keep both diskettes in secure areas with controlled access, such as a safe or safe deposit box.

Policies, Procedures, and Guidelines

The AIRES Wire Transfers Questionnaire inquires about internal control practices pertaining to the wire transfer operation and, more specifically, whether the written policies and procedures address certain practices. Examiners should determine that employees follow written procedures.

Written internal control procedures help ensure consistent application, enforcement, and accountability, even when a change of staff or management occurs. Appropriate procedures should include:

- Written funds transfer agreements. The credit union should have a written funds transfer agreement with each applicable institution,

outlining the duties and responsibilities of each party to protect the interests of both institutions. The agreement should specify the responsibilities of the institutions regarding security features such as passwords, PIN numbers, test keys, and telephone callback.

The institutions should also have written documentation that authorizes certain employees or officials to request or send funds transfers. If this is the only documentation, the examiner should take exception and require the development of a formal funds transfer agreement.

Credit unions that send members' wires should also have written agreements with their members notifying them of their duties and responsibilities, assigning liability in the event of a loss, and documenting the security procedures to be used.

- Personnel policies for wire transfer operation. To enhance the funds transfer operation internal controls, written personnel policies should incorporate items that may help improve the credit union's chances of collection if someone files a bond claim against an employee who violates the policy. These should include restricting or limiting the hiring of relatives for key areas, filling vacancies internally, and eliminating access on termination or resignation.

- Contingency planning for wire transfer operation. The examiner should determine that the credit union has an adequate disaster recovery plan for its wire transfer operation, and that management has sufficiently familiarized all wire unit employees with the plan. Some credit unions, particularly those whose disaster recovery plans include relocating to a "hot site," may have the capability of remaining online with the Federal Reserve during a disaster. For those, procedures and controls should remain much the same as during normal operations. However, many credit unions plan for their funds transfer operations to go offline in case of a disaster. Either way, the credit union must maintain proper security over the operation during execution of the disaster plan and must periodically test the plan and document the test results.

- Audit or review of wire transfer operation. The sensitive nature of wire or securities transfers requires an audit or review at least annually. The credit union's internal audit department or external auditors may perform the review. If the credit union has its own wire or securities transfer system, it should hire auditors who have independent training in the credit union's wire transfer communication system, and who participate in planning for changes in equipment, systems, and operating procedures. The auditors should establish a formal audit program covering all aspects of the wire or securities transfer operation.

Record-keeping Requirements

The Federal Financial Institutions Examination Council (FFIEC) encourages credit unions to support law enforcement's efforts to identify and prosecute money laundering activities involving large-value funds transfer systems. This support includes maintaining, to the extent practical, complete originator and beneficiary information when sending payment orders over any funds transfer system.

Additionally, the Bank Secrecy Act (BSA)[1] requires certain recordkeeping requirements for credit unions engaged in wire transfer operations on behalf of their members (applies only to transmittals of $3,000 or more).

- The credit union must retain records (originals, copies, electronically, or on microfilm) for five years; and
- When the credit union is the originator's financial institution, it must retain the following records:

  - Name and address of the originator;
  - Amount of the payment order;
  - Execution date of the payment order;
  - Payment instructions received from the originator with the payment order; and
  - Name, address, account number and any other specific identifier of the beneficiary, if these are received with the payment order.

[1] NCUA Letter to Credit Unions No. 173, July 1995, contains additional information about the BSA revision.

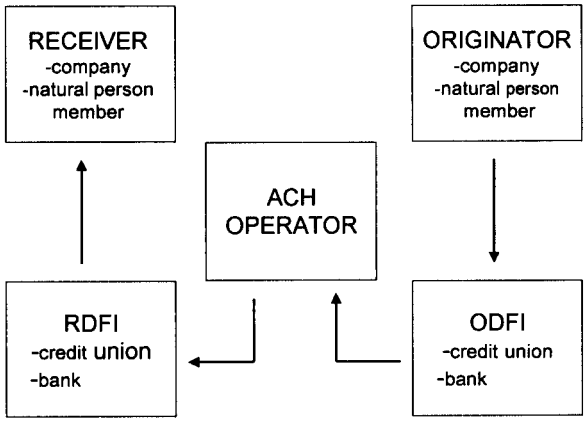
AUTOMATED CLEARING HOUSE NETWORK - APPENDIX 9B

Overview

The Automated Clearing House (ACH) network electronically exchanges funds and related information among individuals, businesses, financial institutions, and government entities. The ACH Operator provides a central distribution and settlement point for transmitting funds electronically between an originating depository financial institution (ODFI) and a receiving depository financial institution (RDFI.)

The following illustration depicts the ACH Network and their interrelationships:

How the ACH System Works



- Originator. The originator directs a transfer of funds to or from a receiver's account by providing the ODFI with payment instructions. The originator agrees to initiate ACH entries into the payment system according to an agreement with a receiver. A company usually acts as the originator (but an individual member can also originate ACH transactions) directing a transfer of funds to or from a consumer's or another company's account. The term "company" refers to the originator of electronic ACH entries and does not imply exclusion of other types of organizations.

