OCC 2006-39

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject:	Automated Clearing House Activities	Description:	Risk Management Guidance

TO: Chief Executive Officers, Chief Risk Officers, and Compliance Officers of All National Banks, Federal Branches and Agencies, Technology Service Providers, Department and Division Heads, and All Examining Personnel

TABLE OF CONTENTS

PURPOSE

This bulletin provides guidance for national banks and examiners on managing the risks of automated clearing house (ACH) activity. National banks may be exposed to a variety of risks when originating, receiving, or processing ACH transactions, or outsourcing these activities to a third party. This bulletin outlines the key components of an effective ACH risk management program. Each bank should use this guidance to develop an ACH risk management program that reflects the nature and complexity of the bank's activities.

This bulletin supplements guidance on ACH activities contained in the *FFIEC IT Examination Handbook on Retail Payment Systems*[1], dated March 2004, and National Automated Clearinghouse Operating Rules[2] and replaces OCC Bulletin 2002-2 (ACH Transactions Involving the Internet).

[1] http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html
[2] See NACHA Operating Rules on the Internet at http://pubs.nacha.org/

SCOPE

This guidance applies to

- Banks acting as originating depository financial institutions (ODFIs),
- Banks acting as receiving depository financial institutions (RDFIs),
- Banks considering these activities, and
- Third-party service providers acting on behalf of an ODFI or RDFI.

BACKGROUND

Advances in technology have brought about significant changes in the nature and volume of ACH activity. The growth in ACH volume results from fundamental changes in payment methods used by consumers and businesses. Recently, the OCC has seen banks engage in new ACH activities without enhancing existing risk management systems and controls. Failure to implement appropriate controls for these activities is an unsafe and unsound practice and can result in increased credit, compliance, reputation, strategic, and transaction risks, and in some cases, deterioration in the bank's condition.

ACH origination volume has increased as consumers and businesses look for more cost-effective and convenient payment alternatives. The most pronounced growth in ACH transactions over the last several years has been for nonrecurring payments. Consumers may initiate such payments over the telephone, on the Internet, or simply by writing a check that is converted to an ACH transaction. Some common nonrecurring payment types include accounts receivable conversion (ARC)[3], point-of-purchase (POP), Internet-initiated (WEB), telephone-initiated (TEL), and re-presented check (RCK) entries.

In addition to new and evolving types of ACH transactions, there are new participants in the ACH network, including certain merchants and third parties known as third-party senders. Whereas a bank is a client of a traditional third-party service provider (often called an ACH vendor), the merchant is the customer of a third-party sender (often called an originator aggregator or merchant processor) and the third-party sender is a customer of the bank. When a third-party sender is interposed between the bank and the originator, there is no contractual agreement between the bank and originator. A bank should be aware of the distinct risks arising from relationships with third-party senders. Although third-party senders are bank customers, they require oversight by bank management. Guidance on managing third-party senders can be found in the *Third Party Senders* section of this document.

DISCUSSION

ACH Risk Management Program

Banks that participate in the ACH network, as well as their service providers, should have in place systems and controls to mitigate the risks associated with ACH activities. A strong risk management program begins with clearly defined objectives, a well-developed business strategy, and clear risk parameters. Both the board of directors and management are responsible for

[3] NACHA operating rules provide that originators must allow consumers to opt out of ARC check conversion and establish reasonable procedures under which consumers may notify originators that their checks are not to be converted.

ensuring that the ACH program does not expose the bank to excessive risk. The board's role is to establish the bank's overall business strategy and risk limits for the ACH program and to oversee management's implementation of the program. Bank management is responsible for establishing effective risk management systems and controls and regularly reporting to the board on the results of the ACH program.

The bank's ACH program should include an ongoing process that evaluates whether ACH activities are conducted within the risk parameters established by the board of directors. This process should also determine whether existing policies, procedures, and controls effectively address all aspects of the bank's ACH activities.

