OCC 2002-2

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: ACH Transactions Involving the Internet
Description: Guidance and Examination Procedures

TO: Chief Executive Officers of All National Banks, Service Providers and Software Vendors, Department and Division Heads, and All Examining Personnel

PURPOSE

This bulletin highlights the risks associated with automated clearing house (ACH) transactions that involve the use of the Internet and provides guidance for managing those risks. The OCC considers compliance with this bulletin to be critical in ensuring safe and sound ACH activities. This bulletin incorporates and replaces OCC Advisory Letter 2001-3: Internet-Initiated ACH Debits/ACH Risks (January 29, 2001) regarding an amendment to the National Automated Clearing House Association (NACHA) Operating Rules (NACHA Rules).

SCOPE

This guidance applies to

- Banks acting as originating depository financial institutions (ODFIs) that offer ACH payment options to their originator customers that involve the use of the Internet.
- Banks acting as receiving depository financial institutions (RDFIs).
- Third-party service providers acting on behalf of ODFIs or RDFIs.

When assessing the risks of ACH transactions involving the Internet and the efficacy of a bank's risk management practices, examiners will use the attached examination procedures. Refer to appendix A for a discussion of the ACH Network and the roles and responsibilities of network participants.

TABLE OF CONTENTS

RISK ASSESSMENT

Banks that participate in the ACH Network, as well as their service providers, should have well-established risk management practices governing ACH activities. Management should review these practices to ensure that risk exposures from ACH transactions involving the Internet are identified and appropriately managed. The innate characteristics of the Internet warrant this review. In particular, the Internet creates an environment in which parties may not be certain with whom they are doing business. This poses unique opportunities for fraud. The Internet is also an open network, that requires special security procedures to prevent unauthorized access to consumer financial information. Finally, the sheer volume and speed with which payments can be transacted over the Internet must be taken into account.

The following is a discussion of the risks arising from ACH transactions involving the Internet and associated risk management practices.[1] Special considerations for banks that conduct ACH transactions involving the Internet through third-party service providers are separately discussed.

Strategic Risk

ACH transactions involving the Internet are a new service that banks can use to help achieve strategic goals. As with any new product or service, an adverse business decision regarding these transactions or the improper implementation of this service exposes the bank to risk. These transactions may also involve the use of new technologies or strategic alliances that pose risks that must be identified, monitored, and controlled. The ultimate success of this service depends on adequate planning, execution, and monitoring by the board of directors and management.

Reputation Risk

Under the NACHA Rules, ODFIs are deemed to make certain warranties regarding entries they initiate on behalf of their originator customers, including that the entries have been authorized by a receiver. In addition, certain consumer debit entries authorized via the Internet (WEB entries) involve additional specific warranties—the ODFI assumes liability for failure of its customers to assure a secure Internet environment and establish reasonable fraud controls (see appendix B). ODFIs should ensure that their agreements with originators take account of these warranties and liabilities.

Some banks use third-party service providers to conduct their ACH activities. Agreements between an ODFI or RDFI and a service provider should provide reasonable assurances that the service provider will be in compliance with the NACHA Rules. In addition, service provider support should be properly controlled to ensure timely and reliable service to customers. Addressing these issues can increase a bank's ability to meet customer expectations and reduce the risk of lawsuits and potential damage to public confidence and trust.

Transaction Risk

The unique characteristics of the Internet warrant specific security measures to control the risk of fraud and possible service disruption. Stronger logical and physical security controls regarding authentication, network management, and business continuity are needed to ensure proper execution of transactions and to control the risk of identity theft. Banks must use a commercially reasonable method to authenticate their customer.[2] In addition, compliance with the

[1] For a broader discussion of electronic banking risks and risk management issues, see "Risk Management Principles for Electronic Banking," Basel Committee on Banking Supervision (May 2001).