- Originating Depository Financial Institution (ODFI.) The ODFI receives the payment instruction from the originator and forwards the instructions to the ACH operator. A depository financial institution (DFI) may participate in the ACH Network as a RDFI without being an ODFI; however, if a DFI chooses to originate ACH entries as an ODFI, it must also agree to act as an RDFI.

- ACH Operator. The ACH operator is a central processing facility operated by the Federal Reserve Bank or a private sector organization that (1) receives entries from ODFIs, (2) distributes entries to appropriate RDFIs, and (3) performs settlement functions for the affected financial institutions.

- Receiving Depository Financial Institution (RDFI.) The RDFI receives ACH entries from the ACH operator and posts them to the accounts of its depositors (receivers.)

- Receiver. The receiver is a natural person or organization whose account is either debited or credited in payment or collection. The receiver must authorize an originator to initiate an ACH entry to the receiver's account with the RDFI.

- Third-Party Processor. Third-party processors are data processing service bureaus, financial institutions, or other organizations that provide ACH processing services for financial institutions. A third-party processor may serve as an agent for an ODFI or RDFI; however, the ODFI or RDFI remains responsible for compliance with ACH rules.

Small credit unions and large credit unions approach ACH transactions differently.

- Small credit unions usually perform transactions through a third-party processor. The parties either courier or fax detailed information back and forth or communicate using modem communications.

- Large credit unions usually perform transactions directly on a FEDLINE terminal that communicates with a Federal Reserve

Bank (ACH operator) or uses alternative software to communicate with a processor.

Data Flow versus Fund Flow

Unlike the wire transfer and check systems, the ACH is both a credit and a debit payment system. ACH credit transactions transfer or distribute funds from the originator to the receiver, resulting in a deposit to the receiver's account. Conversely, ACH debit transactions transfer or collect funds from the receiver to the originator resulting in a withdrawal from a receiver's account.

Regardless of the funds flow, ACH data flows in the same direction, from originator to receiver as follows:

1) The originator initiates a debit or credit payment order to the ODFI.
2) The ODFI transmits the payment information to the ACH operator.
3) The ACH operator receives data from the ODFI and sorts the entries by routing number.
4) The ACH operator transmits the entries to the RDFI.
5) The RDFI receives, processes, and posts the ACH data to the receiver account on settlement day.

ACH Applications Codes and Uses

The ACH Network supports a number of different payment applications. A unique Standard Entry Class (SEC) Code identifies each application and the related ACH record format used to carry the payment and payment-related information. An originator initiating entries into the system codes the entries as either a debit or credit, which affects either a consumer or a corporate account at the RDFI. Listed below are SEC Codes and the different products each code supports.

Consumer Applications

- Prearranged Payment and Deposit Entries (PPD) include both Direct Deposits and Direct Payments.

  - Direct Deposit is a credit application that transfers funds into a consumer's account at the RDFI. These funds represent a variety of products, such as payroll, interest, pension, etc.

- Direct Payment (Preauthorized Bill Payment) is a debit application. Companies with billing operations may participate in the ACH Network through the electronic transfer (direct debit) of bill payment entries. Through standing or single entry written authorizations, the consumer grants the company authority to initiate periodic charges to their account as bills become due. Examples of recurring bills paid by ACH include insurance premiums, mortgage payments, and installment loan payments. Utility payments represent a non-recurring bill (i.e., the amount varies) paid by ACH.

- Point of Purchase Entries/Shared Network Transactions (POP/SHR). Two SEC Codes that the consumer most often initiates via a plastic access card, representing point of sale debit applications in either a shared or non-shared environment. POP transactions also include conversion of checks to an ACH debit application at the point of sale.

- Machine Transfer Entries (MTE). The Network supports the clearing of transactions from automated teller machines (ATMs.)

- Customer Initiated Entries (CIE). Credit applications where the consumer initiates the transfer of funds to a company for payment of funds owed to that company, typically through some type of home banking product.

- Telephone Entries (TEL). A single entry debit application initiated by an originator pursuant to an oral authorization obtained over the telephone to effect a transfer of funds from an account of the receiver. This type of entry applies only to a single entry where no standing authorization exists and originator and receiver have an existing relationship or, absent the existing relationship, the receiver initiates the call.

- Web Entries (WEB). Debit applications initiated by an originator pursuant to an authorization from the receiver via the Internet to effect a transfer of funds from an account of the receiver.

Corporate Applications

- Cash Concentration or Disbursement (CCD). A credit or debit transaction where corporate entities either disburse or collect funds between themselves. This application can serve as a stand-alone funds transfer (CCD) or it can support a limited amount of payment-related data with the funds transfer (CCD+).

