Introduction

This module applies to examinations of the Federal Home Loan Banks (FHLBanks), the Office of Finance; Fannie Mae and Freddie Mac. The module refers to these institutions collectively as the regulated entities; and to Fannie Mae and Freddie Mac as the enterprises.

Payment and securities settlement systems consist of numerous financial intermediaries, financial services firms, and non-bank businesses that create, distribute, and process electronic transactions to purchase, sell, or finance securities transactions; disburse or repay loans; settle real estate transactions; and make large-value time-critical payments, such as payments for the settlement of Interbank purchases and sales of federal funds, settlement of foreign exchange transactions, or other financial market transactions.

Wire transfers via the Federal Reserve's Fedwire® Funds Service (Fedwire) are used for making large-value payments. Fedwire is the electronic payments and securities transfer service that banks, businesses and government agencies rely upon for mission-critical same-day transactions. There are two primary aspects of the Fedwire service:

1. Fedwire Funds Service A real-time gross settlement system that enables an entity to send or receive time-critical payments for its own account or on behalf of clients, settle commercial payments or positions with other financial institutions or clearing arrangements, submit federal tax payments or buy and sell federal reserve funds.
2. Fedwire Securities Service A book-entry securities transfer system that provides cost-effective safekeeping, transfer and delivery-versus-payment settlement services with flexible account structures and automated claim adjustment features.

Another widely utilized system is the ACH. The Automated Clearing House (ACH) network is a nationwide mechanism that processes electronically originated batches of high-volume, low-value credit, and debit transfers. Rather than sending each payment separately, ACH transactions are accumulated and sorted by destination for transmission during a predetermined time period. This provides significant economies of scale and faster processing than paper checks. The ACH network is also used to convert check payments into ACH debit transfers, which provides faster processing and reduces payment processing costs.

A discussion of wire transfers and ACH transactions follows below:

Wire Transfers

The primary function of wire transfer systems is to transfer assets from the control and guardianship of one institution to the control and guardianship of another institution in a timely and efficient manner. Most financial transactions are conducted through telecommunications systems designed to handle the daily exchange of large volumes of funds and securities. Although several different mechanisms comprise the U.S. payments system, most of the dollar value of all funds transfers and much of the associated risk is concentrated in two electronic systems used principally to transfer large-dollar payments between financial institutions. Foremost is the Federal Reserve Banks' Fedwire® Funds Service (Fedwire). Second is the Clearing House InterBank Payments System (CHIPS), operated by the New York Clearing House Association and utilized primarily for international transfers.

A given funds transfer is a series of payment orders, beginning with the originator's instruction to its "sending bank" and ending with the acceptance by the "receiving bank" of the payment order for the benefit of a beneficiary. A "payment order" is an instruction from a sending bank to a receiving bank to pay or cause another bank to pay a fixed amount to a beneficiary. The order must be transmitted directly or through an agent to the receiving bank.

Controls at both sending and receiving banks must focus on the authentication of payment orders. Acceptance of a payment order by the receiving bank is based on a belief that the sender properly authorized the order. Acceptance means that the receiving bank is obliged to pay the beneficiary.

A materially erroneous or fraudulent transaction could have a significant effect on the financial condition of the regulated entity and could have associated legal and reputational risks. If a loss resulting from the transmission of an erroneous payment or fraudulent payment order will be borne by the receiving bank or by the sending bank depends on: (a) whether a "commercially reasonable security procedure" was in place by the respective financial institutions; and, (b) whether actual execution complied with the security procedure.

Automated Clearing House (ACH)

The following are examples of payment transactions that can be conducted through the ACH Network:

1) Payroll payments;

2) Cash concentrations and disbursements;
3) Pension payments;
4) Loan and interest payments;
5) Tax payments;
6) Corporate-to-corporate payments;
7) Vendor payments;
8) Point-of sale-payments;
9) Insurance payments;
10) Utility payments; and
11) Customer initiated transactions.

It is important to identify the role played by the regulated entity in the ACH transaction, as there are different rules and requirements for the various participants. In addition, different rules and requirements exist for corporate and consumer accounts. The primary participants in an ACH transaction are described below.

1) Originator

An originator (Originator) is a person or entity that agrees to initiate ACH entries into the payment system according to an arrangement with a receiving person or entity (Receiver). The Originator is usually a company or an individual directing a transfer of funds to or from a consumer's or a company's account. Examples of Originators are:

a) A corporate employer offering its employees direct deposit of payroll;
b) A merchant or financial institution that offers point-of-sale activity to consumers; and
c) An individual that initiates an entry through a bill payment service to a company for monies owed.

The Originator must initiate the transmission of batches into the ACH Network according to an arrangement with an originating depository financial institution (ODFI). The primary participant relationships for the Originator are with the Receiver and the ODFI, both of which should be identified and defined in relevant legal agreements.

2) Originating Depository Financial Institution (ODFI)

The ODFI is the institution that receives payment instructions from Originators and forwards the entries to an ACH operator (ACH Operator). A depository financial

institution (DFI) may participate in the ACH system as a receiving depository financial institution (RDFI) without acting as an ODFI; however, if a DFI chooses to originate ACH entries, it must also agree to act as an RDFI.

Primary ODFI responsibilities include:

a) Ensuring that all entries are authorized;
b) Transmitting the entries to the ACH Network in a timely manner in order to effect the transfer of funds on the appropriate date;
c) Terminating the origination of entries when appropriate;
d) Meeting the requirements for data security and personal identification numbers when applicable;
e) Ensuring that the entries contain the appropriate information;
f) Ensuring that information contained within reclamation entries is accurate;
g) Ensuring that an agreement has been entered into with a sending point when a sending point is used to transmit ACH entries;
h) Ensuring that the ODFI and any third-party service provider that performs a function of ACH processing on behalf of the ODFI are in compliance with the audit requirements as defined by National Automated Clearing House Association (NACHA); and
i) Compliance with ACH operating rules adopted by NACHA (NACHA ACH Operating Rules).

The ODFI is solely responsible for entries originated by its corporate customers. The ODFI must execute a written agreement with its corporate customer that will, at a minimum, require the latter to adhere to NACHA ACH Operating Rules.

ODFIs are required to establish limits upon and monitor their exposure to risk when transmitting ACH credit and debit entries on behalf of their corporate customers. The limits should reflect ACH processing activity and should be monitored as a part of daily operations.

3) Automated Clearing House Operator

The ACH Operator is the central clearing facility operated by a private organization or a Federal Reserve Bank acting on behalf of DFIs, to or from which participating DFIs transmit or receive ACH entries. In some cases, there are two ACH Operators involved in a transaction, one operating as an originating ACH Operator and the other as a receiving ACH Operator. ACH Operators provide ACH processing services to

DFIs under a written agreement or contract.