[2] *See* the Internet Banking booklet of the *Comptroller's Handbook* and OCC Advisory Letter 2001-8: Authentication in an Electronic Banking Environment (July 30, 2001). *See* also, the discussion on "commercially reasonable" in appendix B of this bulletin.

requirements set forth in the Interagency Guidelines for Establishing Standards for Safeguarding Customer Information[3] and in the OCC's supplementary guidance dealing with identity theft[4] is critical in the conduct of ACH activities involving the Internet.

ODFIs are liable under warranties in the NACHA Rules if their customer originators fail to comply with certain obligations imposed on them, including the originator's obligation to ensure the receiver has authorized a transaction. For WEB entries, these originator obligations include deploying commercially reasonable fraudulent transaction detection systems and routing number verification procedures, establishing a secure Internet session, and conducting an annual security audit. In light of their warranty exposures, ODFIs should have sound risk management practices and controls to ensure that originators comply with their obligations under the NACHA Rules. In addition, for transactions not defined as WEB entries but involving some use of the Internet, the ODFI's risk management approach should still consider the security of originators' Internet operations.

Credit Risk

For ACH credit entries, the ODFI incurs credit risk upon initiating the entries until its customer funds the account at settlement. Generally, this exposure is from one to two business days. The RDFI's credit risk with respect to such an entry arises if it grants funds availability to its customer prior to the time at which the settlement of the credit entry is final. For ACH debit entries, the ODFI incurs credit risk from the time it grants funds availability to the originator (usually on the settlement day) until the ACH debit can no longer be returned by the RDFI. Assuming the transaction has been properly authorized, returns generally must be made no later than the second banking day following settlement. An ODFI will normally charge back a returned ACH debit to the originator. However, the ODFI may suffer a loss if the originator's account has insufficient funds, has been closed, or is frozen because of bankruptcy or other legal action. The RDFI's credit risk with respect to a debit entry arises if it allows the debit to post, even if it overdraws its customer's account.

To manage their credit exposures, ODFIs (and their service providers) should monitor the creditworthiness of their customers and establish and periodically review ACH exposure limits for them. In addition, ODFIs should implement procedures to monitor ACH entries relative to the originator's exposure limit across multiple settlement dates. Separate exposure limits and monitoring should be established for WEB entries. RDFIs should establish prudent overdraft and funds availability policies and practices to mitigate their credit exposures.

Compliance Risk

When a bank fails to comply with the NACHA Rules, it exposes itself to contractual liability and possible fines under NACHA's national system of fines. Banks that transact ACH debits authorized by consumers via the Internet must ensure they are in compliance with NACHA's new requirements for WEB entries.[5] In addition, Regulation E applies to electronic financial services operations, including ACH transactions. The notice, authorization, and timing requirements of Regulation E are of particular importance. Noncompliance with Regulation E

[3] 66 FR 8616 (February 1, 2001). The OCC's standards are codified at 12 CFR 30, appendix B.

[4] OCC Advisory Letter 2001-4: Identity Theft and Pretext Calling (April 30, 2001).

[5] *See* appendix B, "NACHA Requirements for WEB Entries."

exposes a bank to liability in litigation and possible civil money penalties. Moreover, banks need to monitor their compliance with Office of Foreign Assets Control (OFAC) requirements concerning accounts of blocked parties.[6]

Liquidity Risk

Banks must understand the impact that certain risks associated with ACH transactions, such as credit or transaction risks, may have on their liquidity. For example, an ODFI may not be able to settle (collect) an ACH debit, or an RDFI may not be able to settle an ACH credit because of the default of an ACH Network participant, fraud, or service disruption. This could impair the bank's ability to meet its other obligations in a timely manner without incurring unacceptable losses. Banks should consider the volume of their uncollected ACH transactions as part of their liquidity risk management practices.

Third-Party Service Providers

While a bank's responsibilities do not change with the use of a third party for ACH processing, its risk exposure may increase as a result of third-party direct access to an ACH operator.[7] A third-party service provider may transmit ACH transactions directly to an ACH operator using the ODFI's routing number, provided it has obtained permission from the ODFI. However, it is the ODFI that warrants the validity of each entry transmitted by the service provider, including the basic requirement that each entry has been authorized by a receiver.