- Corporate Trade Payments (CTP). These allow corporations to transfer funds (debit or credit) within a trading partner relationship.

- Corporate Trade Exchanges (CTX). These support the transfer of funds (debit or credit) within a trading partner relationship in which a corporation sends full ANSI ASC X12 message or payment-related UN/EDIFACT information with the funds transfer.

Other Applications

- Automated Accounting Advice (ADV). An optional service provided by ACH operators that identifies automated accounting advises of ACH accounting information in machine readable format to facilitate the automation of accounting information for participating DFIs.

- Automated Notification of Change or Refused Notification of Change (COR). An RDFI or ODFI uses this when originating a notification of change or refusing notification of change in automated format. Also, the ACH operator uses it when converting paper notifications of change to automated format.

- Death Notification Entries (DNE). Agencies of the federal government use these to notify a DFI that the recipient of government benefits has died.

- Returned Entries (RET). ACH operators that convert paper returns to automated format use these. ODFIs that originate dishonored returns also use them when the dishonored return carries the SECC RET.

- Truncated Entries (TRC/TRX). These identify batches of truncated checks.

- Destroyed Check Entries (XCK). An institution can use these for collecting certain checks that were destroyed.

Regulations That Apply to ACHs

ACH Rules. National Automated Clearing House Association (NACHA), the governing body for the ACH network, publishes the rules annually. The rules incorporate those items approved by the NACHA members.

User compliance with the ACH rules enables the ACH Network to operate efficiently. These rules provide warranties and indemnification addressing origination, receipt, and prompt return of the entries. Primary responsibility rests with ODFIs for most of the warranties and indemnifications. However, if the parties enact an agreement stipulating different responsibilities, many of the ODFI's responsibilities can pass through the ODFI to the originator. These warranties and indemnifications reside with ODFIs and originators because they have primary control over the initiation of entries.

- ODFIs must:

  - Ensure proper authorization of the entries;
  - Submit timely entries into the ACH system;
  - Terminate the origination of entries when appropriate;
  - Meet the requirements for data security and personal identification numbers in certain applications, when appropriate;
  - Ensure that the entries contain the appropriate information;
  - Assure an agreement is in place with originators and sending points; and
  - Comply with the ACH rules.

  The ODFI indemnifies the RDFI, ACH operator, and ACH association against loss when breaching any of these warranties. NACHA may require ODFIs that fail to adhere to the ACH rules to reimburse an RDFI or ACH operator for claims, losses, or expenses (including attorneys' fees and costs) that result directly or indirectly from the breach of warranty. Thus, a failure to comply with the warranties may result in a loss to an ODFI. While ODFIs assume responsibility for most warranties related to ACH

transactions, the RDFI warrants to each ODFI, ACH operator, and ACH association that the law permits it to receive entries allowed by the ACH rules and to comply with the requirements of the rules concerning RDFIs and participating DFIs.

- RDFIs must perform the following in a timely manner:

  - Receive and validate all ACH entries;
  - Post to receiver's accounts;
  - Validate pre-notifications;
  - Return entries that do not post within proper timeframes;
  - Handle remittance data as receiver requires;
  - Make funds available to the receiver within proper timeframes; and
  - Fulfill responsibilities when using a receiving point.

To limit their risk exposure, credit unions must acquire information and knowledge of ACH rules. They must also comply with the following applicable regulations:

- Electronic Funds Transfer Act (EFTA). Provides for rights and duties of consumers and financial institutions regarding electronic funds transfer. EFTA covers transfers initiated by both the private sector and the government;

- Regulation E. Issued by the Federal Reserve Board of Governors implementing EFTA to ensure consumers a minimum level of protection in disputes arising from electronic funds transfers;

- UCC-4A. Developed in part for wire transfers, but also applies to wholesale (institution-to-institution) ACH credit transactions and certain ACH credit transactions that are not subject to the EFTA. UCC-4A does not apply to ACH debit or to ACH credit transactions subject to EFTA; and

- Green Book. Published by the Financial Management Services agency of the Treasury Department. The Green Book specifies procedures for ACH transactions originated for the Federal Government.

Risks to the Credit Union

The amount of risk associated with processing ACH payments varies based on whether the item is an ACH debit or an ACH credit, and whether the credit union receives or originates the item. Similar risks exist in the ACH system as those within the wire transfer and check payment systems.

Credit unions must understand payment processing risks (i.e., credit or exposure, operational, fraud, systemic, and third-party processing) and implement detailed written policies and procedures in place to control them.

Credit (Exposure) Risk

The risk that a party to a transaction will not have sufficient funds for settlement is called credit (exposure) risk. This risk often arises when one company that is a party to the transaction fails or is bankrupt before settlement occurs. The examiner must determine that the credit union limits the risk through necessary controls.