4) Receiving Depository Financial Institution (RDFI)

An RDFI is a participating depository financial institution that receives entries directly or indirectly from its ACH Operator for debit or credit to the accounts of its customers as Receivers.

An RDFI's responsibilities include the following in regard to receipt of ACH files:

a) Timely receipt and validation of all ACH entries;
b) Timely posting to the Receiver's accounts;
c) Timely validation of pre-notifications;
d) Timely return of entries not posted;
e) Timely return of pre-notification entries;
f) Notification to Originators of incorrect information on accepted entries;
g) Timely handling of remittance data as required by NACHA ACH Operating Rules; and
h) Transmission to a federal government agency of a consumer's or company's automated enrollment for a future credit or debit application.

The RDFI must execute the appropriate agreements with its ACH Operator in order to have ACH files delivered to the proper receiving point (Receiving Point).

5) Receiver

A Receiver is a natural person or an organization that has authorized an Originator to initiate an ACH entry to the Receiver's account with the RDFI.

6) Receiving Point

A Receiving Point is any site where entries are received from an ACH for processing. This may be a financial institution, its data center, or a data processing service authorized to receive entries on behalf of the financial institution.

7) Net Settlement

Net settlement (Net Settlement) allows participants in private-sector clearing arrangements to exchange and settle transactions on a net basis through reserve or clearing account balances. Net Settlement is available to transactions that settle

across Federal Reserve Districts as well as transactions that settle entirely within a single Federal Reserve Bank.

The net debit and credit positions of the financial institutions are calculated and debited or credited to the reserve accounts of the financial institutions. A daily settlement occurs with the Federal Reserve Bank unless a financial institution designates another member to settle on its behalf.

An agreement should exist between the financial institutions and the Federal Reserve Bank that establishes the terms of ACH funds transfers.

8) Sending Point

A sending point (Sending Point) is a processing site that sends entries to an ACH. This may be a financial institution or a data processing service operating on its behalf. An agreement should exist between the financial institutions and/or the data processing service and the Federal Reserve Bank that establishes the terms of the ACH funds transfers.

9) Third-Party Service Providers and Third-Party Senders

A third-party service provider (Third-Party Service Provider) is an entity other than an Originator, ODFI, or RDFI that performs any functions on behalf of the Originator, the ODFI, or the RDFI related to the ACH processing of entries, including but not limited to, the creation of ACH files or acting as a Sending Point or Receiving Point on behalf of a participating DFI.

A third-party sender (Third-Party Sender) is an entity that is not an Originator that has authorized an ODFI or another Third-Party Sender to transmit, for the account of the Third-Party Sender or another Third-Party Sender, (i) a credit entry to the account of a Receiver with an RDFI in order to effect a payment from the Originator to the Receiver, or (ii) a debit entry to the Receiver's transaction account or general ledger account with an RDFI in order to effect a payment from the Receiver to the Originator.

In distinguishing between a Third-Party Service Provider and a Third-Party Sender, ACH participants should understand that Third-Party Senders are a subset of Third-Party Service Providers. A Third-Party Sender is always a Third-Party Service Provider that acts on behalf of an Originator, but a Third-Party Service Provider does not always act as a Third-Party Sender.

NACHA's ACH Operating Rules require that an Originator and an ODFI have an agreement that binds the Originator to these rules. However, in today's environment, it is a common practice among some Originators and ODFIs to have agreements with a Third-Party Service Provider that stands between the Originator and the ODFI and acts in an intermediary capacity between these two parties. In such circumstances, the lack of a direct contractual relationship between the Originator and the ODFI has the potential to increase the risk incurred by the ODFI since it may be unable to establish a claim against the Originator in the event of loss.

Examples of a Third-Party Service Provider include a data processing service bureau, payroll processor, correspondent bank, payable-through bank, or a financial institution acting as an agent on behalf of another financial institution. Specific duties and responsibilities should be detailed in the applicable legal agreements.

10) Gateway Operators

A gateway operator (Gateway Operator) is a financial institution that receives an ACH file from a customer and transmits the file to another financial institution, which, in turn, sends the file to a foreign financial institution.

Regulatory Environment

The primary authorities governing, or relevant to, wire transfer and ACH activities of the regulated entities are set forth below. The examiner should ensure that the application of such authorities to a regulated entity has been considered by the regulated entity and its legal counsel.

1) Rules and Regulations of the Federal Housing Finance Agency (FHFA) and the Office of Federal Housing Enterprise Oversight (OFHEO), which include the following parts and sections relevant to the Enterprises' wire transfers and ACH activities:

12 CFR Part 1710 addresses powers and responsibilities of the boards of directors for Fannie Mae and Freddie Mac. In particular, 12 CFR 1710.19 regarding the compliance program and the risk management program is pertinent.

12 CFR Part 1720 establishes minimum safety and soundness requirements. In particular, Appendix A of Part 1720, Section B. IV. - Information Technology and Section B. V. - Internal Controls are pertinent.

2) ***Rules and Regulations of the FHFA and its predecessor, the Federal Housing Finance Board (Finance Board),*** which include the following parts and sections relevant to the FHLBanks' wire transfers and ACH activities:

   12 CFR Part 917 of the Finance Board regulations addresses powers and responsibilities of FHLBank boards of directors and senior management. In particular, 12 CFR 917.3, Risk Management, 12 CFR 917.4, Bank Member Products Policy, and 12 CFR 917.6, Internal Control System, are pertinent.

3) ***Rules and Regulations of the Federal Housing Finance Agency***

   12 CFR 1233 establishes that each regulated entity report to FHFA upon discovery that it has purchased or sold a fraudulent loan or financial instrument, or suspects a possible fraud relating to the purchase or sale of any loan or financial instrument.

   12 CFR part 1235 establishes minimum requirements for a record retention program for all regulated entities (including the Office of Finance). It is intended to further prudent management as well as to ensure that complete and accurate records of each regulated entity and the Office of Finance are readily accessible to FHFA.

   12 CFR Part 1236 establishes FHFA's Prudential Management and Operations Standards ("PMOS"). Standard 1 emphasizes the need for the regulated entities (excluding the Office of Finance, which is not covered by the PMOS standards) to establish effective internal controls over systems and require secure information systems that are supported by adequate contingency arrangements.

4) ***Advisory Bulletins of the Finance Board*** that provide supervisory guidance relating to the topic of wire transfer and ACH activities are:

   Advisory Bulletin 03-2, dated February 10, 2003 and Advisory Bulletin 02-3, dated February 13, 2002, provides guidance on specific attributes to be considered by FHLBanks in the formulation of their business continuity plans, and the establishment of bilateral agreements with other FHLBanks.

