Chapter 306

AUTOMATED CLEARING HOUSE

Introduction

The Automated Clearing House (ACH) is a network for electronically exchanging funds and related information among individuals, businesses, financial institutions, and government entities. ACH rules and regulations are established by the National Automated Clearing House Association (NACHA). Private ACH operators and other local and regional ACH associations provide input into the rules. Federal government ACH transactions fall under the government's "Green Book" ACH Rules.

The ACH Network

The Federal Reserve is the principal ACH operator, distributing ACH transactions through Fedline. There are also over 20 private sector operators, such as EastPay, Inc., Mid-America Payment Exchange, Visa U.S.A., Payment Resources One, and Western Payments Alliance. All participants in the network fall into one or more of these six categories:

1. Originator - The Originator is the entity that agrees to initiate ACH entries into the payment system according to an arrangement with a Receiver. The Originator is usually a company directing a transfer of funds to or from a consumer's or another company's account. In the case of a consumer-initiated entry; however, the Originator may be an individual initiating funds transfer activity to or from his or her own account.
2. Originating Depository Financial Institution (ODFI) – An institution that receives the payment instruction from the Originator and forwards the entry to the ACH operator. A DFI may participate in the ACH Network as a RDFI (see below) without being an ODFI; however, if a DFI chooses to originate ACH entries, it must also agree to act as an RDFI.
3. ACH Operator - A central processing facility operated by the Federal Reserve Bank or other private sector organization. The operator receives electronic entries from ODFI's and distributes entries to the appropriate RDFIs (see below), and performs the settlement functions for the affected financial institutions.

4. Receiving Depository Financial Institution (RDFI) - A financial institution, which receives ACH entries from the ACH Operator and posts to the receiver (depositor) account.
5. Receiver - A natural person or organization, which has authorized an Originator to initiate an ACH entry to the Receiver's account with the RDFI.
6. Third Party Processor - A third party processor may serve as an agent for an ODFI or RDFI. The ODFI and RDFI are still responsible for compliance with ACH rules and regulations.

ACH System Operations

The ACH system supports both credit and debit transactions. In credit transactions, funds flow from the Originator's account through the ODFI to an account held by the receiver at the RDFI. For ACH debit transactions, the funds flow from the receiver's account at the RDFI through the ODFI to the account of the Originator.

Examples of ACH Credits	**Examples of ACH Debits**
• Payroll direct deposits	• Insurance premium collections
• Social Security payments	• Mortgage and loan payments
• Dividend and interest payments	• Consumer bill paying
• Corporate bill payments to contractors and vendors	• Corporate cash concentration transactions

ACH data transmissions always flow in the same direction - from Originator to the ODFI to the ACH operator to the RDFI. This is true whether the item is a debit or a credit. For credits, the ODFI's settlement account is debited and the RDFI's settlement account is credited. For debits, the ODFI's settlement account is credited and the RDFI's settlement account is debited.

The following are the steps for ACH origination:

1. The Originator (individual or business account holder) initiates a 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 entry is transmitted to the RDFI; and
5. The RDFI receives, processes, and posts the ACH data to the receiver account on settlement day.

ACH return items flow from the RDFI to the ACH Operator to the ODFI. The ODFI must notify the Originator of return items.

Third party processors may become involved at any step in the process. They may prepare files and send them to the ACH Operator on behalf of ODFI or they receive them on behalf of the RDFI. Regardless of the role third party processors play, the responsibility for rules adherence and liability falls on the appropriate financial institution using the third party processor.

ACH 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 initiates entries into the system, authorizes either a debit or credit, which affects either a consumer or a business account at the RDFI. Listed below are SEC codes and the different products each code supports. This list is not all-inclusive since new codes are always being developed and used.

Consumer Applications

1. Pre-arranged Payment and Deposit Entries (PPD) include both Direct Deposits and Direct Payments, as follows:

    a) Direct Deposit is a credit application that transfers funds into a consumer's account at the RDFI. These funds represent a variety of products (e.g., payroll, interest, and pension.); and
    b) Direct Payment (Pre-authorized 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 pre-established or single entry written authorizations, the consumer grants the company authority to initiate periodic charges to their account. Examples of recurring bills paid by ACH include insurance premiums, mortgage payments, and installment loan payments. An example of a non-recurring bill (i.e., the amount varies) paid by ACH is utility payments.