- ODFI Credit Risks

  - ACH Credits. An ODFI incurs temporary exposure to credit risk for the period of time between the initiation of an ACH credit file (from one of its originating companies) and the time when the company funds the account (normally on the settlement day, which is one to two business days after initiation.) ACH rules do not allow the ODFI to reverse ACH credits for failure of the originator to fund its account at the ODFI. Therefore, the ODFI is financially responsible for one to two days or until it receives funding from the originator. During this period of time the ODFI has, in effect, granted an unsecured short-term loan. Losses could occur if the company went bankrupt or failed to fund the account between the date of origination and the date of settlement.

    The amount of risk an ODFI assumes is the total amount of the file not the individual transactions. Therefore, ODFIs must establish risk control parameters and limits based on the file totals as well as transaction amounts.

If a credit union is an ODFI, it must establish credit monitoring and control procedures over its members for whom it originates ACHs (similar to business lending requirements.) Credit union ODFIs must assign members' ratings and exposure limits and must continuously monitor them throughout the various departments of the credit union.

Requiring pre-funding of the accounts also enables credit unions to protect themselves. When credit unions take this step, they are only at risk if the originating company filed for bankruptcy between the origination date and the settlement date. In this instance, the funds may become property of the trustee of the bankruptcy court. Usually, this would merely delay the credit union's obtaining final funds. To further protect themselves, credit unions could require that the originating party deposit pre-funded amounts on the origination date into an escrow account in the credit union's name. This would reduce the likelihood of a dispute between the bankruptcy court and the credit union. Examiners should note that ACH rules do not require pre-funding and credit unions that require pre-funding could put themselves at a competitive disadvantage.

- ACH Debits. The ODFI incurs temporary risk from the day the originating company has the funds available until the RDFI or the receiver can no longer return the individual ACH debit entries. An ACH return is an ACH debit or credit that the ACH operator, receiver, or the RDFI returns to the ODFI. Reasons for returning ACH debits include insufficient funds, closed accounts, unauthorized transactions, stop payments, etc.

  Return time for ACH debits falls within two general categories: (1) RDFIs may return non-authorized or revoked authorization consumer debits up to 60 calendar days after the original settlement date, and (2) all other returns, which the RDFI's operator must receive by its deposit deadline in order to make the return entry available to the ODFI no later than the opening of business on the second banking day following the settlement date of the original entry.

Normally, the ODFI charges back a returned ACH debit item to the account of the originating company. However, when bankruptcy or other legal actions leaves the originator's account closed, frozen or with insufficient funds, the ODFI may suffer a loss for the amount of the returned ACH debit item. Controlling this risk presents difficulty because an institution cannot judge whether or not the RDFI and receiver will have the funds necessary for the transaction to occur.

The amount of risk from originating an ACH debit application is generally for the amount of returned individual items and not for the amount of the entire file. Typically, this risk is low, particularly for consumer ACH debit applications such as preauthorized debits and point of purchase (POP) transactions. These consumer transactions generally have small dollar amounts. However, the consumer's right of recision under the ACH rules and Regulation E can cause greater temporary risk. Examiners should be aware of one exception: the ODFI can have risk for the entire amount of the originated file for cash concentration debits.

Credit unions can control the risk of ACH debit returns by placing holds on a portion of the originator's account for a reasonable period of time until the receiver most likely will not return the items. Additionally, they can require the originator to place collateral in an account in the credit union's name. Ensuring against return of all originated volume would require holds for up to sixty business days, a rarely encountered practice. Generally, hold amounts equal a percentage of the total files and reflect historic return rates for each originator and application. Credit unions can also control debit return risk by lowering the exposure limits for the originating company.

- RDFI Credit Risks

  - ACH Credits. The risk to the RDFI in receiving an ACH credit corresponds directly to the finality granted by its ACH operator and can vary. If the Federal Reserve serves as the ACH operator, ACH credits received by an RDFI are final (the point in time where the Federal Reserve cannot reverse the entry

from the RDFI's reserve account) after the close of business on settlement day. The Federal Reserve interprets finality for ACH credits as when the credit union posts the transactions to its reserve account, which can be as late as just prior to the opening of business on the day following settlement.

If the ODFI fails before or during the day of settlement, the Federal Reserve may reverse ACH credit transactions originated by the ODFI and settling on that day. Usually, when the RDFI receives credits, the Federal Reserve credits the receiver's account on the settlement day leaving the credit union open to risk if the ODFI fails and the Federal Reserve reverses the entries. The RDFI's exposure extends only to the amount of funds it made available before settlement is final. If it reverses the transaction, the RDFI will debit the member's account that it previously had credited. The RDFI runs the risk that the receiver's bankruptcy or failure will prevent it from recovering these funds.

RDFIs face operational risks related to ACH credits. Most liability centers on promptly posting the credits. RDFIs may expose themselves to legal costs and civil penalties when they fail to comply with these posting deadlines. Therefore, credit unions acting as RDFIs must comply with the rules governing ACH transactions.