Risk Management Systems and Controls

The systems and controls needed for an effective ACH risk management program include written policies and procedures, strong internal controls, and a risk-based audit program. The depth and breadth of a bank's ACH policies and procedures will depend on the scope and complexity of the ACH activities. Adequate policies and procedures generally include the following basic components:

- A summary of the ACH program's objectives and its role within the bank's strategic plan;
- Board-approved risk tolerances that outline the types of activities the bank may conduct and the types of businesses approved for ACH transactions;
- Clearly defined duties and responsibilities that ensure strong internal controls over transactions;
- An ACH credit-risk management program; and
- An effective vendor management program, including a due diligence process for selecting third-party service providers, and an oversight process for monitoring them.

Reporting to the Board of Directors

To oversee management's execution of the ACH program effectively, the board of directors, or a committee thereof, should receive periodic reports that allow the board to determine whether ACH activities remain within board-established risk parameters and are achieving expected financial results. Such reports generally include:

- Metrics and trend analyses on ACH volume, returns, operational losses, and transaction types, with explanations for variances from prior reports;
- Metrics and trend analyses related to the composition of the bank's portfolio of originators and, as applicable, third-party senders;
- Capital adequacy relative to the volume of ACH activity and the level of risk associated with originators;
- The percentage of the deposit base that is linked to ACH origination activity;
- A summary of return rates by originator, and, as applicable, third-party senders[4];
- Unauthorized returns that exceed board-established thresholds;
- Notices of potential and actual rules violations and fines by NACHA;
- Financial reports on profitability of the ACH function as a cost center; and

[4] At a minimum, returns rates should be reviewed at the originator level for all originators.

- Risk management reports, including a comparison of actual performance to approved risk parameters.

Audit

The depth and breadth of a bank's ACH audit program will depend on the volume and complexity of its ACH operations. The OCC has seen several cases in which a bank's ACH audit program was not enhanced or strengthened to cover new or expanded products and services, including high-risk activities. Common deficiencies include inadequate audit coverage, inexperienced audit staff, and a lack of appropriate auditor training.

When establishing the ACH audit scope, auditors should consider issues such as growth in transaction volume, new products and services, new ACH systems, underwriting policies and customer due diligence (CDD) policies and practices, and customers' online access to the ACH network. Bank management should also ensure that periodic audits of third-party service providers and third-party senders are performed. The audit should also check for completion of the annual National Automated Clearing House Association (NACHA) Rules Compliance Audit (Rules Audit) by the bank or third-party service provider. The Rules Audit, however, is only one element of an effective ACH audit program and is not a substitute for a comprehensive, risk-based audit.

The audit function should be staffed appropriately with auditors who have sufficient expertise to evaluate all aspects of the ACH program. The board should ensure that there is sufficient expertise to carry out the bank's ACH audit activities, whether the function is performed by internal audit staff or an external audit firm. The board should also ensure that auditors attend training periodically to ensure that their skills keep pace with any expansion in the bank's ACH program.

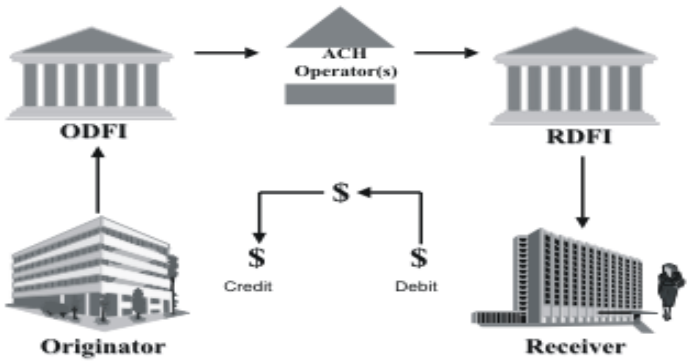
Credit Risk

Banks' credit-risk exposures have increased significantly with the expansion into higher-risk ACH activities such as nonrecurring payments. Credit risk occurs in different forms, depending on the type of transaction and the bank's role in the transaction. For ACH *credit* entries, the originating bank (ODFI) incurs credit risk upon initiating the entries until its customer funds the account at settlement. The receiving bank (RDFI) incurs credit risk if it grants its customer funds availability prior to settlement of the credit entry. For ACH *debit* entries, the ODFI incurs credit risk from the time it grants its customer funds availability until the ACH debit can no longer be returned by the RDFI.[5] The RDFI's credit risk from a debit entry arises if it allows the debit to post and overdraw its customer's account. *(See Figure 1.)*

