Federal Financial Institutions Examination Council

FFIEC

Wholesale Payment Systems

WPS

JULY 2004

IT EXAMINATION

HANDBOOK

Table of Contents

Introduction

This Wholesale Payment Systems Booklet (Booklet) is one of several that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook (IT Handbook). It provides guidance to examiners and financial institution management regarding the risks and risk-management practices when originating and transmitting large-value payments. It replaces and rescinds Chapter 18 of the 1996 Information Systems Examination Handbook.

This booklet is organized into the following four sections describing the various aspects of wholesale payment systems, followed by examination procedures, a glossary, a discussion of the legal framework for interbank payment systems, a discussion of the Federal Reserve Board's Payments System Risk (PSR) Policy, and a discussion of the "Interagency Paper on Sound Practices to Strengthen the Resiliency of the U.S. Financial System." Management action summaries are included in each of the four sections providing a snapshot of the risks and risk management practices described in the text.

- Interbank Payment and Messaging Systems - The first section includes a discussion of interbank funds transfer and messaging systems, and interbank clearing and settlement systems. This section concludes with a discussion of Internet-based wholesale payment systems.
- Intrabank Payment and Messaging Systems - The second section provides an overview of the funds transfer and messaging systems employed by typical financial institutions.
- Securities Settlement Systems - The third section provides an overview of the major securities markets and securities settlement systems. Securities settlement generates a large volume of wholesale payments typically processed by financial institutions. The information presented in this section describes these settlement processes. While securities settlement generally involves both the delivery of a security and the corresponding payment, this section focuses on the wholesale payments generated by these transactions, and does not cover the complete range of activities associated with securities processing, including the transfer and delivery of securities, custodial arrangements, and related trading activities. [1]
- Wholesale Payment Systems Risk Management - The fourth section describes the risks associated with wholesale payment systems, using various risk categories, including reputation, strategic, credit, liquidity, legal/compliance, and operational/ transaction risk. This section also describes the risk management measures management should establish to mitigate the risks described.

The booklet references a number of other IT Handbook booklets, including the "Information Security Booklet," "Business Continuity Planning Booklet," "Outsourcing Technology Services Booklet," and the "FedLine Booklet." [2] In addition to describing the information technology risks and controls, the booklet also describes certain credit and liquidity risks that may be present when conducting wholesale payment services. A full review of a financial institution's wholesale payment system environment may require the

use of examiners with experience in credit, liquidity, and compliance issues and additional agency-specific examination procedures.

Examiners should use the examination procedures (detailed in Appendix A) for reviewing risks in wholesale payment systems. These procedures address services and products of varied complexity, and examiners should adjust the procedures for the scope of the examination and the size and risk profile of the institution. Examiners may use the procedures independently or in combination with procedures from other IT Handbook booklets and agency specific handbooks and guidance.

For financial institutions whose primary method for originating, transmitting, and receiving large-value payment orders is the use of the FedLine Funds Transfer (FT) application, examiners should use the "FedLine Booklet" to assess the wholesale payment systems and funds transfer environment. In addition, examiners should also review the "Legal Framework" and "PSR" discussions in Appendices D and E, respectively, if an expanded evaluation of the funds transfer operation is necessary.

Interbank Payment and Messaging Systems

Fedwire and Clearing House Interbank Payments System (CHIPS)

In the United States, payment and securities settlement systems consist of numerous financial intermediaries, financial services firms, and non-bank businesses that create, distribute, and process large-value payments. The bulk of the dollar value of these payments are processed electronically and are generally used 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.

There are two primary networks for interbank, or large-value, domestic, funds transfer payment orders. The first, Fedwire® Funds Service, is operated by the Federal Reserve Banks, and is an important participant in providing interbank payment services as well as safekeeping and transfer services for U.S. government and agency securities, and mortgage-backed securities. [3] Funds Service and the Federal Reserve's National Settlement Service (NSS) are critical components used in other payment systems' settlement processes.The Clearing House Interbank Payments Company L.L.C. (CHIP Co.) operates the second, the Clearing House Interbank Payments System (CHIPS). [4]

Processing large-value funds transfers involves two key elements: clearing and settlement. Clearing is the transfer and confirmation of information between the payer (sending financial institution) and payee (receiving financial institution). Settlement is the actual transfer of funds between the payer's financial institution and the payee's financial institution. Settlement discharges the obligation of the payer financial institution to the payee financial institution with respect to the payment order. Final settlement is irrevocable and unconditional. The finality of the payment is determined by that system's rules and applicable law.