Although the ODFI is exposed to increased risk, allowing a third-party service provider direct access to an ACH operator is not necessarily an unsafe practice. To reduce risk to the bank and to protect all parties, the bank should establish procedures that will give it necessary controls over operations carried out by a third-party service provider. The ODFI must maintain absolute control over its own settlement accounts. Further, the ODFI must have an agreement with the third-party service provider that has direct access to an ACH operator setting out the rights and responsibilities of the parties. The agreement should include:

1) A requirement that the third-party service provider obtain the prior approval of the ODFI before originating ACH transactions for originators under the ODFI's routing number. The ODFI's approval of each originator should be contingent upon the creditworthiness of the originator and the execution of an originator/ODFI agreement;

2) The establishment by the ODFI of dollar limits for files that the third-party service provider deposits with the ACH operator. A file that would exceed the dollar limits should be brought to the ODFI's attention before the file is deposited at the ACH operator so that the ODFI can either approve it as an exception or ask that it be held until the next day; and

3) A provision that restricts the third-party service provider's ability to initiate corrections to files that have already been transmitted to the ACH operator. The ODFI should implement risk control measures with the ACH operator that limit such correction ability to itself. If the ability to make corrections to such files is provided to the third-party service provider, it should be given only under controlled circumstances that require the ODFI to authorize any changes to the file totals and require the ODFI to instruct the ACH operator to release the file for processing. This process should be a positive check-off process; *i.e.*, the ACH operator must receive the

[6] *See* the Bank Secrecy Act/Anti-Money Laundering booklet of the *Comptroller's Handbook* and OCC Alerts 2001-9, 2001-13, and 2001-14.

[7] For guidance on managing the risks associated with other types of third-party service providers, see OCC Bulletin 2001-47: Third-Party Relationships (November 1, 2001).

authorization in order to process a file, and the failure to receive the authorization will result in the file being deleted. In this way, the ODFI has control over its exposure from files originated by the third-party service provider.

In addition, it should be noted that the NACHA Rules require any third-party service provider that performs a function of ACH processing on behalf of an ODFI or RDFI to conduct an annual audit of compliance with the requirements of the NACHA Rules. The bank warrants completion of such audit by its service provider.

Questions concerning this bulletin should be directed to the OCC's Core Policy Division at (202) 874-5490 or Bank Information Technology Operations at (202) 874-4740.

Mark L. O'Dell Deputy Comptroller for Core Policy	Ralph E. Sharpe Deputy Comptroller for Technology