Banks need to implement credit-risk controls that establish underwriting standards, require analysis of originators' creditworthiness, and set appropriate credit exposure limits. Banks with more complex ACH programs or banks that do not mitigate credit risk through holdbacks or reserve accounts will need to develop more expansive credit-risk management systems.

[5] ODFIs generally charge back a returned ACH debit to the originator. But the ODFI may suffer a loss if, for example, the originator's account has insufficient funds or has been closed.

Figure 1 – Depicts the funds flow for an ACH debit transaction[6]



Establishing Originator Underwriting Standards

As with other types of credit exposures, each bank's loan policies should include formal underwriting standards and an approval policy for ACH originators. During an initial review of originator information, banks typically reject originators that have a history of excessive unauthorized returns, or that do not operate a legitimate business. The depth of a bank's initial review should match the level of risk posed by the originator.

Underwriting standards enable bank management to clearly communicate the process and documentation required for approving new originators and expanding existing originators' ACH activities. Under the board's direction, bank management should implement underwriting standards for all originators. Such standards generally

- Define desirable, prohibited, and restricted originators[7];
- Require a background check of the originator to validate the legitimacy of the business (if necessary, this check can be supplemented with a background check on the principal business owners of the originator);
- Require evaluation of the originator's creditworthiness, including a comprehensive financial analysis (similar to that performed on other potential unsecured borrowers);
- Outline the type and timing of financial information to be provided by the originator;
- Require review of the originator's sales history;
- Summarize documentation requirements, including social security number or tax identification number;
- List permissible Standard Entry Class (SEC) types[8];
- Provide authorization procedures for approved originators;
- Provide guidelines for setting exposure limits, including requirements for pre-funding or collateral requirements;

[6] Copyright held by NACHA. Reprinted with the permission of NACHA. All rights reserved.
[7] Originators are generally classified based on their principal business activity, and in some cases their geographic location (e.g., some banks may choose to not act as the ODFI for originators located outside of the United States). For additional information on restricted merchants and risk management related to merchant underwriting, refer to the Merchant Processing booklet of the Comptroller's Handbook (2001).
http://www.occ.treas.gov/handbook/merchproc.pdf
[8] The SEC Code identifies the specific computer record format that will be used to carry the payment and payment-related information.

- Establish overlimit monitoring and approval;
- Outline originator account termination procedures; and
- Allow the bank to audit originators' ACH processes and controls at the bank's discretion.

Banks should use the underwriting standards listed above as guidance, to be adapted as necessary to reflect each bank's specific circumstances and individual risk profile. Banks engaged in complex or high-risk ACH transactions should implement more stringent underwriting standards than banks that only conduct traditional, lower-risk ACH transactions.

Risk Selection – Analyzing Originator Creditworthiness and Establishing Exposure Limits

Banks should perform ongoing credit analysis on ACH originators. Analyzing creditworthiness is a critical step in establishing and monitoring appropriate exposure thresholds for the type and volume of transactions processed by the bank. Banks should approach ACH credit analysis the same way they evaluate other credit arrangements by considering the proposed activity (such as purpose of the loan), and determining through financial and other analysis how much unsecured credit to extend. The bank should maintain a credit file on the originator that will include the types of ACH transactions that are authorized, the bank's financial analysis and evaluation of creditworthiness, and approved exposure limits for daily and multi-day settlements.