2. Point of Sales Entries and Shared Network Transactions (POS and SHR) are two SEC codes, which are most often initiated by the consumer via a plastic access card. They represent point of sale debit applications in either a shared or non-shared environment;
3. Machine Transfer Entries. The Network supports the clearing of transactions from Automated Teller Machines (ATMs); and

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

Corporate Applications

1. Cash Concentration or Disbursement (CCD) can be either a credit or a debit transaction where funds are either disbursed or collected between corporate entities. This application can serve as a stand-alone funds transfer or it can support a limited amount of payment-related data with the funds transfer.
2. Corporate Trade Exchanges (CTX) support the transfer of funds (debit or credit) within a trading partner relationship in which a full (ANSI ASC X12) message or payment-related (UN/EDIFACT) information is sent with the funds transfer. Upon receiver request, the ODFI must provide all payment related information in the addenda records transmitted with CCD and CTX entries. The information must be provided by the opening of business
   on the second banking day following the settlement date of the entry.

Other Applications

1. Automated Accounting Advice is an optional service provided by ACH operators that identifies automated accounting advices of ACH accounting information in a machine-readable format. This facilitates the automation of accounting information for participating depository financial institutions (DFIs).
2. Automated Notification of Change (NOC) or Refused Notification of Change (COR) is used by an RDFI or ODFI when originating a notification of change or refused notification of change in an automated format.
3. Death Notification Entries (DNE) is used by agencies of the federal government to notify a DFI that the recipient of government benefits has died.
4. Return Entries (RET) are used by ODFI's that convert paper returns to an automated format. They may also be used by ODFIs that are originating dishonored returns, when the return that is being dishonored carries the SEC RET. Upon request of the receiver, the ODFI must provide all payment related information contained in the addenda records transmitted as CIE entries. Information must be provided by the opening of business on the second banking day following the settlement date of the entry.

5. Truncated Entries (TRC/TRX) is used to identify batches of truncated checks. TRC is used for individual items and TRX is used for batches.
6. Destroyed Check Entries (XCK) can be used by an institution for collecting certain checks that have been destroyed.
7. Represented Check Entries (RCK). A standard entry class code RCK is used for collection of re-presented checks through the ACH network.
8. Cross-border payments to Canada are permitted using SEC codes CBR and PBR.
9. Consumer checks converted to an ACH transaction with the conversion completed at the point of purchase identified by standard entry class code POP.
10. Consumer authorization of non-recurring ACH debits can be initiated by telephone or by the Internet using the SEC codes TEL and WEB.
11. ACH debits and credits may be made directly to a financial institution's general ledger accounts for institutions whose ACH systems are interfaced with its loan accounts, including ACH credits posted directly to loan accounts.

Applicable Regulations

ACH Rules

NACHA ACH Rules are published annually and incorporate rules approved by the NACHA board. The NACHA is a self-regulated body, which depends on users' compliance with ACH rules for the system to operate efficiently. The rules provide warranties and indemnification requiring entries to be originated, received, and returned promptly.

ODFIs are responsible for most of the warranties and indemnifications; however, many responsibilities pass through the ODFI to the Originator. The warranties and indemnifications reside mostly with the ODFIs and Originators because they have primary control over the initiation of entries. The passing through of responsibility to the Originator relies heavily if not exclusively on the agreements between the ODFI and the Originator.

Responsibilities of ODFI's include:

1. Ensuring entries are properly authorized;
2. Submitting timely entry of transactions into the ACH system;
3. Terminating the origination of entries, when appropriate;

4. Meeting requirements for data security and personal identification numbers in certain applications;
5. Ensuring the entries contain the appropriate information;
6. Assuring an agreement is in place with Originators and sending points; and
7. Complying with 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 breach of warranty. Thus, a failure to comply with the warranties may result in a loss to an ODFI. 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. RDFI also warrants it is in compliance with the rules concerning RDFIs and participating DFIs.

Responsibilities of RDFIs:

1. Receiving and validating all ACH entries;
2. Posting to receiver's accounts;
3. Validating pre-notifications;
4. Returning entries which do not post within proper time frames;
5. Handling remittance data as required by the receiver;
6. Making funds available to the receiver within proper time frames; and
7. Fulfilling responsibilities when a receiving point is used.

Electronic Funds Transfer Act (EFTA)

The EFTA provides for rights and duties of consumers and financial institutions regarding electronic funds transfers. EFTA covers both private sector and government-initiated transfers.

Regulation E

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

Uniform Commercial Code Form UCC-4A (UCC4A)

UCC4A was developed in part for funds transfers, but also applies to wholesale (institution-to-institution) ACH credit transactions and certain ACH credit transactions not subject to the EFTA.