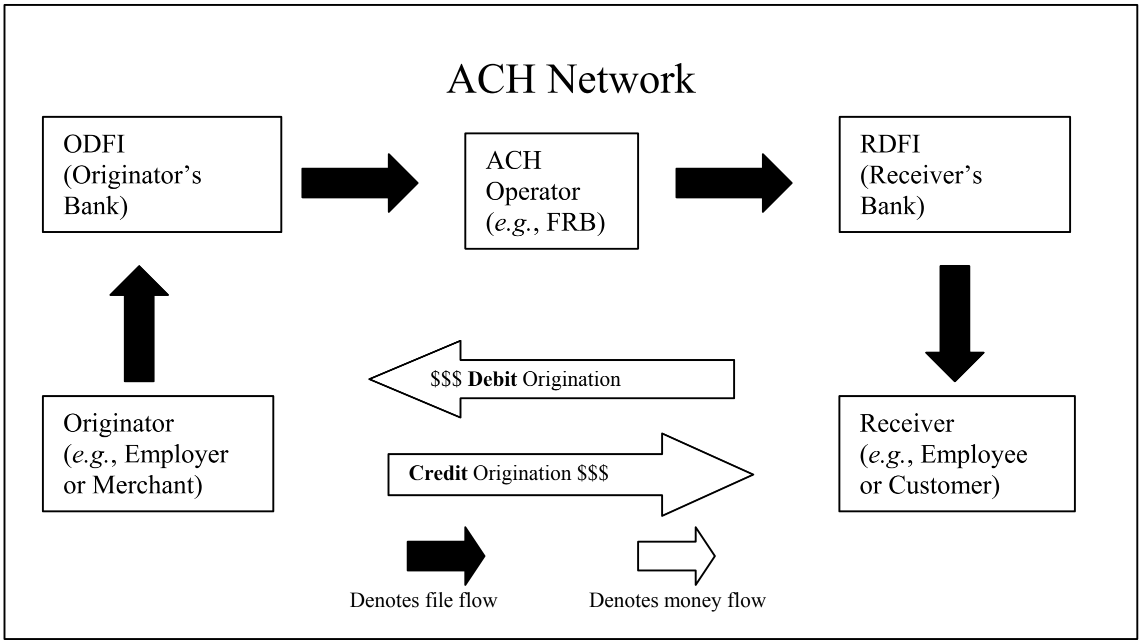
The ACH Network

The ACH Network is a nationwide, batch-oriented electronic transfer system that provides for the interbank clearing of payments among participating depository financial institutions. The ACH Network was developed in the early 1970s as a response to the massive growth of check payments.

NACHA was established in 1974 to coordinate the ACH Network. NACHA's primary roles are to develop and maintain the NACHA Operating Rules, to promote growth in ACH volume, and to provide educational services to its members and other ACH participants.

The process by which funds are transferred through the ACH Network operates from beginning to end through a series of legal agreements between the parties and pursuant to the NACHA Operating Rules. The rules are enforceable by the parties pursuant to the common law of contract. In addition, ACH entries are also subject to applicable federal and state law, such as the Electronic Fund Transfer Act (EFTA), implemented by Regulation E, and Article 4A of the Uniform Commercial Code, as enacted by a particular state.

For a given transaction, up to five entities may participate in the ACH Network—the originator, the originating depository financial institution (ODFI), the ACH operator, the receiving depository financial institution (RDFI), and the receiver. In addition, some of the entities may use a third-party service provider as part of the process.


ACH Network
ODFI (Originator's Bank)
ACH Operator (*e.g.*, FRB)
RDFI (Receiver's Bank)
$$$ **Debit** Origination
Credit Origination $$$
Originator (*e.g.*, Employer or Merchant)
Receiver (*e.g.*, Employee or Customer)
Denotes file flow
Denotes money flow

The *originator* is the party 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, but may be an individual initiating funds transfers to or from the individual's own account.

The *ODFI* is the institution that receives the payment instructions from its customers, the originators, and transmits the entries to the ACH operator. An ODFI can also initiate ACH entries for itself, in which case it is both ODFI and originator.

The *ACH operator* is the central clearing facility, operated by a Federal Reserve Bank or a private organization, that receives entries from ODFIs, distributes the entries to appropriate RDFIs, and performs the settlement functions for the affected institutions.

The *RDFI* is the institution that receives entries from the ACH operator and posts them to the accounts of its depositors, the receivers.

The *receiver* is the party that has authorized an originator to initiate an ACH entry to the receiver's account with the RDFI.

Unlike the wire transfer and check systems, the ACH Network is both a credit and a debit payment system. ACH credit transactions transfer funds *from the originator to the receiver*. For example, an originator may arrange to meet its payroll obligations by causing an ODFI to transmit ACH credit entries so that employees' salaries are credited to their accounts and the originator's account is debited in the total amount of the payroll. ACH debit transactions, on the other hand, transfer funds *from the receiver to the originator*. For example, a merchant originator may permit a customer to purchase goods or services through the Internet when the customer authorizes the merchant to initiate an ACH debit to the customer's account. Although credits and debits transfer funds in different directions, the entry information and the functional processing always flows in one direction, from the originator to the receiver.