   Advisory Bulletin 04-01, dated March 10, 2004, provides guidance on the evaluation of a service organization providing services to an FHLBank whose activities could affect the FHLBank's financial condition. This includes the performance of an assessment of the service organization's internal controls, such as the procurement of a service auditor's report in accordance with Statement on Standards for Attestation

Engagements (SSAE) No. 16 or the performance of alternative methods necessary to gain confidence in the service organization's internal controls.

Advisory Bulletin 04-5, dated September 29, 2004, and Advisory Bulletin 05-05, dated May 18, 2005, provide guidance on the risk management responsibilities of the board of directors, senior management, and risk management function.

5) ***Regulatory Policy Guidance (RPG) of the Federal Housing Finance Agency*** that provide clarity for regulations applicable across all entities.

RPG-2011-01, dated March 2011, is directed to all entities to develop, implement and/or enhance existing reporting structures, policies, procedures, internal controls, and operational training programs to sufficiently discover and report fraud or possible fraud in accordance with the guidance. As there are significant differences in the product offerings and investments of the regulated entities, some sections of the guidance are directed towards these differences and not all the guidance is appropriate for all regulated entities.

6) ***OFAC Letter GEN-235613 (November 2004) and OFAC Screening from FFIEC's BSA/AML Examination Manual.***

GEN-235613 provides guidance to the ACH community for cross-border ACH transactions and encourages the NACHA's rulemaking process to continue to move towards adopting cross-border standards and formatting requirements. The OFAC Screening section from the BSA/AML manual provides OFAC's rules for domestic and cross border ACH transactions, and it provides more detailed guidance on cross-border ACH transactions.

7) ***Regulation J of the Board of Governors (Board of Governors) of the Federal Reserve System (Regulation J), Collection of Checks and Other Items by Federal Reserve Banks (Subpart A) and Funds Transfer through FedWire, incorporating Article 4A (Funds Transfers) of the Uniform Commercial Code (Subpart B).***

Regulation J promotes efficient payment systems by establishing the respective responsibilities of sending and receiving banks and establishes incentives to ensure appropriate controls against unauthorized transactions. In the process, it allocates liability for failure of transaction participants to comply with their assigned responsibilities.

Regulation J allows for a "commercially reasonable security procedure" for wire transfer security which, if followed, will avoid legal liability for any wire transfer not authorized by the customer. A security procedure covered by Subpart B is one that:

1. Verifies that a payment order or communication amending or canceling a payment order is that of the customer; or

2. Detects errors in the transmission or the content of the payment order or communication.

8) National Automated Clearing House Association (NACHA) ACH Operating Rules.

NACHA oversees the ACH network and its primary roles are to develop and maintain the NACHA ACH Operating Rules, promote growth, and provide educational services to its members.

9) Federal Reserve Bank Operating Circulars and Appendices that set forth the terms for maintaining accounts with and obtaining other services from the Federal Reserve Banks. Specifically:

a) Operating Circular No. 1-Account Relationships, Agreements and Forms;
b) Operating Circular No. 4-Automated Clearing House Items (Applies to ACH only);
c) Operating Circular No. 5-Electronic Access, Certification Practice Statement, and Password Practice Statement;
d) Operating Circular No. 6-Funds Transfers Through the Fedwire Funds Service (Applies to wire transfers only).
e) Operating Circular No. 9-Federal Tax Payments and Treasury Tax and Loan Depositories (Applies to ACH only); and
f) Operating Circular No. 12-Multilateral Settlement (Applies to ACH only).

10) Issuances by the Federal Reserve Banks and Federal Financial Institutions Examination Council (FFIEC) that address specific controls and procedures as to Fedwire, FedACH Services, privately operated payment systems and the Electronic Payments Network. Specifically:

a) Federal Reserve Banks' FedLine Direct and Advantage References;
b) FFIEC Information Technology Handbooks:
    i. Information Security

ii. Business Continuity Planning
iii. Wholesale Payment Systems
iv. Retail Payment Systems
v. Operations

c) FFIEC Guidance-Authentication in an Internet Bank Environment
d) FFIEC BSA/AML examination manual (applicable sections).
e) Other relevant, applicable resource materials identified by examination staff

11) Issuance of the Board of Governors of the Federal Reserve System that addresses Intraday Liquidity Management and Payment System Risk Policy.

In July 2006, the Board of Governors implemented changes in its daylight overdraft policy for government-sponsored enterprises and certain international organizations. The changes required the organizations to eliminate their daylight overdrafts at the Federal Reserve Banks relating to their interest and redemption payments and to pay a penalty fee and post collateral if daylight overdrafts occur in their accounts as a result of their general corporate payment activity.

12) The Bank Secrecy Act (BSA), as amended by the USA Patriot Act, and the regulations and interpretations of the U.S. Department of the Treasury and Financial Crimes Enforcement Network (FinCEN) thereunder.

The BSA was enacted to safeguard the U.S. financial system from illicit use and combat money laundering and other illegal activity. Specific requirements under the BSA that may apply to financial institutions engaged in securities safekeeping services include, but are not limited to, the establishment of an anti-money laundering (AML) program reasonably designed to prevent the financial institution from being used to facilitate money laundering or the financing of terrorist activities. Additional information may be found on FinCEN's website at http://www.fincen.gov.

Failure by an institution to comply with BSA requirements may result in the imposition of civil and criminal penalties and damage the institution's reputation in the marketplace.

13) Statutes and Regulations administered by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC).

OFAC, an agency of the U.S. Department of the Treasury, administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics

traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

All U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches.

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them. Prohibited transactions are defined broadly and may include payments or transfers to a designated country or national thereof. Financial institutions are generally required to conduct screening to identify transactions involving any counterparty that has been designated by OFAC and to follow specific procedures such as blocking or freezing such counterparty's assets and providing reports to OFAC and the institution's board of directors.

OFAC maintains and periodically updates the SDN List, which may be viewed and/or searched on its website at http://www.treasury.gov/resource-center/sanctions/Pages/regulations.aspx

For more information on OFAC's sanctions programs OFAC has produced a brochure titled "Foreign Assets Control Regulations For The Financial Community," which is available on OFAC's website.

Failure by an institution to comply with OFAC requirements may result in the imposition of severe civil and criminal penalties and damage the institution's reputation in the marketplace.

14) State privacy laws that require disclosures to customers of the recording of conversations to which they are a party.

Specific requirements may vary, from state to state. Regulated entities should be aware of the laws in the states both where the caller and the other party are located.