- ACH Debits. The RDFI's operational risk in processing ACH debits lies in deciding whether or not to return an ACH debit by its ACH operator's deposit deadline, so the ODFI has the return entry available no later than the opening of business on the second banking day following the settlement date of the original entry. However, deadlines for unauthorized debits, and instances where authorization has been revoked, allow up to sixty days for a return. RDFIs that fail to meet these return timeframes may experience a loss if the ODFI dishonors the return as untimely.

  Credit unions can control this risk by automatically returning ACH transactions for insufficient funds. However, some credit unions may choose to assume some credit risk in processing

ACH debits by allowing an ACH debit to post, even if it overdraws the receiver's account. While some credit unions may allow this as a common practice (similar to allowing members to overdraw their checking accounts), the examiner should determine whether or not the credit union has implemented adequate controls and monitoring procedures.

Operational Risk

Operational risk, which varies with the type of processing, is the danger that an unintentional error will alter or delay a transaction. Examiners should determine that the credit union has implemented necessary controls to limit this risk. Following are examples of operational risks and the necessary controls that credit unions must have in place to protect against them:

- Hardware failure. Management reduces this risk through reliable equipment, regular maintenance, responsive service personnel, and adequate backup (including addressing hardware substitution or replacement in the credit union's disaster recovery plan.)

- Software failure. Management limits this risk by adequately testing the vendor's or service provider's software before relying on it for processing. Credit unions that develop their own software can reduce the risk of disruption due to software problems with sound software development practices (e.g., adequate documentation, sound testing procedures, tight change control procedures, effective recovery facilities, and periodic internal and external audits.)

- Data loss. Management can reduce this risk by implementing the following controls:

  - Storing data securely. Management must protect electronic files against unauthorized or inadvertent change by using file security techniques and must keep hard copy records in locked storage;
  - Limiting access to data to authorized personnel;
  - Duplicating, backing up, and storing data offsite to protect against data loss or destruction;
  - Establishing and maintaining audit trails of all transactions and changes;

  - Accounting for all files to ensure that staff (1) only processes current files, and (2) does not inadvertently duplicate or omit a file from processing; and
  - Balancing file totals during processing to ensure that staff does not drop, change, or duplicate transactions.

- Telecommunications failure. Management can limit this risk by (1) maintaining telecommunications equipment (lines, modems, authentication or encryption devices, etc.) in working order; (2) physically protecting the equipment; and (3) developing diagnostic tools and backup modes of transmission in the event of a problem.

- Power failure. Management can reduce this risk by obtaining an uninterruptible power supply system to remove spikes and transients from public power and provide auxiliary power during a blackout. Additionally, management should arrange for a generator to handle longer-term power failures.

- Human error. Management can reduce this risk through (1) good supervision, (2) detailed operating procedures, (3) effective training, (4) periodic internal and external audits, (5) monitoring file and dollar controls, and (6) adequate audit trails.

- Staffing problems. Management can reduce the risk of problems resulting from absences, turnover, work stoppages, etc., which vary with the size of the credit union, by emphasizing cross training and good supervision. Staffing problems in small credit unions often result from only one or two people knowing the process. In very large credit unions, the specialized nature of each activity enables few people to know the overall process.

- Natural disasters. Management cannot control this broad category of operational risk, which includes disasters such as earthquake, flood, and fire. However, management must develop and test disaster recovery plans to identify alternate modes of operations and alternate operating sites and to ensure that operations will continue should a disaster occur.

Fraud Risk

Fraud risk is the danger that an employee or interlopers who gain unauthorized access to the system will initiate or alter a payment transaction in an attempt to misdirect or misappropriate funds.

Examiners should review for adequacy the credit union's controls, which should include the following:

- Personnel practices. Management must write personnel policies that enhance internal controls within the ACH operation.

- Physical security. Management must (1) limit access to computer and communications equipment sites to authorized personnel, (2) protect sensitive equipment within the secured area using access controls or device locks, and (3) secure and limit access to all data on portable media (tapes, disks, hard copies, microfiche, etc.)

- Data security and integrity. Management should (1) purchase commercially available software products to access production data files; (2) limit access to specified programs or user IDs by setting up each file for read-only or read-and-write access; and (3) employ encryption, authentication, and dial back data protection techniques when accessing data-in-transit from one participant to another.

  Both the encryption and authentication require the use of a key, which may reside on a hardware component such as a circuit card or may be a data element that authorized personnel enters into a security program or system. The assignment, distribution, and control of encryption or authentication keys represent important data security controls.

- Software and data changes controls. Management must maintain detailed written development and change policies.