Green Book

The Green Book is published by the Financial Management Services agency of the Treasury Department. It specifies procedures for ACH transactions, which are originated for the Federal Government.

ACH Risk Assessment

The risks associated with processing ACH payments vary based on whether the item is an ACH debit or credit, and whether the item is received or originated. ACH risks are similar to those within the funds transfer and check payment systems. Although ACH transactions are generally for small dollar amounts, participating financial institutions may be exposed to credit risk for the entire ACH transmission file, not just individual entries in the file.

Corporates must understand payment processing risks (i.e., credit/exposure, operational, fraud, systemic, and third party processing) and have detailed written policies and procedures in place to control them.

Credit (Exposure) Risk - ACH Credits

The risk that a party to a transaction will not have sufficient funds for settlement is called credit (exposure) risk. Credit risk is also defined as “temporal” (time) risk. There is credit risk to both the ODFIs and RDFIs.

For ODFIs, this risk is associated with sending credit files to the ACH before funds are obtained from the Originator. This may occur when a member that is a party to the transaction fails or goes bankrupt before settlement. NACHA rules require credit limits be set, monitored, and reviewed by the ODFI for each Originator of credit entries. Due to the system’s settlement delay, credit limits must also be monitored across multiple settlement days.

If a corporate acts as an ODFI, it must assign credit ratings and exposure limits to each of its Originators. Exposure limits must be monitored. An alternative would be requiring the members’ accounts be pre-funded and/or collateralized. However, ACH rules do not

require pre-funding or collateralization, and corporates that require this could put themselves at a competitive disadvantage.

For RDFIs, credit risk is minimal. The ODFI warrants its ACH credit transmissions and is liable for them. The RDFI is not at risk unless the ODFI fails, which would cause the Fed to reverse the transaction. Even a failed ACH Originator still leaves the ODFI liable for any ACH transmissions sent.

For ACH debits the RDFI has no credit risk. The ODFI has some credit risk if funds are made available to the Originator. Returns, stop payments, and NSF accounts may come back, in some cases, up to 60 days after the original settlement date. The ODFI might be required to return the funds to the receiver of the ACH debit. This risk is generally managed by requiring the Originator to maintain a reserve for returns at the ODFI, based on industry standards for returns of like debits, or based on experience with that customer. Immediate funds availability is given only for amounts in excess of the reserve. The amount of the reserve varies depending on the application. For instance, the collection of mortgage payments would likely have a much lower return rate than something like magazine subscription payments.

Operational Risk

Operational risk, which varies with the type of processing, is the danger an unintentional error will alter or delay a transaction. Corporates must limit operational risk by implementing appropriate management controls. The following are examples of operational risks and the controls corporates should have in place.

Hardware failure - The risk of hardware failure is reduced by purchasing reliable equipment, observing regular maintenance, hiring and/or contracting for responsive service personnel, and ensuring adequate backup exists.

Software failure - Operational problems caused by software failure are reduced by carefully testing the vendor's or service provider's software before relying on it for live processing. Corporates 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).
Security breaches and data loss - This risk can be managed by the use of security policies which require passwords, IDs, dual controls, and

random changes in personnel and duties. Specific examples are discussed as follows:

1. Protect electronic files against unauthorized changes by using file security procedures and maintaining all hard copy records in locked storage;
2. Limit data access to authorized personnel;
3. Duplicate, back up, and store data off-site to protect against data loss or destruction;
4. Establish and maintain audit trails of all transactions and changes;
5. Account for all files to ensure staff only processes current files and does not inadvertently duplicate or omit files; and
6. Balance file totals during processing to ensure transactions are not dropped, changed, or duplicated.

Telecommunications failures can be avoided by implementing the following:

1. Maintaining equipment (lines, modems, authentication or encryption devices, etc.) in working order;
2. Physically protecting the equipment; and
3. Developing diagnostic tools and backup transmission modes in the event of a problem.

Power failure can be avoided by obtaining an uninterruptible power supply system (UPS). A UPS removes spikes and transients from public power, and provides auxiliary power during a blackout. Management should arrange for a generator to handle longer-term power failures, if cost effective.

Human error can be managed by following documented procedures for operating systems, security controls, and by providing adequate training for personnel. Management can further reduce the risk of human error through:

1. Proper oversight and supervision;
2. Ensuring detailed operating procedures are in place;
3. Providing for periodic internal and external audits;
4. Monitoring file and dollar controls; and
5. Ensuring an adequate audit trail exists.