To manage credit risk effectively, banks should set ACH credit and debit exposure thresholds for originators and monitor the appropriateness of, and compliance with, such limits on a regular basis. Consistent with NACHA requirements, banks should establish separate exposure limits and monitoring practices for WEB entries. Banks should also implement procedures to monitor ACH entries relative to the exposure limit across multiple settlement dates. Banks need to be aware of the extended return time frames for consumer debit transactions.[9] Management should

- Set limits and obtain appropriate internal approvals before allowing ACH transactions to be initiated;
- Establish processes to ensure bank management remains abreast of originators' ongoing financial condition so management can take timely mitigating action, such as amending exposure limits or requiring pre-funding; and
- Implement a process to ensure that approvals of over-limit transactions are well controlled and consistent with the bank's policies for extending unsecured credit.

In cases in which the bank requires pre-funding before transactions are originated through the ACH network, the bank should ensure that it has collected funds before an ACH file is sent to the ACH Operator. Banks require pre-funding for a variety of circumstances, but, at a minimum, should impose such requirements on troubled borrowers.[10]

To further reduce credit risks, management should implement procedures that require lending and ACH operations personnel to consult with one another at least annually or more often, if

[9] Consumer debit transactions may be returned for certain reasons (such as a consumer believes that the transaction is not authorized) through the ACH network for up to 60 days. In addition, an ODFI's potential liability under the NACHA Rules for breach of warranty is not limited to the return time frames, but is limited only by the statute of limitations for breach of contract claims under applicable law. See NACHA Operations Bulletin (Mar. 28, 2003).
[10] A troubled borrower is defined as having credit rated by the OCC as special mention, substandard, doubtful, or loss, or adversely rated by the bank's internal rating system.

necessary, to confirm that the originator's financial condition has not changed from the time the credit facility was approved.[11]

High-Risk Activities

Banks that engage in ACH transactions with high-risk originators or that involve third-party senders face increased reputation, credit, transaction, and compliance risks. High-risk originators include companies engaged in potentially illegal activities or that have an unusually high volume of unauthorized returns. High-risk originators often initiate transactions through third-party senders because they have difficulty establishing a relationship directly with a bank.

Examples of high-risk parties include online payment processors, certain credit-repair services, certain mail order and telephone order (MOTO) companies, illegal online gambling operations, businesses located offshore, and adult entertainment businesses. These operations are inherently more risky and incidents of unauthorized returns are more common with these businesses.[12]

Before a bank engages in high-risk ACH activities, the board of directors should consider carefully the risks associated with these activities, particularly the increased reputation, compliance, transaction, and credit risks. The board should provide clear direction to management on whether, or to what extent, the bank may engage in such ACH activities. Some banks have established policies prohibiting transactions with certain high-risk originators and third-party senders.

Banks that engage in high-risk ACH activities should have strong systems to monitor and control risk. These systems should monitor the level of unauthorized returns, identify variances from established parameters such as origination volume, and periodically verify the appropriate use of SEC codes, as transactions are sometimes coded incorrectly to mask fraud.[13] In addition, transactions with higher-risk elements, such as TEL and WEB, should be monitored to ensure that they are within the institution's risk tolerance. A high level of unauthorized returns is often indicative of fraudulent activity.[14] This indication may prompt management to terminate the relationship with the originator or third-party sender, or signal that additional training is needed to ensure compliance with ACH rules.

Compliance Risk

A bank's compliance risk management system should incorporate applicable policies, procedures, and processes for its ACH activities, including those conducted through third parties.[15] ACH reviews should be comprehensive and should test for compliance with a number of regulatory requirements, including Regulations CC, DD, and E, Bank Secrecy Act/Anti-

[11] Some banks may choose to use the same risk management policies and procedures they use for short-term unsecured extensions of credit to manage the risk associated with merchants and commercial customers originating ACH transactions.

[12] Risks may include the risk of legal liability or damage to an institution's reputation when originators or third-party senders facilitate or engage in activities that violate criminal laws.

[13] Fraud analysts should not rely exclusively on excessive unauthorized returns to identify fraud. Unusually high levels of returns for other reasons (e.g., nonsufficient funds (NSF), invalid account, or account not found) may also be indicative of fraud for some originators.