In general, payment messages may be credit transfers or debit transfers. Most large-value funds transfer systems are credit transfer systems in which both payment

messages and funds move from the payer financial institution to the payee financial institution. An institution initiates a funds transfer by transmitting a payment order (a message that requests the transfer of funds to the payee). Payment order processing follows the predefined rules and operating procedures of the large-value payment system used. Typically, large-value payment system operating procedures include identification, reconciliation, and confirmation procedures necessary to process the payment orders. In some systems, financial institutions may contract with one or more third parties to help perform clearing and settlement activities on behalf of the institution.

The legal framework governing payment activity and the regulatory structure for financial institutions that provide payment services is complex. [5] There are rules for large-value payments that are distinct from retail payments. Large-value funds transfer systems differ from retail electronic funds transfer (EFT) systems, which generally handle a large volume of low value payments including automated clearinghouse (ACH) and debit and credit card transactions at the point of sale.

Fedwire Funds Service

Fedwire Funds Service is a real-time gross settlement system (RTGS) enabling participants to transmit and receive payment orders between each other and on behalf of their customers. Real-time gross settlement means that the clearing and settlement of each transaction occurs continuously during the processing day. Payment to the receiving participant (payee) over Fedwire Funds Service is final and irrevocable when the Federal Reserve Bank either credits the amount of the payment order to the receiving participant's Federal Reserve Bank reserve account or sends notice to the receiving participant, whichever is earlier.

Fedwire Funds Service participants must maintain an account with a Federal Reserve Bank. Because of this requirement, non-financial organizations are not permitted direct access to Fedwire Funds Service, although these entities may use these services indirectly as customers of deposit-taking financial institutions.Subject to the Federal Reserve Bank's and the Federal Reserve Board's risk reduction policies, where applicable, entities authorized by law, regulation, policy, or agreement to be participants include depository institutions, agencies and branches of foreign banks, member banks of the Federal Reserve System, the Treasury and any entity specifically authorized by federal statute to use the Reserve Banks as fiscal agents or depositories, entities designated by the Secretary of the Treasury, foreign central banks, foreign monetary authorities, foreign governments, and certain international organizations; and any other entities authorized by a Federal Reserve Bank to use Fedwire Funds or Security Services. See Appendix E for a discussion of the Federal Reserve Board's PSR Policy. Certain payment and securities settlement systems, such as CHIPS and CLS, also rely upon Fedwire Funds Service to allow participants or their correspondents to provide necessary funding.CHIPS and CLS also use Fedwire Funds Service for settlement services by establishing zero-balance settlement accounts to settle clearinghouse participant obligations. The Federal Reserve Bank requires participants in a net debit position to make a Fedwire Funds Service funds transfer payment to the settlement

account. It then pays participants in a net credit position by means of a Fedwire Funds Service funds transfer from that settlement account. Once the Federal Reserve Bank processes these funds transfers, they are final and irrevocable.

Financial institutions sending a Fedwire Funds Service payment order irrevocably authorize their Federal Reserve Bank to debit (charge) their Federal Reserve account for the transfer amount and to give credit in the same amount to the payee. Only the originating financial institution can have funds removed from its Federal Reserve account using the Fedwire Funds Service. Depository institutions that maintain a reserve or clearing account with a Federal Reserve Bank may use Fedwire Funds Service to send payments to, or receive payments from, other account holders directly. Once the Federal Reserve Bank credits the receiving institution's account, it will not reverse the transaction at the request of the originating institution.

Financial institutions may access the Fedwire Funds Service via high-speed direct computer interface (CI), FedLine, or with off-line telephone connectivity with a Federal Reserve Bank. Financial institutions may also access certain Fedwire Funds Service inquiry information via FedLine for the Web.By year-end 2004, customers should be able to initiate Fedwire Funds Service and Fedwire Securities Service transactions through the web via FedLine Advantage. On-line participants, using either a CI or FedLine PC connection to Fedwire Funds Service, require no manual processing by the Federal Reserve Banks. Off-line participants provide funds transfer instructions to one of two Federal Reserve Bank customer support sites by telephone, and after authenticating the participant, the Federal Reserve Bank enters the transfer instruction into the Fedwire Funds Service system for execution. The manual processing required for off-line requests makes them more costly and suitable only for institutions processing a small number of funds transfer payment orders.