NACHA Requirements for WEB Entries

Effective March 16, 2001, NACHA amended its rules to establish a new standard entry class (SEC) code—Internet-Initiated Entry (WEB)—to which a number of unique requirements apply. The WEB SEC code must be used to identify an ACH debit entry to a consumer account that a receiver authorizes through the Internet. This code applies to both recurring and single-entry ACH debits. ODFIs that transmit WEB entries are deemed by the rules to warrant that their originators initiating the entries have met certain standards. The goal of the amendment is to protect the security and integrity of the ACH Network and consumer financial information. The new requirements primarily affect ODFIs, their service providers, and their originators. The following highlights the key requirements of WEB entries for both originators and ODFIs.

- Originators of WEB entries must
  - Obtain consumer authorization prior to initiating a WEB entry (this requirement applies to all ACH debit entries). An authorization must provide evidence of the consumer's identity and assent to the authorization.
  - Employ commercially reasonable, fraudulent-transaction detection systems to screen the entries in order to minimize the risk of fraud related to Internet-initiated payments. The level of authentication used should reflect the risk of the transaction.
  - Use commercially reasonable procedures to verify that routing numbers are valid. Originators can use commercially available databases or directories, or other reasonable methods.
  - Establish a secure Internet session with each consumer using a commercially reasonable security technology that, at a minimum, is equivalent to 128-bit encryption. The secure session must be in place from the time consumers enter their banking information through the time of transmission to the originator. This requirement also applies to any transmission to a service provider.
  - Conduct an annual security audit to ensure that the financial information obtained from consumers is protected by security practices and procedures that include, at a minimum, adequate levels of (1) physical security to protect against theft, tampering, or damage; (2) personnel and access controls to protect against unauthorized access and use; and (3) network security to ensure secure capture, storage, and distribution of financial information. The first audit must be completed by December 31, 2001.
- ODFIs are required to
  - Identify the entries with the new WEB SEC code.
  - Warrant that each of its originators has: employed a commercially reasonable fraudulent transaction detection system; used commercially reasonable procedures to verify that routing numbers are valid; established a secure Internet session with each consumer; and

conducted an annual security audit. (As with all ACH debit entries, the ODFI also warrants that a WEB entry has been authorized by the consumer).

- Use a commercially reasonable method to establish the identity of the originator.[8]

- Establish procedures to monitor the creditworthiness of the originator on an ongoing basis. When a service provider has the direct relationship with the originator, the ODFI must ensure that its agreement with the service provider obligates the service provider with respect to creditworthiness and credit exposure management.[9]

- Establish a WEB entry exposure limit for the originator and implement procedures to review that exposure limit periodically.

- Implement procedures to monitor WEB entries initiated by the originator relative to its exposure limit across multiple settlement dates.

- Verify that its procedures ensure that originators are kept informed of and are in compliance with their new obligations on a continuing basis as part of the ODFI's existing rule compliance audit requirements.

KEY CONCEPTS

Commercially Reasonable

For all WEB entries, each originator must ensure that certain aspects of a transaction conform to a commercially reasonable standard. In addition, each ODFI warrants that the originator has handled those aspects of a transaction in a commercially reasonable manner. Those aspects of the transaction include commercially reasonable fraudulent-transaction detection systems, security technology to establish a secure Internet session, and procedures to verify the validity of the RDFI's routing number.

The concept of commercially reasonable means that an originator, given the facts of a specific transaction, acted in a way that other similar originators would have acted regarding systems, technologies, practices, and procedures. Whether an originator has fulfilled its obligations to perform in a commercially reasonable manner will be determined by an evaluation of the circumstances. The evaluation will include weighing the cost to the originator to employ a particular technology or procedure against the level of protection it affords to the originator and other ACH participants. What constitutes a commercially reasonable system, technology, practice or procedure may change over time. Originators, ODFIs, and their service providers should keep current with new technology and work together to meet their obligations.