[14] NACHA operating guidelines state that a return rate of 2.5 percent is well above the acceptable rate for normal business purposes.

[15] The terms "third-party service provider" used in the Compliance section of this guidance means a third-party service provider or a third-party sender, or both, depending on the context.

Money Laundering (BSA/AML) and Office of Foreign Assets Control (OFAC) requirements, and NACHA and other network rules.

If the bank's compliance review detects regulatory violations or errors on a consumer's account, bank management should correct them in a timely manner. Remedial action includes the timely crediting of the consumer's account, identifying the cause of the violation or error, and implementing any new policies, procedures, or controls needed to prevent recurrence.

The Bank Secrecy Act requires banks to have BSA/AML compliance programs and appropriate policies, procedures, and processes in place to monitor and identify unusual activity, including ACH transactions.[16] ACH transactions that are originated through a third-party service provider (when the originator is not a direct customer of the ODFI) may increase BSA/AML risk. Risks are heightened when neither the third party nor the ODFI performs due diligence on the companies for which they are originating payments.[17]

For relationships with a bank's or an originator's third-party service provider, CDD on the third-party service provider can be supplemented with due diligence on the principals associated with the third-party service provider. When a bank is heavily reliant upon its third-party service provider, it should review the third-party service provider's suspicious-activity monitoring and reporting program, either through its own or an independent inspection.[18]

ACH transactions can be used in the layering and integration stages of money laundering. Detecting unusual activity in the layering and integration stages can be a difficult task, because ACH may be used to legitimize frequent and recurring transactions. Banks should consider the layering and integration stages of money laundering when evaluating or assessing the ACH transaction risks of a particular customer. Because of the nature of ACH transactions, adequate and effective customer and originator due diligence policies, procedures, and processes are critical in detecting unusual and suspicious activities.

Equally important is an effective risk-based suspicious activity monitoring and reporting system. For banks originating transactions for noncustomers (i.e., through third parties), the suspicious-activity monitoring and reporting systems should include the monitoring of ACH detail activity when the batch-processed transactions are returned or separated for other purposes.[19]

The ODFI may need to more closely scrutinize transaction details for international ACH activities.[20] The ODFI, if frequently involved in international ACH, may develop a separate process for reviewing international ACH transactions that minimizes disruption to general ACH processing, reconcilement, and settlement.

All parties to an ACH transaction are subject to the requirements of OFAC. With respect to domestic ACH transactions, the ODFI is responsible for verifying whether the originator is not a

[16] The FFIEC's Bank Secrecy Act/ Anti-Money Laundering Examination Manual provides additional information on BSA/AML, OFAC, and CDD requirements for ACH transactions.
[17] *ibid*, page 196. http://www.occ.gov/handbook/1-BSA-AMLwhole.pdf.
[18] Payment processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, and fraud schemes. For additional information, refer to the Third-Party Payment Processors section of the FFIEC's BSA/AML Examination Manual.
[19] Additional information on suspicious activity monitoring and reporting systems can be found in the Automated Clearing House Transactions – Examination Procedures section of the FFIEC's BSA/AML Examination Manual.
[20] The ODFI should also apply increased due diligence for domestic ACH transactions when the originator is based in a foreign country.

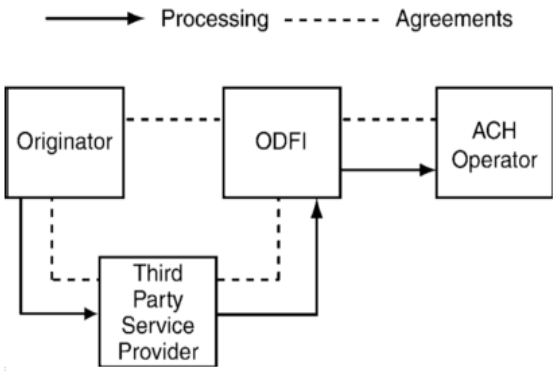
blocked party and for making a good faith effort to determine that the originator is not transmitting blocked funds. The RDFI similarly is responsible for verifying that the receiver is not a blocked party. ODFIs are not responsible for unbatching transactions if they receive those transactions already batched from their customers who have been placed on notice about their own responsibilities with regard to OFAC regulations. In such cases, ODFIs may rely on RDFIs for compliance with OFAC requirements with respect to blocking accounts and transactions on the RDFI's books. However, to the extent that unbatching occurs, the ODFI is responsible for screening as though it had done the initial batching.