13) ***Principles for Financial Market Infrastructure Consultative Report, dated March 2011, issued jointly by the Committee on Payment and Settlement Systems of the Bank for International Settlements and the Technical Committee of the International Organization of Securities Commissions.***

The draft report establishes a set of principles aimed to strengthen current international standards for financial infrastructures that are systematically important, including payment systems, central securities depositories, securities settlement systems, and central counterparties.

Issues Specific to the Regulated Entities

ACH Risk Management Program

The regulated entities that participate in the ACH network 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 ensuring that the ACH program does not expose the regulated entity to excessive risk. The board's role is to establish the overall business strategy and risk limits for the ACH program and to oversee management's implementation of the program. Senior 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 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 the 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:

1) A summary of the ACH program's objectives and its role within the regulated entity's strategic plan;
2) Board-approved risk tolerances that outline the types of activities the regulated entity may conduct and the types of businesses approved for ACH transactions;
3) Clearly defined duties and responsibilities that ensure strong internal controls over transactions;
4) An ACH credit-risk management program; and
5) 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 board committee, should receive periodic reports that enable the board to determine whether ACH activities remain within board-established risk parameters and are achieving expected financial results. Such reports generally include:

1) Metrics and trend analyses on ACH volume, returns, operational losses, and transaction types, with explanations for variances from prior reports;
2) Metrics and trend analyses related to the composition of the regulated entity's portfolio of originators and, as applicable, third-party senders;
3) Capital adequacy relative to the volume of ACH activity and the level of risk associated with originators;
4) A summary of return rates by originator, and, as applicable, third-party senders;
5) Unauthorized returns that exceed board-established thresholds;
6) Notices of potential and actual rules violations and fines by NACHA;
7) Financial reports on profitability of the ACH function as a cost center; and
8) Risk management reports, including a comparison of actual performance to approved risk parameters.

Internal Audit

The depth and breadth of a regulated entity's ACH internal audit program will depend on the volume and complexity of its ACH operations. 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 policies and practices, and customers' online access to the ACH network. Management should also ensure that periodic audits of third-party service providers and Third-Party Senders are performed. The internal audit function should also check for

completion of the annual NACHA Rules Compliance Audit (Rules Audit) by the regulated entity 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 internal 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 regulated entity's ACH audit activities, whether the function is performed by internal audit staff or an external audit firm. Internal auditors should attend training periodically to ensure that their skills keep pace with any expansion in the regulated entity's ACH program.

Credit Risk

Credit risk occurs in different forms, depending on the type of transaction and the regulated entity'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. 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. The RDFI's credit risk from a debit entry arises if it allows the debit to post and overdraw its customer's account.

The regulated entities need to implement credit-risk controls that establish underwriting standards, require analysis of originators' creditworthiness, and set appropriate credit exposure limits. Please see the credit risk module from the examination manual for further credit risk guidance.

Establishing Originator Underwriting Standards

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

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

1) Define desirable, prohibited, and restricted originators;
2) 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);
3) Require evaluation of the originator's creditworthiness, including a comprehensive financial analysis (similar to that performed on other potential unsecured borrowers);
4) Outline the type and timing of financial information to be provided by the originator;
5) Require review of the originator's sales history;
6) Summarize documentation requirements, including social security number or tax identification number;
7) List permissible Standard Entry Class types;
8) Provide authorization procedures for approved originators;
9) Provide guidelines for setting exposure limits, including requirements for pre-funding or collateral requirements;
10) Establish over limit monitoring and approval;
11) Outline originator account termination procedures; and
12) Allow the regulated entity to audit originators' ACH processes and controls at the regulated entity's discretion.

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

Establishing Exposure Limits

To manage credit risk effectively, regulated entities 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, regulated entities should establish separate exposure limits and monitoring practices for WEB entries. Regulated entities should also implement procedures to monitor ACH entries relative to the exposure limit across multiple settlement dates. Regulated entities need to

be aware of the extended return time frames for consumer debit transactions. Management should:

1) Set limits and obtain appropriate internal approvals before allowing ACH transactions to be initiated;
2) Establish processes to ensure 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
3) Implement a process to ensure that approvals of over-limit transactions are well-controlled and consistent with the regulated entity's policies for extending unsecured credit.

In cases in which the regulated entity requires pre-funding before transactions are originated through the ACH network, the regulated entity should ensure that it has collected funds before an ACH file is sent to the ACH Operator.

Regulatory Environment: Safety and Soundness Risks and Compliance Risks

The compliance risk management system should incorporate applicable policies, procedures, and processes for its ACH activities. This risk management system is applicable to both the regulated entities and third party service providers.. ACH reviews should be comprehensive and should test for compliance with a number of regulatory requirements, including Federal Reserve Regulations CC, DD, and E; Bank Secrecy Act / Anti-Money Laundering (BSA/AML); OFAC requirements; and NACHA and other network rules.

The Bank Secrecy Act and applicable Treasury regulations require certain financial institutions to have BSA/AML compliance programs and appropriate policies, procedures, and processes in place to monitor and identify unusual activity. Transaction monitoring is generally required for all payment activities, including ACH transactions. 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 compliance risk. Risks are heightened when neither the third party nor the ODFI performs due diligence on the companies for which they are originating payments.

All parties to an ACH transaction, including originators located outside the United States, are subject to the requirements of OFAC. With respect to domestic ACH transactions, the ODFI is responsible for verifying that the originator is not designated on OFAC's SDN list 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 designated on OFAC's SDN list. 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 the transactions against the SDN list as though it had done the initial batching. Please refer to OFAC letter GEN-235613 (November 2004) and "OFAC Screening" in the FFIEC BSA/AML examination manual.

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.

Information Technology

The regulated entities use internet-based software applications to conduct ACH transactions. The *FFIEC Information Technology Examination Handbook* 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 chapters are relevant to the systems used to provide ACH services, and the "Retail Payments Systems Booklet" provides additional specific guidance related to ACH systems.

The regulated entities 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 the regulated entity's information security program. At a minimum, the information security program should address:

1) Access by counterparties or FHLBank members – Management should ensure dual control and confidentiality in the initial setup and activation when providing access to new users regardless of the communication channel. Similarly, regulated entities should secure the distribution and reset process for any authenticators used to access ACH services.

2) Employee access – Regulated entities should minimize and monitor the number of personnel with access to systems that support ACH services. Regulated entities should minimize and segregate duties of 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).

3) Data security – Regulated entities 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. Regulated entities 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 regulated entity's ACH activities should be factored into the 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 map interdependencies between units that support ACH services. Regulated entities 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.

Specific Risk Controls Relating to Wire Transfer and ACH Activities

A regulated entity's controls relating to wire transfer and ACH activities are set forth below.