[8] This requirement is consistent with the OCC's authentication requirements for banks engaged in electronic banking activities. See footnote 2 above.

[9] *See* the NACHA Operations Bulletin (June 2, 2000) discussing the risks involved with third-party direct access to the ACH Network, available at http://www.nacha.org/ACHNetwork/2000_bulletins_2.doc.

Single-Entry and Recurring Transactions

The WEB SEC code applies to both single-entry and recurring Internet-initiated payments. A single-entry payment means a one-time transfer of funds initiated by an originator in accordance with the receiver's authorization for a single ACH debit to the receiver's account (*e.g.*, to purchase a book online). A recurring payment is either (1) a payment that the receiver authorizes through the Internet to occur at regular intervals without any additional intervention of the consumer (*e.g.,* monthly mortgage payment), or (2) multiple payments (based on an authorization through the Internet establishing a relationship for a certain type of activity) that are initiated each time upon the specific instructions of the consumer *(e.g.*, periodic sale or purchase of stocks from a brokerage).

The rules provide that WEB entries must be coded to reflect whether they are single-entry or recurring payments. The distinction is important since there are different rules regarding returns and stop payments for each type of entry. This requirement will also permit ODFIs and RDFIs to track the entries and analyze whether certain entries pose more risk than others.

Authentication: The process of verifying the claimed identity of an individual user, machine, software component, or any other entity.

Authorization: A written agreement with the originator signed by an employee, customer, or member to allow payments processed through the ACH Network to be deposited in or withdrawn from his or her account at a financial institution.

Automated Clearing House (ACH) Network: A funds transfer system governed by the rules of NACHA that provides for the interbank clearing of electronic entries for participating financial institutions.

Automated Clearing House (ACH) Operator: A central clearing facility, operated by a Federal Reserve Bank or a private-sector organization on behalf of depository financial institutions (DFIs), through which participating DFIs transmit or receive ACH entries.

Consumer: Usually refers to an individual engaged in other than commercial transactions.

Consumer Account: A deposit account held by a participating DFI and established by a natural person primarily for personal, family, or household use and not for commercial purposes.

Credit Entry: An entry to the record of an account to represent the transfer or placement of funds into the account.

Debit Entry: An entry to the record of an account to represent the transfer or removal of funds from the account.

Encryption: A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

Exposure Limit: Referring to the settlement of operating services, the maximum amount an originator is allowed to originate. This amount is based on the originator's credit rating, historical or predicted funding requirements, and the type of obligation.

Internet: A worldwide network of computer networks.

National Automated Clearing House Association (NACHA): The national association that establishes the rules and procedures governing exchange of Automated Clearing House payments by DFIs.

Originating Depository Financial Institution (ODFI): A participating financial institution that originates entries at the request of and by agreement with its originators, in accordance with the provisions of the ACH rules.

Originator: A person that has authorized an ODFI to transmit a credit or debit entry to the deposit account of a receiver with an RDFI, or, if the receiver is also the RDFI, to such receiver.

Receiver: An individual, corporation, or other entity who has authorized a company or an originator to initiate a credit or debit entry to a transaction account held at an RDFI.

Receiving Depository Financial Institution (RDFI): Any financial institution qualified to receive debits or credits through its ACH operator in accordance with the ACH rules.

Regulation E: A regulation (12 CFR 205) promulgated by the Board of Governors of the Federal Reserve System to ensure consumers a minimum level of protection in disputes arising from electronic fund transfers.

Return: Any ACH entry that has been returned to the ODFI by the RDFI or by the ACH operator because it cannot be processed. The reason for each return is included with the return in the form of a "return reason code." (See the *NACHA Operating Rules and Guidelines* for a complete reason code listing.)

Routing Number: A nine-digit number (eight digits and a check number) that identifies a specific financial institution. Also referred to as the ABA Number.

Security: Procedures used to protect the authenticity and accuracy of ACH entries.