With respect to OFAC screening, these same obligations hold for cross-border ACH transactions. For outbound cross-border ACH transactions; however, the ODFI cannot rely on OFAC screening by the RDFI outside of the United States.

Third-Party Service Providers

The use of third parties in ACH transactions adds complexity and increases a bank's exposure to compliance, credit, transaction, and reputation risks. Use of third-party service providers, which conduct activities on behalf of a bank, increases risk because the bank remains legally responsible, but does not have direct control over the functions performed by the third party. (*See Figure 2.)* Risks are even higher when the third party is permitted direct access to the ACH Operator on behalf of the bank.[21] Bank management should effectively oversee all ACH activity that is conducted through the bank.[22]

Figure 2 – Depicts the funds flow of a Third-Party Service Provider[23]



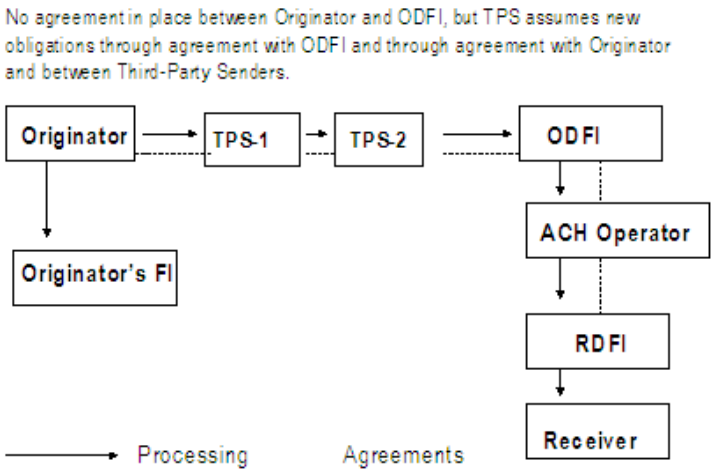
To effectively manage risk from third-party service providers, bank management should establish procedures that allow the bank to monitor the third-party service provider's operations. The first step in this process is identifying and validating the third party and the type of business it conducts. Banks should check thoroughly the background of each third-party service provider, including the principal owners, and also verify the organization's financial capacity to absorb losses. This step is particularly important if the bank allows the third party to have direct access to the ACH Operator.

[21] A third-party service provider may transmit ACH transactions directly to an ACH Operator using the bank's routing number, provided it has obtained permission from the bank. However, the bank warrants the validity of each entry transmitted by the service provider, including the basic requirement that a receiver has authorized each entry.
[22] For additional guidance on managing third-party relationships, refer to OCC Bulletin 2001-47. http://www.occ.treas.gov/ftp/bulletin/2001-47.doc
[23] Copyright held by NACHA. Reprinted with the permission of NACHA. All rights reserved.

Third-Party Senders

Third-party senders are bank customers to which originators outsource payment services, but the bank has no direct customer or contractual relationship with the originator. The third-party sender provides services to the originator and, in that capacity, acts as an intermediary between the originator and the ODFI. Because of the complexity of these arrangements, banks often lack appropriate controls over activities involving third-party senders. *(See Figure 3.)*

Figure 3 – Depicts a Third-Party Sender (TPS) acting as an intermediary between an Originator and ODFI[24]



Banks that initiate ACH transactions for third-party senders should know, at a minimum, for which originators they are initiating entries into the ACH network. Thus, banks should require third-party senders to provide certain information on their originator customers such as the originator's name, taxpayer identification number, principal business activity, and geographic location. Also, before originating transactions, a bank should verify (directly or through a third-party sender) that the originator is operating a legitimate business.[25]

Banks should be alert to whether third-party senders are using more than one bank to originate transactions. Third parties that use multiple banks to originate ACH transactions require greater scrutiny before being approved to originate transactions through the bank. For example, some third-party senders may use multiple banks to process their transactions because they had their contract with another bank terminated.