The Federal Reserve Bank's FedLine for the Web currently offers access to low-risk Federal Reserve Bank financial services. FedLine Advantage, which should begin a graduated rollout by year-end 2004, will allow depository institutions access to additional Federal Reserve financial services, including the Fedwire Funds Services and the Fedwire Securities Service, via a secure Internet Protocol (IP) gateway to Federal Reserve Bank financial services. Residing on a secure Web server, FedLine Advantage will be accessible to customer financial institutions with authenticated credentials using digital certificates.

CHIPS

CHIPS is a privately operated, real-time, multilateral, payments system typically used for large dollar payments. CHIPS is owned by financial institutions, and any banking organization with a regulated U.S. presence may become an owner and participate in the network. The payments transferred over CHIPS are often related to international interbank transactions, including the dollar payments resulting from foreign currency transactions (such as spot and currency swap contracts) and Euro placements and returns. Payment orders are also sent over CHIPS for the purpose of adjusting correspondent balances and making payments associated with commercial transactions, bank loans, and securities transactions.

Since January 2001, CHIPS has been a real-time final settlement system that continuously matches, nets and settles payment orders. This system provides real-time finality for all payment orders released by CHIPS from the CHIPS queue. To achieve real-time finality, payment orders are settled on the books of CHIPS against participants'

positive positions, simultaneously offset by incoming payment orders, or both. This process is dependant on up to two rounds of required prefunding.

To facilitate this prefunding, CHIP Co. members jointly maintain a pre-funded balance account (CHIPS account) on the books of the Federal Reserve Bank of New York. Under the real-time finality arrangement, each CHIPS participant has a pre-established opening position (or initial prefunding) requirement, which, once funded via a Fedwire Funds Service funds transfer to the CHIPS account, is used to settle payment orders throughout the day. [6] A participant cannot send or receive CHIPS payment orders until it transfers its opening position requirement to the CHIPS account. Opening position requirements can be transferred into the CHIPS account any time after the opening of CHIPS and Fedwire Funds Service at 9:00 p.m. Eastern Time. However, all participants must transfer their requirement no later than 9:00 a.m. Eastern Time.

During the operating day, participants submit payment orders to a centralized queue maintained by CHIPS. Participants may remove payment orders from the queue at any time prior to the daily cutoff time for the system (5:00 p.m. Eastern Time). When an opportunity for settlement involving one, two or more payment orders is found, the system releases the relevant payment orders from the central queue and simultaneously marks the CHIPS records to reflect the associated debits and credits to the relevant participant's positions. Debits and credits to the current position are reflected only in CHIPS records and are not recorded on the books of the Federal Reserve Bank of New York. Under New York law and CHIPS Rules, payments orders are finally settled at the time of release from the central CHIPS queue.

This process, however, typically will be unable to settle all queued messages. Soon after 5:00 p.m. Eastern Time, CHIPS tallies any unreleased payment orders remaining in the queue on a multilateral net basis. The resulting net position for each participant is provisionally combined with that participant's current position (which is always zero or positive) to calculate the participant's final net position; if that position is negative, it is the participant's "final position requirement."

Each participant with a final position requirement must transfer, via Fedwire Funds Service, this second round of prefunding to the CHIPS account. These requirements, when delivered, are credited to participants' balances. Once all of the Fedwire Funds Service funds transfers have been received, CHIPS is able to release and settle all remaining payment orders. After completion of this process, CHIPS transfers to those participants who have any balances remaining the full amount of those positions, reducing the amount of funds in the CHIPS account to zero by the end of the day. In the event that less than all final position requirements are received, CHIPS settles as many payments as possible, subject to the positive balance requirement, and deletes any remaining messages from the queue. Participants with deleted messages are informed of which messages were not settled, and may choose, but are in no way required, to settle such messages over Fedwire Funds Service.

Other Clearinghouse, Settlement, and Messaging Systems

National Settlement Service (NSS)

NSS is a multilateral settlement service owned and operated by the Federal Reserve Banks. It allows participants in private clearing arrangements to settle their net

obligations with same-day finality using participant's reserve or clearing account balances maintained at the Federal Reserve Banks. NSS participants include local check clearinghouse associations, automated clearinghouse (ACH) networks, credit card processors, and automated teller machine (ATM) networks.