- Access restriction. Management must restrict access on software products using (1) operator passwords to prohibit entry by unauthorized personnel; (2) automatic features to control the number of unsuccessful password attempts, password expiration, or designated periods of inactivity; (3) multilevel functions by password to require dual control and ensure that no single employee can create and send transactions (e.g., restricting one

operator to file creation and a second operator to file approval or transmission); and (4) system administration level procedures that require secondary approval to assign, initiate, and maintain passwords.

- Processing dollar and file limit controls. Management must require use and enforcement of exposure limits (1) at the time of entry, batch, or file creation; (2) at the time of transmission; or (3) both (1) and (2.)

- Operational controls. Management must require procedures to implement the following operational controls:

  - File controls to ensure that staff (1) accounts for all files at each step in ACH processing, (2) only processes current files, and (3) does not accidentally or intentionally duplicate or omit files from processing;

  - Dollar controls to (1) confirm dollar totals at each step in ACH processing, and (2) help ensure in-balance ACH files, accurately posted accounts, and properly settled ACHs;

  - Date controls (file creation date, effective entry date, and settlement date) to monitor that staff processes the files within the time frames established by the various regulations;

  - Exception reporting to monitor (1) circumstances such as over-limit activity, (2) anticipated files not received, and (3) file inconsistencies that may suggest error, intrusion, or duplication;

  - Audit trails including procedures to (1) maintain a record of all ACH transaction data and all changes to static data, (2) respond to member inquiries, (3) reconstruct a sequence of events if a problem occurs, and (4) comply with NACHA rules;

  - Reconciliation of the actual entries on the Federal Reserve Statement of Account or similar statement from a correspondent financial institution to verify that the ACH work settled as anticipated. Proper segregation of duties requires that

the staff member responsible for reconciling ACH transactions should not be otherwise involved in the ACH processing; and

- Internal audits of the ACH process. NACHA rules require each financial institution to complete an internal audit of its ACH operations at least once every year (a copy of which the credit union must retain on file.) Completion of the audit by all financial institutions reinforces compliance with the ACH rules and improves the overall quality of the ACH network.

Systemic Risk

Systemic risk is the danger that the inability of one funds transfer system participant to settle its commitments prevents other participants from settling their commitments. Systemic risk is closely related to credit risk. While a fraudulent or erroneous transaction could constitute a source of systemic risk, a participant's failure would more likely trigger a major settlement failure.

The likelihood of systemic risk varies greatly among payment systems. A connection exists between the dollar volumes a network handles and the systemic risk involved: the greater the number of high dollar payments a network processes, the greater the systemic risk, and the greater the need for elaborate risk controls.

A small threat of systemic risk relates to ACH transactions, because a far less average dollar value exists for ACH transactions than for FEDWIRE or CHIPS. Rarely does a financial institution's position with respect to gross ACH settlement approach its capital level. A financial institution's position on the FEDWIRE or CHIPS network will more likely exceed its capital.

Third-Party Risk

Third-party processors include data processing service bureaus, financial institutions, or other organizations that provide ACH processing services for credit unions. Examiners should understand the risks and concerns present when a credit union uses a third-party processor and should determine that the credit union has current, detailed agreements in place that fix responsibility and accountability between the parties. Third-party risks are as follows:

- Allowing a corporate member to send files directly to the ACH operator. A credit union, acting as an ODFI, that allows a corporate member (originator) direct access to its ACH operator exposes itself to credit, fraud, and operational risk. The credit union warrants the validity of the transactions sight unseen and bears ultimate responsibility for the transactions. If the corporation fails or transmits fraudulent or erroneous entries, the credit union bears responsibility for the corporation's actions.

- Using a correspondent DFI for processing and/or settlement. A correspondent bank or corporate credit union provides processing and/or settlement services to the credit union acting as an ODFI. This situation exposes the credit union to credit, operational, and fraud risk because the correspondent could make a mistake or fail to process or settle its transactions.

- Using a correspondent DFI or data processing organization for ACH processing only (not settlement.) A credit union acting as an ODFI is exposed only to the risk that the third party will make a mistake or error. In this situation, the credit union faces only fraud and operational risk with respect to the third-party processor.

ACH Risk Management Handbook and Self-Audit Survival Guide

NACHA publishes a comprehensive guide called the *ACH Risk Management Handbook*, which further details the ACH risk issues and control procedures discussed in this appendix. Additionally, NACHA publishes a self-audit survival guide for financial institutions that anticipate conducting or have conducted audits of its compliance with the ACH operating rules. These required annual audits assist the credit union in assessing its risk regarding its wire transfer activities and compliance responsibilities. The examiner should ask the credit union if it has completed this audit and if it has obtained the results of each third-party processor's annual ACH self-audit. The credit union can obtain both publications by writing or calling NACHA at National Automated Clearing House Association, 607 Herndon Parkway, Suite 200, Herndon, Virginia 22070, telephone: (703) 742-9190.