To effectively manage the risk from these arrangements, banks should have strong oversight of all third-party senders. Bank management should stay abreast of the ongoing financial condition of third-party senders and take timely mitigating action, such as amending exposure limits or requiring pre-funding. Bank management should establish a written agreement with each third-party sender. Generally, these agreements

[24] Copyright held by NACHA. Reprinted with the permission of NACHA. All rights reserved.
[25] Bank management should ensure that the bank's audit program checks for adherence to bank policy in third-party sender arrangements.

- Outline the specific board-approved risk parameters within which the third-party sender must operate;
- Detail the obligations and liabilities of the third-party sender;
- Define the information that must be provided to the bank before the third-party sender can submit transactions for a new originator;
- Define approved and disallowed originator and transaction types;
- Provide the bank ongoing access to all originators' files; and
- Outline the bank's right to audit periodically such files and/or third parties so that the bank can verify the third-party sender's compliance with bank policies.

Bank management should also ensure that there is a process to monitor third-party senders, and should establish a system to audit periodically such senders to ensure that they are operating in a sound manner.

Direct Access to the ACH Operator

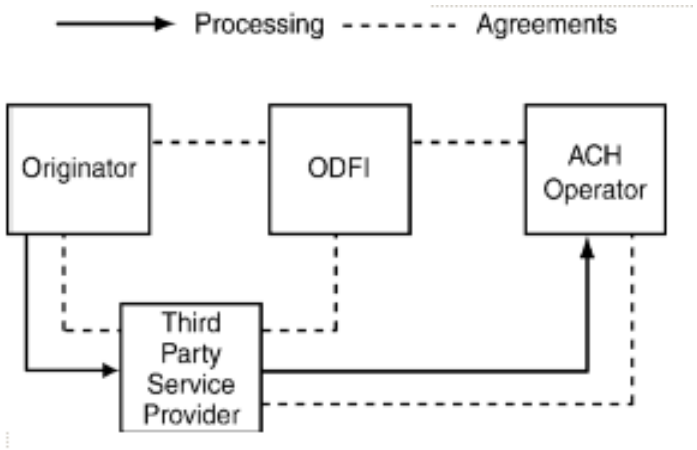
A bank that permits an originator or a third party (either its third-party service provider or an originator's third-party sender) to have direct access to the ACH Operator should maintain control over its own settlement accounts at all times. (*See Figure 4.*) To do so, a bank should enter into a written contract with the party granted access outlining the rights and responsibilities of the parties, and include a provision permitting the bank to audit the party granted access, as needed, to monitor performance and ensure compliance with applicable laws and regulations. Written contracts usually include:

- A requirement that the party granted access obtain the bank's prior approval before originating ACH transactions under the bank's routing number.

- Bank-established dollar limits for files that the party granted access deposits with the ACH Operator. A file that exceeds these dollar limits should be brought to the bank's attention before being deposited with the ACH Operator so the bank can either approve it as an exception or require that it be held until the next business day.

- A provision that restricts the other party's ability to initiate corrections to files. The bank should implement with the ACH Operator risk-control measures that limit the correction ability of the party granted access. If bank management allows the other party to correct files, it should impose and enforce strict controls over these corrections. Specifically, management should first authorize any changes to the file totals and then instruct the ACH Operator to release the file for processing. This should be a positive check-off process; *i.e.*, the ACH Operator should receive the authorization to process a file, and failure to receive the authorization should result in the file being deleted. In this way, the bank has control over its exposure from files processed by the other party.