1) Origination and Authorization

The primary control for processing wires is the adequate segregation of duties that relate to the input of the wire request, the review and release of the wire, the review and release of wires that require supervisory review such as risk and OFAC queues, the establishment and maintenance of member or counterparty profiles, and the

establishment and distribution of personal identification numbers and test codes.

Outgoing wires may be originated by telephone, fax, FedLine, and the Internet and are categorized as repetitive or non-repetitive. Repetitive wires are wire transfers sent to destinations with the same bank and account number to be credited that have been preauthorized and are generally used as a routine matter. A non-repetitive wire is not preauthorized and requires closer review and performance of callbacks to ensure proper authorization.

Wire requests that lack necessary information and/or contain incorrect information such as the routing number or account number, or requests that seek to transfer funds from accounts containing insufficient funds, are transferred to the risk queue, which requires supervisory review and release of the transaction. A similar process occurs with the OFAC queue if potential "hits" are identified.

Non-repetitive wire requests represent a higher degree of risk due to error and the potential for defalcation. Therefore, such requests must require two, and sometimes three, levels of authorization, and callback verifications. For a non-repetitive wire, there must be segregation of duties between the employee that inputs the wire transaction and the employee that verifies and releases the wire transaction. Wire transfer agreements and applicable addenda such as resolutions, repetitive agreements, and authorization schedules for each customer must be maintained by the regulated entity.

In accordance with UCC-4A, the agreements should detail the duties, responsibilities, and liabilities of the regulated entity and the parties on whose behalf the transactions are being carried out. The repetitive wire addendum details the account(s) at other financial institutions to which the member or counterparty wishes to transfer funds, and the authorization schedules detail the personnel that the parties have authorized to either initiate and/or verify wire transfers. The regulated entity should review and update authorization schedules on a regular basis.

Repetitive wire information is automated and controlled through wire templates. Specific authorizations are required to add or change a repetitive wire template. This responsibility should be assigned to personnel who are not involved with the daily processing of wire transactions. Once automated, a single person may process repetitive wires, and, unless required by the wire transfer authorization schedules, callback verification does not have to be performed.

As it pertains to originating ACH transactions, the primary control is the adequate segregation of duties that relate to the input, review, and release of the ACH request, the completion of agreements and establishment of security procedures in accordance with UCC-4A and NACHA requirements.

2) Recording and Reconciliation

Wire transfer and ACH entries are processed and recorded to the counterparty's demand deposit accounts and applicable general ledger accounts such as the "Federal Reserve Bank," or "correspondent." The responsibility for the review and reconciliation of the entries should be segregated from that for the processing of the daily transactions.

Critical access controls and segregation of duties must be in place to prevent the processing of erroneous and fraudulent transactions. A material erroneous or fraudulent transaction could have a significant effect on the financial condition of the regulated entity and result in a poor image and reputation in the marketplace.

3) Daylight and Deposit Overdrafts

The Federal Reserve Banks provide the unsecured intraday credit needed to support clearing of large transactional volumes. Such credit extensions occur when a Federal Reserve Bank allows institutions to initiate transactions that exceed, at a given moment, the balance in their reserve or clearing accounts, which leaves the institution in a net debit position with the Federal Reserve Bank. These intraday overdrafts of accounts are referred to as "daylight overdrafts."

The amount of credit available to any institution is usually limited by "net debit sender caps," which establish the maximum unsecured exposure that a Federal Reserve Bank is willing to accept. As the regulated entities do not have any net debit sender caps, they must monitor their position with the Federal Reserve Bank continuously.

Repeated daylight overdrafts may result in discontinuation by the Federal Reserve Bank of services such as wires, ACH, securities, and access to capital markets, which could limit a regulated entity's ability to meet its financial obligations and provide services to its customers.

The responsibility for monitoring the regulated entity's position with a Federal Reserve Bank is usually assigned to cash management/treasury personnel. Such

personnel customarily have inquiry access to the wire system, which allows them to monitor large incoming/outgoing activity. In addition, the automated wire system has software controls that establish internal dollar limits and mitigate daylight overdraft possibilities. Deposit overdrafts represent an unsecured credit exposure, and should require the approval of credit personnel and line management.

4) Legal

In connection with wire transfer and ACH activities, legal staff review applicable regulatory requirements, vendor contracts, and other documentation to protect the regulated entity's interests. In addition, the business units coordinate a periodic review with legal staff to ensure current operating practices comply with regulatory requirements.

5) Business Continuity and Recovery

The regulated entity should have written procedures for operations at its designated hot-site. Back-up tapes should be stored off-site and be easily retrievable. If the automated wire system is not available at the hot-site, FedLine terminals, off-line codeword authorizations, and bilateral agreements with a third party, including another FHLBank, if applicable, may need to be used to effectuate the regulated entity's wire transfer and ACH activities. Each regulated entity must have at least one back-up system and must test it periodically to ascertain its reliability.

Issues Specific to the Enterprises

FedLine Direct

The Enterprises primarily use the Federal Reserve Bank's FedLine Direct® system. A FedLine Direct connection is an Internet Protocol (IP)–based access solution designed for higher-volume Fedwire participants that require an unattended connection to the Fedwire services. Operating procedures for this system are primarily governed by the Federal Reserve Bank.

Wire Transfers

Fannie Mae uses the Fedwire funds and security settlement systems to send funds and security wires to their customers. Wire activity includes, but is not limited to, investment activity, the buying or selling of whole loan mortgages, debt issuance, mortgage-backed

securities and debt principal and interest payments, real estate owned (REO) dispositions, and swap payments.

Freddie Mac uses the Fedwire funds and security settlement systems to send wires to their customers. Wire activity includes, but is not limited to, customer payments, investment activity and settlement and issuance of Freddie Mac securities.

The Enterprises do not participate in the CHIPS network.

ACH

Fannie Mae acts as an ODFI and a RDFI for the settlement of ACH activity. They are a sending point for ACH files to settle Fannie Mae-related customer transactions and activity. ACH activity includes, but is not limited to, payroll, guaranty fee receipts, and servicer, mortgage-backed securities and debt principal and interest payments collections.

Freddie Mac is an ACH originator for Payroll, Accounts Payable, and Seller billing.

Daylight Overdrafts

The Enterprises may not have daylight overdrafts at the Federal Reserve Banks relating to their interest and redemption payments. Therefore, the Enterprises must establish policies and procedures to monitor and prevent daylight overdrafts. The existence of overdrafts should be communicated to key line management, such as the regulated entity's operations and treasury operations. Treasury operations personnel should conduct ongoing monitoring to prevent the creation of daylight overdrafts.