ITEM PROCESSING - APPENDIX 9C

Overview

Item processing is the internal processing of share drafts or checks by the credit union. The three basic types of item processing are in-clearings, transit items, and inter-clearing arrangements, defined below. Item processing results in settlement (payment or collection) through the Federal Reserve Bank (FRB) or a correspondent bank and posting of transactions to the member's account. Many larger credit unions are developing in-house item processing to reduce the costs of external check processing. Services are also available in corporate credit unions, credit union service organizations (CUSOs), banks, and national or regional check-processing service centers.

Third-Party Item Processing

Many third-party institutions have a contractual arrangement with the credit union whereby the credit union pre-funds processing activities by placing and maintaining a deposit at the institution. The required deposit relates to the credit union's average daily processing activity and, though it varies from institution to institution, may represent a substantial portion of the credit union's assets. When the deposit exceeds the insured limit (if applicable), the credit union is at risk for this excess in the event that the third-party institution fails.

Credit unions using third-party institutions for item processing must institute policies and procedures to minimize the potential risk of loss. Additionally, credit unions must exercise due diligence, both before entering into a contract with a third-party institution and periodically thereafter. At a minimum, credit unions should:

- Contact several processors. By reviewing the financial statements, the most recent audit report, and other pertinent reports or correspondence, the credit union can assess the financial condition of each institution before entering into a contract.

- Review contract terms and conditions. The credit union and its legal counsel should carefully review the terms and conditions of each institution's contract.

- Assess periodically the financial condition of the institution. On an ongoing basis, credit unions should review the institution's financial statements, peer group ratios and rankings, and audit reports at least annually, paying particular attention to capital and profitability ratios.

- Change processors, if necessary. If the financial stability of the institution becomes questionable, the credit union should consider changing to another institution. The credit union must consider issues such as the cost of changing processors and the terms of the contract. Credit unions can considerably reduce the cost of changing processors if they use their own routing and transit number on share drafts (payable-at method) rather than using the routing and transit number of the payable-through bank (payable-through method.) Credit unions using their own routing and transit number need not reissue new share drafts if they change processors. Before selecting the payable-at method, officials should discuss this option with individual processors. The terms, conditions, and level of credit union responsibility for a routing and transit program vary from processor to processor.

Share Draft In-Clearings

Some credit unions process their own checks. After a member writes a share draft to pay a bill, the merchant or vendor deposits the share draft in the local bank. The bank encodes (with the bank's routing and transit number on the drafts) the deposit and sends the share draft to the FRB. The FRB processes the draft, credits the local bank's account, and charges the credit union's account. The FRB then sends the share drafts to the credit union by courier.

The credit union sorts and microfilms the drafts and posts the in-clearings to the members' draft accounts. The next morning, a share draft exception report identifies accounts with insufficient funds. The credit union pulls returns and sends them to the FRB for return to the local bank. The bank charges the vendor's account.

Deposit Processing

Some credit unions process in-house check deposits for credit to members' accounts. The credit union takes the day's deposits, encodes the checks with the credit union's routing and transit number,

processes them, and sends them to the FRB for credit to the credit union's account.

Local Clearing House Arrangements

A group of banks or other financial institutions in a defined geographical area may form a local clearing association to directly process their checks.

A member writes a share draft and the payee deposits it at the local bank. After processing, the local bank sends the checks and a cash letter by courier directly to the credit union. The credit union processes the checks, confirms the payment amounts on the cash letter, and posts the amounts to the members' share draft accounts. The credit union then pays the local bank (usually by FEDLINE wire).

The credit union then sorts the members' local checks deposited at the credit union according to bank, and sends each participating bank a cash letter and a bundle of checks issued by that bank with a demand for payment. The bank processes the checks and wires settlement to the credit union.

Examination Concerns

Item processing involves substantial risk. Deficiencies in the internal controls, such as failure to process items promptly or correctly, could result in significant losses.

When examining credit unions involved in item processing, the examiner should (1) evaluate management control of operations, (2) determine the risks to the credit union, and (3) ensure that the credit union has instituted policies and procedures to minimize the potential risk of loss. Individual item processing operations will vary; however, all operations require necessary management and internal controls.

The examiner should develop an understanding of the credit union's item processing operation. At a minimum, the examiner should review policies and procedures and understand the flow of items through the entire system. This understanding comes through discussions with management and system demonstrations. The examiner should also determine that the credit union accurately and promptly posts all

general ledger accounts used in the process and promptly clears exceptions.

If deficiencies exist, the examiner should expand the scope of the review (after obtaining the supervisory examiner's concurrence), which may require additional examiner staff with item processing expertise.