Settlement: A transfer of funds between two parties in cash, or on the books of a mutual depository (*e.g.,* a Federal Reserve Bank), to complete one or more prior transactions, made subject to final accounting. Currently, settlement for the automated clearing house system usually occurs through the Federal Reserve.

Settlement Date: The date on which an exchange of funds with respect to an entry is reflected on the books of the Federal Reserve Bank(s).

Single-Entry: A one-time transfer of funds initiated by an originator in accordance with the receiver's authorization for a single ACH credit or debit to the receiver's consumer account.

Standard Entry Class Code: A 3-character code within an ACH company/batch header record to identify the payment type within an ACH batch (*e.g.,* PPD, WEB, etc.)

Third-Party Service Provider: An entity other than an ODFI or RDFI that performs any functions on behalf of the ODFI or the RDFI related to ACH processing of entries, including but not limited to, the creation of ACH files or acting as a sending or receiving point on behalf of a participating DFI.

WEB Entry: A debit entry initiated by an originator pursuant to an authorization that is obtained from the receiver via the Internet to effect a transfer of funds from a consumer account of the receiver.

ACH Transactions Involving the Internet

Banks are exposed to diverse risks as a result of their participation in the ACH Network. Therefore, an integrated team approach, including safety and soundness examiners, as well as bank information technology, credit, and compliance specialists, is ideal for assessing the risks. Portfolio managers should identify banks that offer ACH transactions involving the Internet and discuss current and anticipated business volumes with bank management to determine if the supervisory strategies should be expanded to include reviews of these activities.

The objective of the examination is to determine the adequacy of the bank's policies, processes, personnel, and control systems to mitigate the risks of ACH transactions involving the Internet. The extent of testing and procedures performed should be based upon the examiner's assessment of risks and risk management practices. This assessment should include consideration of formal policies and procedures related to such transactions, including WEB entries, the results of the bank's compliance audit required under the NACHA Rules, and the bank's knowledge of its originator or receiver customers. In many cases, not all of the procedures will need to be performed.

Examination Planning

Set the scope for the examination. Consider the following:

- Comments regarding ACH/payment systems activities in previous examination reports
- Supervisory strategy
- Risk assessments
- EIC scope memorandum
- Follow-up activities
- Work papers from previous examinations
- Internal and external audit reports, including the DFI's NACHA rule compliance audit
- Related correspondence
- Volume of ACH transactions involving the Internet, including WEB entries
- Changes in ACH policies, processes, personnel, products, and services since the previous examination

Policies

Determine whether the bank has adopted adequate policies and procedures regarding ACH transactions involving the Internet, including WEB entries. Consider whether they

- Are in writing and are approved by the board or a designated committee.
- Adequately address ODFI or RDFI responsibilities.
- Establish management accountability.
- Include a process to monitor policy compliance.
- Include a mechanism for periodic reviews and updates.

Processes

1. Determine if the ODFI has adequate procedures to identify ACH transactions involving the Internet with the proper SEC code.

2. Determine if agreements between ODFIs and originators adequately address

   - Liabilities and warranties.
   - Responsibilities for processing arrangements.
   - Other originator obligations such as security and audit requirements.

3. Determine if the ODFI employs a commercially reasonable method to authenticate the originator. Consider whether

   - Documentation of the method is adequate.
   - The frequency of the review of the commercially reasonable standards is sufficient.

4. Determine if the ODFI conducts risk assessments of its originators and that they reflect a reasonable exercise of business judgment. Consider whether

   - The scope of risk assessments include
     - Receiver authorization.
     - Originator's Internet security, including
       - Commercially reasonable fraudulent transaction detection systems and routing number verification.
       - A secure Internet session.
       - Annual security audits.
   - The frequency of risk assessments is satisfactory.
   - Documentation and approval standards are acceptable.

5. Determine if the ODFI has established procedures to monitor the creditworthiness of its originator customers on an ongoing basis. Consider whether

   - Credit ratings are assigned to originators.
   - Monitoring is performed by competent credit personnel, independent of ACH operations.
   - Written agreements with originators require the submission of periodic financial information.