Issues Specific to the FHLBanks

FedLine Advantage

The FHLBanks primarily use the Federal Reserve Bank's FedLine Advantage® system. A FedLine Advantage connection provides web-based access to the FedPayments® Manager tool, which allows participants to create and submit Fedwire funds and securities transfer messages, as well as to view incoming messages online. Operating procedures for this system are primarily governed by the Federal Reserve Bank.

Wire Transfers

Wire transfers are a critical operation in an FHLBank's activities for purposes of the purchase/sale of money market transactions and on behalf of its members. FHLBank members use the wire system to transfer funds between their accounts at other financial institutions for the purchase/sale of advances, securities, and money market instruments; and to make payments to third-parties. The FHLBanks do not participate in the CHIPS network. Therefore, international wires are processed through a correspondent bank relationship and others.

The FHLBanks often rely on vendor software to process wires. The software provides an audit trail necessary to comply with UCC-4A and BSA requirements. Vendor software is also customarily used by the FHLBanks to ensure compliance with OFAC requirements. There are several different vendors of funds transfer software packages. Each package offers a variety of control features such as automated segregation of duties, risk, and OFAC queues. The software must be compatible with the functionality of the wire system.

ACH

Transactional Capacity

The capacities in which FHLBanks are principally involved in ACH transactions are.

1) Originator. In this capacity, an FHLBank coordinates the processing of FHLBank's payroll with an outside service provider, who transmits the file to an ODFI. Generally, the FHLBank's human resource function has the responsibility for the review, processing, and reconciliation of the payroll.

2) Receiving Point and RDFI. In these capacities, an FHLBank receives debit and credit entries on behalf of its customers.

3) Net Settlement. In this capacity, an FHLBank initiates the settlement of the FHLBank customer's ACH files through a Federal Reserve Bank.

4) Sending Point. In this capacity, an FHLBank creates entries using the routing number of the ODFI, which is transmitted to the ACH Operator on behalf of the ODFI.

ACH responsibility is usually assigned to the demand deposit or the correspondent bank services functions of an FHLBank. The systems principally used for ACH transactions that provide access to the Federal Reserve System's on-line services and information

include the following:

1) Fedwire and FedLine Web® (FedLine Web) and/or FedLine Advantage operated by the Federal Reserve System. Transactions carried out through these systems are processed through the Federal Reserve System's website.

2) Electronic payment network operated by the local automated clearing house. These transactions are processed through its website and transmitted through the Federal Reserve System.

Settlement Processing and Reconciliation

ACH files are usually received, processed, and reconciled in the manner set forth below.

1) An ACH file is transmitted from a Federal Reserve Bank and/or an electronic payment network. It is processed in batch form through the FHLBank's demand deposit account system by an FHLBank's information technology personnel. Financial information should not be posted to the individual accounts until it has been reviewed/reconciled by designated personnel.

2) Designated personnel of an FHLBank reconcile the batch that was processed by information technology personnel to ACH summary reports, deposit reports, general ledger, and the Federal Reserve Bank's statements.

3) Exceptions, as well as rejected and returned items, are researched and resolved prior to posting. Rejected transactions are transactions that cannot be sent through the Federal Reserve Bank or that the Federal Reserve Bank has rejected. Rejected transactions can occur for the following reasons:

   (a) There is an error in the routing number or the account number.

   (b) The account is a "problem" account. The account may be coded "Post No Debits" due to being overdrawn. The FHLBank should review all ACH transactions prior to their posting to an account to determine if the account will become overdrawn if the transaction is posted.

   (c) The account may be in the process of closing. The FHLBank should review any or all transactions that will post to the account to ensure there are sufficient funds for the transactions.

4) The RDFI has the responsibility to verify and confirm with the Originator that the account number in the pre-notification is for a valid account. A "pre-notification" is a non-dollar entry sent through the ACH Network by an Originator to an RDFI.

   A "notification of change" is a non-dollar entry transmitted by an RDFI to the ACH Operator for transmission back to the Originator through the ODFI. It is created when the RDFI receives a pre-notification or a live dollar entry that contains incorrect information.

5) The existence of overdrafts should be communicated to key line management, such as FHLBank operations and treasury operations. FHLBank treasury operations personnel should conduct ongoing monitoring to prevent the creation of daylight overdrafts.

Examination Guidance

The workprogram for the Payment Systems examination module is detailed below. If this module is included in the examination scope, the examiner must perform worksteps sufficient in coverage to document the basis for conclusions on the quantity of risk and quality of risk management pertaining to this area. Transaction testing is mandatory and the examiner must document sufficient work steps from Section 4, *Testing*, to support the findings and conclusions from this examination module.

In determining the extent of review and testing to be conducted in completing each examination, the examiner should take into account any applicable FHFA off-site monitoring or analysis reports, such as analysis of the quality and effectiveness of corporate governance practices, financial condition and performance, economic and housing industry conditions, internal controls, and audit coverage relating to the institution's wire transfer and ACH activities.

NOTE: Text in (*italics*) referenced in a workstep represents illustrative guidance that serves as suggestions for specific inquiry.

1. Scope of Examination Work Performed

1) Review past reports of examination for outstanding issues or previous problems related to payment systems.

2) Review applicable FHFA off-site monitoring or analysis reports, and workpapers produced as part of continuous monitoring, related to payment systems.

3) Assess the status of outstanding examination findings pertaining to payment systems.

4) Review internal audit reports for outstanding issues relating to payment systems.

5) Review minutes of meetings of the board of directors and relevant board and management committees for any issues regarding payment systems.

Summarize the work performed in the examination of payment systems. To the extent there were modifications to the originally planned scope based on concerns identified during the examination, document those changes and the reasons for such changes.

2. Description of Risks

1) Evaluate any significant changes to wire transfer and ACH activities that have been implemented since the last examination or are being considered that may affect the regulated entity's risk profile such as management, systems, key personnel, regulatory requirements, and processing.

2) Identify key risks associated with the regulated entity's Payment Systems. In addition to operational risk, consider other potential risk exposure.

3. Risk Management

Risk Identification Process

1) Based on worksteps performed under **Description of Risks**, assess and conclude on the adequacy of the organization's risk identification process.

2) Determine if the regulated entity has appropriately identified, monitored, and managed the credit and operational risk issues related to wire transfer and ACH activities. (*Do personnel coordinate the mitigation of such risks appropriately throughout the organization and among the divisions of the regulated entity? Coordinate examination activities with other examiners appropriately to ensure potential risk to the entire organization is assessed.)*

Organizational Structure

1) Identify the key personnel and their primary duties, responsibilities and technical expertise to determine if resources are effectively deployed to wire transfer and ACH activities.