To use NSS, a settlement agent transmits a settlement file electronically to a Federal Reserve Bank. The file contains a listing of the participants, the settlers (either the participant itself or the participant's correspondent), and the dollar amount of the debit or credit to be posted to the settler's account. If validity checks are satisfied, the Federal Reserve Bank accepts the file for processing and sends an acknowledgment to the agent. The Federal Reserve Bank accepts NSS files for processing and settlement between 8:30 a.m. and 5:30 p.m. Eastern Time. If an institution submits files earlier than 8:30 a.m. Eastern Time, they enter a queue for processing beginning at 8:30 a.m. Eastern Time. The NSS checks each debit balance on the settlement file against the account balance and intraday credit available to the settlers. The system may reject debit balances if a settler does not have a sufficient balance or sufficient intraday credit to cover the debit. Once it has posted all debit entries on the settlement file, NSS posts the credit balances. All transactions are final and irrevocable once the NSS posts them. The settlement for a file is complete when all credits have been posted. The NSS then sends an acknowledgment message to the settlement agent.

NSS offers payment finality similar to that of the Fedwire Funds Service and provides an automated mechanism for submitting settlement files to the Federal Reserve Banks. NSS improves operational efficiency and reduces settlement risk to participants by providing settlement finality on settlement day. It also enables the Federal Reserve Banks to manage and limit risk by incorporating risk controls similar to those used in the Fedwire Funds Service. NSS can settle transactions across Federal Reserve Districts or within a single Federal Reserve District.

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

International funds transfer operates differently from domestic large-value funds transfer. While the SWIFT operates as a messaging system, transmitting instructions to move funds, the domestic systems discussed above accomplish the actual funds movement.

SWIFT is an industry-owned cooperative, which supplies secure, standardized messaging services and interface software to 7,500 financial institutions in 199 countries. The SWIFT community includes a variety of financial services firms, including banks, broker/dealers, and investment managers, as well as their market infrastructures in payments, securities, treasury, and trade. The SWIFT core application is the FIN (Financial Transaction) application, which provides a store and forward financial messaging service accessed over X.25 network connections. [7] The system now uses bilateral key security and provides message validation to ensure messages are formatted according to SWIFT standards.

SWIFT messages may be used to transmit payment instructions for both domestic and international financial transactions. Financial institutions generating a high volume of funds transfer activity typically establish direct SWIFT connectivity with their internal, intrabank funds transfer system. The SWIFT network controls the integrity of the messages once properly entered at the point of origination. Thus there is no requirement for the receiver to re-verify payment orders. As a result, payment instructions pass through the system without human intervention unless programmed conditions (e.g., overdraft limit excesses) or error messages occur.

In 2002, SWIFT began migrating its core FIN application from an X.25 network to SWIFTNet, an IP-based network using the Secure Internet Protocol Network (SIPN). The introduction of IP-based technologies, that uses both bilateral keys and public keys, will allow SWIFT to expand its services. Payment-related business solutions currently being developed include cash reporting, bulk payments processing, and securities reporting. To promote the use of SWIFTNet and XML (Extensible Markup Language) based cash reporting tools among major cash clearing institutions and their correspondents, a working group has been set up to design the industry solution, including query/response standards and a rule book. In bulk payments, SWIFT developed a new XML-based message standard that was introduced in 2002.

Telex-based Messaging Systems

Several private telecommunications companies offer worldwide or interconnected services that provide a printed record of each transmitted message. Financial institutions that do not have access to SWIFT use Telex-based proprietary systems. Financial institutions access Telex-based systems via a dial-up or a dedicated line with dedicated printers. Some systems are computer monitored 24 hours a day, seven days a week and are fully redundant with automatic switch over and recovery capability.

Telex systems do not include built-in security features. Financial institutions that use Telex must exchange security codes. Typically, senders number messages sent to another institution to provide better audit controls. The sending institution is responsible for incorporating a test key in all instructions to a receiver to execute a payment order. The receiver is responsible for safekeeping the unique test code keys of each sender and decoding each test message. This function should be clearly separated from the Telex operating area and funds payment function. Presently, only a few institutions employ fully automated interface of Telex with their funds payment systems.

Continuous Linked Settlement (CLS) Bank

CLS Bank is a private sector special purpose bank that uses the CLS system to settle payments associated with a foreign exchange (FX) transaction simultaneously.

CLS is designed to eliminate the risk occurring when each leg of certain FX transactions is settled separately, i.e., the payment is made and the corresponding payment is not received. CLS Bank settles payment instructions in the following currencies: Australian Dollar, Canadian Dollar, Danish Krone, Euro, Japanese Yen, Norwegian Krone, Singapore Dollar, Swedish Krona, Swiss Franc, GB Pound, and U.S. Dollar, and is expected to add more currencies over time.