Figure 4 – Depicts a Third-Party Service Provider with direct access to the ACH Operator[26]



Transaction Risk

Many banks process payments across different retail and wholesale payment systems, for example ACH, credit card, debit card, check, and wire that add complexity to transaction-risk management. An effective ACH risk management program should be designed to coordinate with other retail and wholesale payment-risk management programs to mitigate total bank risk exposure. An effective ACH risk management program may not reduce a bank's total risk exposure if activities are allowed to migrate to other payment systems. The industry has identified this additional complexity as "cross-channel risk."

Information Technology

Banks frequently deliver ACH services through a complex technology environment. Bank ACH systems use multiple applications, processing, storage, and communications systems that can be accessed by many internal and external users. Those systems may be operated by the bank, bank customers, or various service providers. An ACH Operator will be used for transaction clearing and settlement. Moreover, many of the communications and processing systems necessary to provide ACH services are not unique to those services. Effective risk management of the complex ACH technology environment requires a disciplined approach to the identification, measurement, and management of technology-related risks.

The *FFIEC Information Technology Examination Handbook*, through a series of 12 booklets, provides guidance in appropriately assessing the various risks associated with technology, employing effective strategies and controls, and monitoring and testing the provision of services to provide assurance that the risks are appropriately mitigated. Many of the booklets are relevant to the systems used to provide ACH services, and the "Retail Payments Systems Booklet" provides additional specific guidance related to ACH systems.[27]

[26] Copyright held by NACHA. Reprinted with the permission of NACHA. All rights reserved.
[27] FFIEC Retail Payments Handbook: http://www.ffiec.gov/ffiecinfobase/html_pages/retail_book_frame.htm

Banks should maintain consistent and effective controls over the technology used to provide ACH services, especially in the key control functions of information security and business continuity.

Information Security

ACH-related systems, processes, and controls should be included in a bank's information security program. Additionally, banks should ensure that their online ACH services comply with OCC Bulletin 2005-35, Authentication in an Internet Banking Environment.[28] (See also, OCC Bulletin 2006-35, (frequently asked questions).[29] At a minimum, the bank's information security program should address

- Customer access – Bank management should ensure dual control and confidentiality in the initial setup and activation of new customers regardless of the communication channel. Similarly, banks should secure the distribution and reset process for any authenticators used to access ACH services.

- Employee access – Banks should minimize and monitor the number of personnel with access to systems that support ACH services. Banks should minimize and segregate ACH staff and limit access to various maintenance and transaction support functions (i.e., changing account numbers, adding or deleting new users, changing transaction limits.).

- Data security – Banks should ensure that sound, risk-based data security controls exist across all ACH-related systems, applications, and processes. Control policies and practices should address data in transit or storage. ACH operations staff should accept data only from properly authenticated sources and provide a secure communication channel for all critical or confidential data. Banks should identify confidential or critical data used in ACH operations and ensure that proper storage and disposal practices are used. Key practices might include purging data from online applications, encrypting data, and destroying trace data from any media.

Business Continuity Planning

A bank's ACH activities should be factored into the bank's overall business continuity plans. Business units should ensure up-to-date assessments in light of the increased corporate-wide and customer reliance on the availability of ACH services. The business unit plans should carefully map interdependencies between units that support ACH services. Banks should also ensure that business continuity test plans are consistent with the criticality and complexity of the supporting operations for ACH services. Some business units may need to increase the scope of their testing to ensure coordinated testing with other units or key infrastructure components, such as mainframe operations, network services, or telecommunications.

CONCLUSION

The OCC supports national banks' participation in the ACH network to serve the needs of legitimate bank customers and to diversify sources of revenue. To maximize the benefits of ACH activities, banks should implement an effective process for managing the associated risks.

[28] http://www.occ.treas.gov/ftp/bulletin/2005-35.doc
[29] http://www.occ.treas.gov/ftp/bulletin/2006-35.doc

The value a bank will derive from its ACH program is directly proportional to the quality of the board's strategic planning and the effectiveness of its ACH risk management program.

ADDITIONAL INFORMATION

You may direct any questions or comments to the Operational Risk Policy Division at (202) 874-5190.

_____

Mark L. O'Dell
Deputy Comptroller for Operational Risk