2) Evaluate the staffing and skill level, segregation of duties, and cross-training of personnel to determine if resources are sufficient to execute the wire transfer and ACH strategies. (*Does staff have appropriate training and experience to carry-out their responsibilities within the organization? Is there segregation of duties in processing, recording, and reconciliation transactions? What steps has the regulated*

entity taken to address identified deficiencies in staff expertise? Are such steps appropriate?)

3) Determine whether sufficient coordination with other departments such as risk management, information technology, treasury and cash management, accounting, credit, and human resources is taking place. (*Are there adequate procedures to limit risk of loss when conducting wire transfer and ACH activities? Are mandatory leave/vacation and out of office protocols in place?*)

Policy and Procedure Development

1) Assess the regulated entity's policies and procedures relating to the following, as applicable:
   a) Wire transfer and ACH operations;
   b) Risk management;
   c) Information security;
   d) OFAC compliance;
   e) Fraud prevention and reporting;
   f) Whistleblower provisions of Sarbanes-Oxley Act of 2002 and Dodd-Frank Wall Street Reform and Consumer Protection Act;
   g) Background and credit investigations;
   h) Business conduct and ethics;
   i) Business continuity and recovery;
   j) Member products; and
   k) Vendors' risk.

   (*Are policies and procedures current, relevant, sufficiently detailed, and consistent with the regulated entity's policies and regulations? Do the policies provide adequate guidance in controlling risk to the institution? Do policies and procedures clearly define responsibility for adhering to established parameters? Are ongoing reporting requirements established and reasonable to adequately monitor potential risk to the institution resulting from wire transfer and ACH activities?)*

2) Assess the risk management function for wire transfer and ACH activities, which may include the following:

   a) Prohibiting or limiting specific types of wire transactions such as international and/or third-party wires;
   b) Limiting or restricting ACH services offered;

c) Establishing timeframes and requiring customer notification for estimated large dollar wire activity;
d) Requiring specific procedures to authenticate wire transfer requests such as agreements, personal identification numbers, passwords, tokens and callback procedures;
e) Requiring the completion of specific agreements to ensure compliance with UCC-4A and NACHA requirements;
f) If operating as an ODFI, requiring specific security procedures to authenticate ACH requests received from an Originator or a Third-Party Sender, and establishing policies and procedures to review and monitor credit exposure limits for each of its corporate Originators;
g) Requiring supervisory reviews of exceptions such as rejected items, deposit and daylight overdrafts, transactions with parties identified on OFAC's "Specially Designated Nationals and Blocked Persons" list, and wire requests that exceed a specific dollar amount;
h) Restricting system access and function capabilities;
i) Segregating processing, recording, and reconciliation duties in transactions;
j) Requiring periodic reissuance of wire transfer personal identification numbers and test codes and reconfirming authorizations with customers; and
k) Mitigating risks and liability with the purchase of specific insurance and bond coverage such as directors and officers liability, errors and omissions, computer cyber crime policies and fidelity bond coverage, and establishing compensating procedures and controls to address any exclusions in the policies.

Risk Metrics

1) Evaluate any risk metrics related to wire transfers and ACH activities. Conclude whether such metrics considered all aspects of potential risk to the organization. (*Are the established limits reasonable and appropriate? Are controls established adequate?)*

2) Determine if risk metrics (composition and levels) are consistent with the risk appetite of the organization. (*Do risk parameters established for payment systems result in risk exposure beyond the regulated entity's overall risk appetite?)*

3) Evaluate the adequacy of the board and management's efforts to ensure compliance with risk metrics. (*Is information reported to the board and management accurate and comprehensive? What actions have been taken when risk metrics are not met by the regulated entity?)*

Reporting

1) Review and assess key management reports of wire transfer and ACH activities. (*Are reports comprehensive and do they address all risk areas?*)

2) Determine the adequacy of senior management and operations committee reporting of key operating procedures controls and deviations. (*Do management committees and board minutes detail sufficient discussion of wire transfer and ACH activities? Are control breakdowns reported?*)

Internal/External Audit

1) Evaluate the effectiveness of evaluations conducted pursuant to SARBOX that identify the key risks and controls pertaining to financial reporting and evaluate potential fraud, and procedures implemented to attest periodically to the adequacy of the control environment.

2) Evaluate the adequacy of the scope and testing performed by external and internal auditors on wire transfer and ACH activities. In addition, verify that an annual audit was conducted to determine compliance with ACH rules no later than December 1 of each year. (*Is testing sufficient to ensure controls reasonably limit potential losses? Does testing ensure that procedures are followed?*)

3) Evaluate the adequacy of the scope and testing performed by outside consultants such as penetration testing. (*Is testing sufficient to ensure controls reasonably limit potential losses? Does testing ensure that procedures are followed?*)

Information Technology

1) Identify and assess the automated and manual systems and applicable controls over wire transfer and ACH activities for processing transactions, including:

   a) Authorized users;
   b) Vendor technical support and access to the automated wire system;
   c) Utilization of spreadsheets;
   d) Exception tracking, escalation, and reporting; and
   e) Business continuity and recovery.

Compliance

1) Review compliance with laws and regulations, including Regulation J of the Board of Governors, the Bank Secrecy Act, and the Office of Foreign Assets Control. (*For instances of violations, identify the cause of the violation. Let the regulated entities determine how internal controls should be strengthened to reduce risk of future regulatory violations.)*

2) Review compliance with the Board of Governor's Operating Circulars and other issuances by the Federal Reserve governing specific controls and procedures for the FedWire applications, intraday liquidity management, and payment systems risk policies. (*For instances of noncompliance, identify the cause of the noncompliance. Let the regulated entities determine how internal controls should be strengthened to reduce risk of future instances of noncompliance.)*

3) Review compliance with the National Automated Clearing House Association ACH Operating Rules. (*For instances of noncompliance, identify the cause of the noncompliance. Determine how internal controls should be strengthened to ensure there is no future noncompliance.)*

4) Assess compliance with FHFA PMOS Standard 1 which requires the regulated entities to establish effective internal controls over systems and requires secure information systems that are supported by adequate contingency arrangements. (*Has the regulated entity ensured that they have implemented appropriate internal controls to limit risk and ensure that information technology systems for wire transfer and ACH are physically secured?)*

4. Testing

1) Follow-up on previous examination findings and evaluate management's efforts to implement corrective actions.

2) Determine if management effectively corrected deficiencies noted by internal audit.