6. Determine if the ODFI has established ACH exposure limits for originators. Consider whether

   - The limit is based on the originator's credit rating and activity levels.
   - The limit is reasonable relative to the originator's overall exposure limit across all services (lending, cash management, foreign exchange, etc.).
   - Limits have been established for originators whose entries are transmitted to the ACH operator by a service provider.

- Written agreements with originators address exposure limits.
- A separate limit for WEB entries has been established.

7. Determine if the ODFI reviews exposure limits periodically. Consider whether

- Limits are adjusted for changes in an originator's credit rating and activity levels.
- Increases in an originator's ACH debit return volume trigger a re-evaluation of the exposure limit.
- Limits are reviewed in conjunction with the review of an originator's overall exposure limit across all services.

8. Determine if the ODFI has implemented procedures to monitor ACH entries initiated by an originator relative to its exposure limit across multiple settlement dates. Consider whether

- The monitoring system is automated and accumulates entries for a period at least as long as the average ACH debit return time.
- Entries in excess of the exposure limit receive prior approval from a credit officer.
- WEB entries are separately accumulated and monitored, yet integrated into the overall ACH transaction monitoring system.

9. Assess the RDFI's overdraft and funds availability policies and practices and determine if they adequately mitigate their credit exposures to ACH transactions.

10. Determine the ODFI's practices regarding originators' annual security audits of physical, logical, and network security. Consider whether

- The ODFI receives summaries or full audit reports from the originators.
- The audits are adequate in scope and performed by independent and qualified personnel.
- Corrective actions regarding exceptions are satisfactory.

11. Determine how the ODFI or RDFI manages its relationship with third-party service providers. Consider whether

- The service provider's financial information is obtained and satisfactorily analyzed.
- Service level agreements are established and monitored.
- Any audit conducted by the service provider, pursuant to the NACHA rule compliance audit requirement, is obtained and analyzed by the bank.

12. Determine if the ODFI allows third-party service providers direct access to an ACH operator. Consider whether agreements between the ODFI and the service providers include

- A requirement that the service provider obtain the prior approval of the ODFI before originating ACH transactions for originators under the ODFI's routing number.
- The establishment by the ODFI of dollar limits for files that the service provider deposits with the ACH operator.
- A provision that restricts the service provider's ability to initiate corrections to files that have already been transmitted to the ACH operator.

- Provisions regarding warranty and liability responsibilities.
- A provision regarding the NACHA rule compliance audit responsibilities of the parties.

13. Determine whether the RDFI has established procedures to deal with consumers' notifications with regard to unauthorized or improperly originated entries or entries for which authorization has been revoked.

14. Determine if the RDFI acts promptly on consumers' stop-payment orders.

15. Determine if the RDFI has procedures that enable it to freeze proceeds of ACH transactions in favor of blocked parties (under OFAC sanctions) for whom the RDFI holds an account.

16. Determine if the bank considers the volume of their uncollected ACH transactions as part of their liquidity risk management practices.

Personnel

Determine if management and personnel display adequate knowledge and technical skills in managing and performing duties related to ACH transactions.

Controls

Review results from the bank's NACHA rule compliance audit. Determine

- The independence and competence of the party performing the audit.
- Whether the board or its committee reviewed and approved the audit.
- Whether WEB entry responsibilities were included in the scope.
- Whether corrective actions are satisfactory regarding any audit exceptions.

Examination Conclusions

1. Discuss your findings with the examiner-in-charge, including relevant assessments of payment systems risks and risk management practices. Prepare summary comments and initiate necessary corrective action on deficiencies found.

2. Discuss your findings with bank management, including conclusions regarding applicable risks. If necessary, obtain commitments for corrective action.

3. Update the OCC's electronic information systems, as appropriate.

4. Organize and reference work papers in accordance with OCC policy.