Staffing problems are manifested by absences, turnover, work stoppages, etc. Staffing problems are reduced by emphasizing cross training and good supervision. Staffing problems in small corporates often result from only one or two people knowing the process.

Conversely, in very large corporates each activity may be so specialized that very few people know the overall process.

Natural disasters are largely out of the control of management. The corporate must develop and test disaster recovery plans utilizing alternative sites and operations.

Fraud risk is increased if an employee or interloper has the opportunity to gain unauthorized access to the system and initiate or alter a payment transaction in an attempt to misdirect or misappropriate funds. Fraud risk is reduced by the following:

1. Written personnel policies and practices should require, at a minimum, that:

    a. Vacancies in the unit be filled by internal transfers versus new employees, when possible;
    b. Relatives be restricted from working in the accounting or data processing departments;
    c. Individual responsibilities relating to security are in writing;
    d. Written organizational security procedures exist;
    e. Actions to be taken in the event of a security related incident be identified;
    f. Formal training programs be developed to emphasize security and control;
    g. Cross training exists within the unit;
    h. Rotation of responsibilities be unannounced;
    i. There be a minimum number of consecutive days of annual vacation;
    j. Reassignment out of the unit be made when a notice of resignation is given; and
    k. Terminated employees' sign-on ability is promptly cancelled.

2. Management also must implement adequate physical security controls, including the following:

    a. Limit access to computer and communications equipment to authorized personnel;
    b. Protect sensitive equipment within the secured area using access controls or device locks; and
    c. Secure and limit access to all data on portable media (tapes, disks, hard copies, microfiche, etc.)

3. Management should implement the following to minimize risk of data loss and/or destruction:

a. Purchase commercially available software products to access production data files;
b. Limit access to specified programs or user ID's by setting up each file for read-only or read-and-write access; and
c. Employing encryption, authentication, and dial back data protection techniques when accessing data-in-transit from one participant to another.

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

4. Management must maintain detailed written policies for software and data change controls. The policies should, at a minimum:

    a. Permit only authorized software and data changes;
    b. Document, review, and approve all changes before coding is done;
    c. Test changes from the developers by a different group;
    d. Install changes utilizing a group other than the developers and testers;
    e. Maintain prior versions of changed programs to reverse changes, if necessary;
    f. Change emergency programs and data only with appropriate management approval; and
    g. Complete audit trails of all the changes, including a record of who requested the change, and the before and after versions.

5. Management must restrict access on software products using:

    a. Operator passwords to prohibit entry by unauthorized personnel;
    b. Automatic features to control the number of unsuccessful password attempts, password expiration, or designated periods of inactivity;
    c. Multi-level functions, by password, to require dual control and ensure 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
    d. System administration level procedures to require secondary approval to assign, initiate, and maintain passwords.

6. Management must set dollar and file exposure controls. These limits are to be used and enforced at the time of entry, batch or file creation, and at the time of transmission. Exposure limits must be established across multiple settlement days to account for the potential of overlapping settlements. NACHA rules require a file limit, a daily aggregate file limit, and a three-day aggregate file limit be established. This is because the first day's transmission does not settle until day two or three, exposing the ODFI to credit risk for the aggregate of all unsettled transmissions over several days.

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

    a. File controls to ensure 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.

    b. Dollar controls to:
        1. Confirm dollar totals at each step in ACH processing; and
        2. Help ensure ACH files are in balance, accounts are accurately posted, and settled as anticipated.

    c. Date controls (file creation date, effective entry date, and settlement date) to monitor that files are processed within the time frames established by the various regulations.

    d. Exception reporting to monitor:
        1. Circumstances such as over-limit activity;
        2. Anticipated files not received; and
        3. File inconsistencies suggesting errors, intrusions, or duplications.

    e. 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.

    f. Reconciliation of entries on the Federal Reserve Statement must be performed to verify the ACH work settled as anticipated. Proper segregation of duties dictates staff

responsible for reconciling ACH transaction not be otherwise involved in the ACH processing.

g. Internal audits of the ACH process: NACHA rules require each financial institution complete an audit of its ACH operations at lease once every year (a copy of which must be retained 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 exists when the inability of one ACH participant to settle its commitments causes other participants the inability to settle their commitments. The consequences could cause a ripple effect throughout the network.

Systemic risk is closely related to credit risk. While a fraudulent or erroneous transaction could be a source of systemic risk, it is far more likely a participant's failure would trigger a major settlement failure.