Business Plan, Budget, Cost Analysis, and Profitability

Before establishing an item processing operation, credit union management must develop a business plan, including a budget that identifies the item processing services offered, and the resources needed to support the service. After developing and analyzing the business plan, the credit union may find that it cannot afford to maintain an item processing operation. The business plan requires periodic revision once the item processing department is operational. The business plan should document:

- The costs and revenue projections associated with an item processing department and the accounting system used;
- The overall effect of the processing operation on the credit union's financial performance;
- Identified risks and internal controls necessary to manage those risks;
- Department structure including staffing and management needs;
- System configurations including hardware and software needs;
- Training, both initial and on-going, for management and staff; and
- Disaster recovery, including testing.

Equipment and Software Requirements

An item processing operation requires a significant investment in hardware and software. A sorter performs sorting, microfilming or imaging, return pulling, data accumulation, and data transmission functions.

A credit union that processes its own checks transmits applicable data to its own information processing system for posting to its members' accounts. A credit union that processes for other credit unions establishes systems to electronically transmit the data to the other credit unions' computer systems for posting.

Other equipment needed includes reject/reentry stations, encoding stations, correspondence desks (positions for resolving and researching differences), check storage areas onsite and offsite, microfilming duplicating services, microfilm machines, and computer terminals.

The credit union must maintain adequate physical access controls and segregation for the item processing equipment, computer controller, storage areas, and different work areas. Climatic controls, fire control equipment, and security controls are examples of other hardware needed.

Staffing Requirements

An item processing operation requires staff with specific experience and training in item processing. Often credit unions recruit staff from the larger banks, corporate credit unions, and service centers. Sufficient internal controls, adequate separation of duties, and corresponding authority on the computer are important for operations of all sizes.

Microfilming and Data Backup

Item processing operations rely heavily on microfilm or electronic imaging. Cash letter differences, other adjustments, and disputes (from members, banks, or FRB) require the evidence that microfilming or imaging provides. The credit union must have controls in place to safeguard the microfilm or image files and ensure readability. The credit union must backup processing data from the sorter and controller daily and must maintain adequate generations both onsite and offsite. (Credit unions must maintain at least two full copies of the microfilm or image files offsite.)

Policies and Procedures

Sound policies control item processing risks, operations, and management. Management must review operations to ensure compliance with policy.

Management must also develop detailed procedures for all item processing positions. These procedures should document required functions, deadlines, internal control steps, and policy requirements.

The board should establish a write-off policy. Management can authorize staff to write off small differences (e.g., those under $1.) Larger write offs should require documentation supporting the write off and management authorization.

Internal Control and Review of Operations

Management must establish internal controls for item processing that include adequate separation of duties, active account reconciliation, and prompt clearing of differences.

The following duties must be separated: reject reentry, return processing, correspondent services (research and clearing of adjustments and differences), Federal Reserve account reconcilements, cash balance management, and review of documentation supporting reconciliation and clearing differences. Cash letter totals must reconcile to transmission totals, and staff must identify and promptly clear any differences.

An independent staff member should review documentation for adjustments of uncleared items. Management should closely control and separate return processing and reject reentry functions from the check processing function. Additionally, staff must reconcile both transmission totals (electronic posting to member accounts) and reconcilement of processing and transmission totals to the FRB account daily.

The item processing operation could involve three computer systems: (1) check processor, (2) general ledger and share and loan trial balance system, and (3) the computer that interfaces the check processor with the general ledger and share and loan trial balance system. The internal control plan must correspond to the plan for appropriate segregation of duties.

Internal Control Review of Accounting

The review of accounting should begin after the examiner obtains a basic understanding of how the system processes, posts, and settles transactions. After performing a test of the FRB account reconciliation and all clearing and suspense accounts, the examiner should then trace all reconciling items for the period tested through to clearing on the statement or to independent source documents.

Legal Agreements

The examiner should review the legal agreements established by the credit union in the following areas:

- Line-of-credit agreements for credit unions that process checks and deposits for other credit unions, transmit posting data to other credit unions, and receive debits or credits at their FRB (or correspondent bank) on their routing and transit number. Settlement lines of credit cover check clearing settlement if the other credit union's account balance is insufficient to cover clearings;
- A disaster recovery plan that includes agreements for alternate site processing and equipment use;
- Vendor agreements outlining responsibility for software and hardware maintenance and support;
- Agreements with the FRB (or other correspondent bank) and hardware and communication vendors for funds settlement and electronic transmission activity; and
- Any other material agreements needed to support the item processing operation.

Disaster Recovery Plan

The examiner should review management's disaster recovery plan to ensure that it enables the credit union to recover from difficulties that could interrupt the item processing operation. Recovery systems should include:

- Staff knowledge about the disaster recovery plan;
- An alternate processing location;
- Offsite maintenance of a copy of the disaster recovery plan;
- Duplicate equipment, either purchased or rented, sufficient to operate the item processing center; and
- A regular review process of the disaster recovery plan to ensure the plan is current and viable.

The credit union should perform full periodic testing of the disaster recovery plan as it relates to the item processing operation originating from alternate site equipment and different system configurations.