3) Conduct testing as appropriate. The scope of testing should be based on the preliminary review of governance, risk management, internal controls, and audit coverage. Specific examples include, but are not limited to, the following:

<u>Wire Transfers</u>

a) Restrictions upon physical access to the wire terminals or, in their absence, compensating controls to ensure proper authorization of transactions such as dual control, limitations upon system access or function capabilities, and managerial review;

b) Verification procedures to ensure proper authorization of wire requests received by telephone, fax, internet, letter and departmental communication such as agreements, personal identification numbers, test codes, tokens, callback procedures, and customer confirmations;

c) System controls applicable to the automated wire system such as the review and establishment of employees' system capabilities; access and function capabilities; system defaults pertaining to user identifications; password composition and length; number of attempts before being locked-out; expiration and timeout; and dollar limitations;

d) Timely recording and reconciliation of wire transactions;

e) Evaluation of deposit and daylight overdrafts that were the result of wire transfer activity and whether the occurrences were isolated or the result of weaknesses in the internal control environment;

f) Periodic coordination with legal counsel to ensure that governing agreements and addenda adequately address UCC 4A requirements;

g) Adequacy of software to identify potential suspects on OFAC's "Specially Designated Nationals and Blocked Persons" list;

h) Recoverability of telephone recordings and compliance with applicable state privacy requirements mandating disclosures to customers when conversations are being recorded;

i) Background and credit investigations for wire transfer personnel and fraud prevention actions such as mandating that wire transfer personnel take the required minimum number of consecutive vacation days;

j) Reissuance of wire transfer personal identification numbers and test codes as well as confirmation of authorizations with the customers;

k) Completion of applicable vendor agreements and compliance with vendors' risk

policies; and

l) Establishment of record retention procedures that pertain to automated and manual records.

ACH

a) ACH transactions are requested and processed by authorized personnel. Observe that physical security has been established over the terminals, or in their absence, compensating controls to ensure proper authorization have been established. Specific attributes to consider are:

   (1) Identify the regulated entity's ACH transactional capacity and evaluate the methodology of receiving the ACH request, such as FedLine Advantage, FedLine Direct, telephone, fax, Internet, or letter. If the regulated entity is operating as an ODFI, evaluate the adequacy of the security procedures established with the Originator and/or Third-Party Sender, and limiting credit risk exposures with its corporate Originators.
   (2) Review the system controls applicable to the terminals such as the review and establishment of employees' system capabilities, access and function capabilities, system defaults pertaining to user identification, password composition and length, number of attempts before being locked-out, expiration and timeout.
   (3) Observe the processing of an ACH transaction. If applicable, verify compliance with dual control requirements.
   (4) Review a sample of incoming, outgoing, and future-dated ACH transactions. Verify authorizations, including agreements and resolutions, and the timeliness and accuracy of posting to the customer's account. Also, if applicable, select a current transaction and trace to the confirmation.
   (5) If applicable, review the supporting documentation of a recently completed pre-notification and determine compliance with NACHA's requirements.
   (6) If applicable, review the supporting documentation of a recently completed Notification of Change and determine compliance with NACHA requirements.

b) Review the ACH reconciliation as of the examination date. In addition, evaluate the adequacy of the following attributes:
   (1) Segregation of duties;
   (2) In the event the assigned employee is absent, another employee has been designated to reconcile the accounts;

(3) Timely review, reconciliation of balances and resolution of differences and rejected items;
(4) Managerial review of the reconciliations; and
(5) Periodic reporting to accounting personnel.

c) Review the most recent deposit overdraft report and daylight overdrafts. If the overdrafts were the result of ACH activity, review with line management the situations that caused the customer deposit and/or daylight overdraft, and corrective action implemented. Evaluate whether the overdrafts were isolated, and whether they were the result of weaknesses in the design of the internal control environment, or lack of compliance with existing policies and procedures.

d) Review a sample of ACH agreements and applicable resolutions. Verify that legal counsel conducts periodic reviews to ensure that the agreements adequately address NACHA, UCC-4A, and OFAC requirements.

5. Conclusions

1) Summarize conclusions for all examination work performed, including work performed by other FHFA staff as it relates to the regulated entity's payment systems function. Develop a memorandum articulating the risks to the institution resulting from payment system practices and the regulated entity's management of those risks. The memorandum should describe the basis of conclusions reached and summarize the analysis completed. Within the memorandum, discuss the types of risk the regulated entity is exposed to (e.g., market, credit, operational); the level of risk exposure; the direction of risk (stable, decreasing, increasing); and the quality of risk management practices (strong, adequate, weak). A memorandum must be prepared irrespective of whether the examiner's assessment is positive or negative.

2) Conclude on the responsiveness to previous examination findings. Evaluate the adequacy of the regulated entity's response to previous examination findings and concerns.

3) Develop findings and prepare findings memoranda, as appropriate. Based on examination work performed, develop findings communicating concerns identified during the examination. Findings should identify the most significant risks to the institution and the potential effect to the regulated entity resulting from the concerns identified. Such documents should describe a remediation plan specifying the appropriate corrective action to address examination concerns and establish a reasonable deadline for the regulated entity to remediate the finding. Communicate preliminary findings to the EIC. Discuss findings with regulated entity personnel to ensure the findings and analyses are free of factual errors.

4) Develop a list of follow-up items to evaluate during the next annual examination. In addition to findings developed in the steps above, include concerns noted during the examination that do not rise to the level of a finding. Potential concerns include issues the regulated entity is in the process of addressing, but require follow-up work to ensure actions are completed appropriately. In addition, potential concerns should include anticipated changes to the institution's practices or anticipated external changes that could affect the institution's payment system practices.

Workprogram

1. Scope of Examination Work Performed

Workpapers must document the examination activities undertaken to evaluate potential risks related to payment systems.

2. Description of Risks

- Identify areas of concern related to payment systems
- Assess current risks and trends in the risk to the organization related to payment systems
- Evaluate changes within the organization or industry affecting risk
- Evaluate the entity's own risk-identification practices and conclude on their adequacy

3. Risk Management

- Assess and conclude on the adequacy of the organization's risk identification process
- Assess and conclude on the overall adequacy of internal controls, including an evaluation of:
    - The regulated entity's organizational structure
    - Policy and procedure development for payment systems
    - Appropriateness of risk metrics established for payment systems
    - Reporting by management and the board
- Assess and conclude on the internal and external audit of risks
- Assess and conclude on the adequacy of information technology and controls related to payment systems
- Assess and conclude on the adequacy of the organization's efforts to ensure:
    - Compliance with laws, regulations and other supervisory guidance
    - Compliance with the organization's policies and procedures

4. Testing

- Complete testing, as appropriate, to assess adherence with examination standards

5. Conclusions

- Summarize conclusions for all examination work performed related to wire transfer and ACH
    - Conclude on the level of risk to the organization
    - Include an assessment of the adequacy of an organization's monitoring of risk and establishment of internal controls to mitigate risk
- Conclude on responsiveness to examination findings from previous examinations

- Develop examination findings as appropriate
- Identify areas requiring follow-up examination activities or monitoring