The likelihood of systemic risk varies greatly among payment systems. There is a connection 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.

The threat of systemic risk related to ACH transactions is very small. The average dollar value of an ACH transaction is significantly less than that of Fedline or Clearing House International Payments System. Rarely does a financial institution's position with respect to gross ACH settlement approach its capital level. It is far more likely a financial institution's position on the Fedwire network will exceed its capital.

Third-Party Risk

Third-party processors are data processing service bureaus, financial institutions, or other organizations that provide ACH processing services. Examiners must be aware of the risks and concerns present when a corporate uses a third-party processor and must determine the corporate has current, detailed agreements in place that fix responsibility and accountability between the parties. Third-party risks are as follows:

1. Allowing a member to send files directly to the ACH operator: A corporate, acting as an ODFI that allows a member direct access to its ACH operator exposes itself to credit, fraud, and operational risk. The corporate warrants the validity of the transactions sight unseen and is ultimately responsible for the transactions. If the member fails or transmits fraudulent or erroneous entries, the corporate is responsible for the member's actions;
2. Using a correspondent DFI for processing and/or settlement: A correspondent bank provides processing and/or settlement services to the corporate acting as an ODFI. This situation exposes the corporate to credit, operational, and fraud risk because the correspondent could make a mistake or fail to process or settle its transactions; and
3. Using a correspondent DFI or data processing organization for ACH processing only (not settlement): A corporate acting as an ODFI is exposed only to the risk the third party will make a mistake or error. In this situation, the corporate faces only fraud and operational risk with respect to the third party processor.

OFAC Compliance with ACH Transactions

The Office of Foreign Assets Control (OFAC) is part of the Department of the Treasury and administers and enforces economic sanctions against targeted foreign countries, terrorism sponsoring organizations, and international narcotics traffickers based on U.S. foreign policy and national security goals. Compliance with OFAC rules for ACH transactions resides with the Originators of the transaction. Third-party processors are not required to "unbatch" transactions to monitor OFAC rules. Corporates who do not originate but process for member credit unions should remind members they may not process ACH payments in violation of OFAC rules. The Originators could face penalties for processing blocked or rejected transactions. Corporates who do originate transactions must verify they are in compliance with OFAC rules on the transactions processed.

ACH Risk Management Handbook

NACHA publishes an ACH Risk Management Handbook, which is a comprehensive guide to the ACH risk issues and control procedures discussed above. Additionally, Western Payments Alliance (We spay) publishes a self-audit survival guide for financial institutions to conduct or have conducted audits of its compliance with the ACH operating rules. The examiner should ask the corporate if they have this information on file to ensure they are informed about the various risks and are performing the necessary compliance audits.

If the corporate does not have this information on file, they can obtain it by writing or calling NACHA at:

National Automated Clearing House Association
13665 Dulles Technology Drive, Suite 300
Herndon, Virginia 20171
(703) 561-1100

Legal Agreements

Detailed agreements must be in place between the corporate and all outside parties (e.g., credit unions, leagues.) using the ACH service which detail the exact services provided and the various liabilities of each party. Also, agreements must be on hand between the corporate and the Federal Reserve or a third party processor, if one is used.

Reference 2 contains a list of issues that should be included in an agreement between an Originator and an ODFI. ACH agreements should be reviewed to determine that each of the recommendations is included.

Examination Objectives

For ACH operations, the objective is to evaluate the adequacy of controls over the ACH environment by determining:

1. The types of ACH services the corporate provides;
2. The corporate's role in the ACH services offered (e.g., ODFI, RDFI, Receiver);
3. Appropriate written agreements are in place for all types of ACH services offered;
4. Adequate balancing procedures are in place for all transactions sent to and/or from the ACH operator;
5. Adequate procedures are in place to control intraday and overnight overdrafts due to ACH settlement;
6. Members originating large volumes of ACH credit transactions, have undergone adequate credit assessment evaluation;
7. The existence and adequacy of exception reports (e.g., large item, new account); and

8. Procedures are in place for retaining records of all ACH entries, returns, and adjustments for a period of six years after their transmittal.

Examination Procedures

See Corporate Examination Procedures - Automated Clearing House

Examination Questionnaire

See Corporate Examination Questionnaires - Automated Clearing House

References

1. FFIEC Information Systems Handbook, 1996 Edition;
2. NACHA Rulebook;
3. Uniform Commercial Code, Article 4A; and
4. ACH Risk Management Handbook.

Appendices

306A Examiner's Guide to APEX Security Settings