Customers may join CLS Bank as either a Settlement Member or User Member. Settlement members have accounts with CLS Bank and must sponsor User members that do not have such accounts. Any Settlement member or User member may submit payment instructions for settlement processing, but the sponsoring Settlement member must authorize each instruction a User member submits. Non-members may settle their FX payments through private arrangements with members who will submit the settlement processing instructions to the service. Such members are responsible to CLS Bank as principals with respect to such payment instructions.

Payment instructions are settled under the CLS Bank rules when it debits and credits the relevant Settlement members' accounts for the amounts involved. This final settlement will only occur within the context of several risk management tests.The risk management tests are: (1) any Short Position in respect to each currency would not exceed the relevant Settlement Member's Short Position Limit (adjusted based on the committed liquidity facilities available to CLS Bank for that day); (2) the Aggregate Short Position in the Settlement Member's Account, calculated as an equivalent U.S. dollar value, would not exceed the Aggregate Short Position Limit which is set for that Settlement Member; and (3) the sum of the Settlement Member's Long Positions and Short Positions (the "Account Balance"), adjusted by applicable Haircuts (the "Adjusted Account Balance), would not be negative. If any of these tests are not satisfied, no debits or credits will be made, and the pair of Settlement Eligible Instructions will remain on the settlement processing queue and be retested each time the queue is cycled through. The risk management tests will continue to be applied to all Settlement Eligible Instructions on the settlement processing queue until the applicable currency closing time has passed or all Settlement Eligible Instructions on the settlement processing queue have been settled. CLS Bank does not (i) guarantee the settlement of every payment instruction that is submitted for settlement or (ii) become a counterparty to any FX transaction referenced in a payment instruction that is submitted for settlement. In the event that a member is unable to provide its expected pay-in, other CLS members may be obligated to provide revised pay-in requirements.

Securities Settlement Systems

The major securities markets in the United States include the government securities market, the corporate equities and bond market, the market for money market instruments, and the municipal bond market. The instruments traded in these markets are generally traded through organized exchanges or through the over-the-counter dealer markets. Major categories of financial instruments commonly traded include U.S. Treasury securities, government agency securities, securities issued by federal government-sponsored enterprises, corporate equities and bonds, money market instruments such as commercial paper, and municipal (state and local) government securities. Participants in these markets include securities issuers; intermediaries such as brokers and dealers; and investors such as insurance companies, investment companies, non-financial corporations and individuals.

The mechanisms for clearing and settling securities transactions vary by market and type of instrument, and generally involve two types of specialized financial intermediaries: clearing corporations and securities depositories. Clearing corporations provide trade confirmation and comparison services, and multilateral netting of trade obligations; while, securities depositories transfer securities ownership on a gross or net basis against payment via book entry transfers.

Depository institutions play several important roles in securities clearing and settlement. Not only do depository institutions participate in clearing and settlement arrangements for themselves, they also act as custodians, issuing and paying agents, and settling banks for their customers. In addition depository institutions provide credit to clearing corporations, securities depositories, and clearing participants for routine and contingency purposes.

U.S. Government Securities

The U.S. government securities market encompasses all primary and secondary market transactions in securities issued by the U.S. Treasury, certain federal government agencies, and federal government-sponsored enterprises.Gove [8] Trading in government securities is conducted over the counter between brokers, dealers, and investors. In over-the-counter trading, participants trade with one another on a bilateral basis rather than on an organized exchange. Nearly all U.S. government securities are issued and transferred through a book-entry system operated by the Federal Reserve.

In the primary market, U.S. Treasury securities are issued through regularly scheduled auctions. The Federal Reserve Banks serve as conduits for the auctions, with the Federal Reserve Bank of New York coordinating much of the auction activity. Individuals, corporations and financial institutions may participate in the auctions. Participation in Treasury auctions, however, is typically concentrated among a small number of dealer firms, known as primary dealers. [9]

In the secondary market for government securities, trading activity takes place between primary dealers and non-primary dealers. Customers of these dealers are financial institutions, non-financial institutions and individuals. The majority of transactions between primary dealers and other large market participants are conducted through inter-dealer brokers that provide both anonymity and price information to market participants. Approximately 2,000 securities brokers and dealers are registered to operate in the U.S. government securities market.

Fixed Income Clearing Corporation (FICC)

FICC,FICC is a subsidiary of the Depository Trust and Clearing Corporation, a holding company that also includes the National Securities Clearing Corporation and the Depository Trust Company. In January 2003, the Mortgage-Backed Securities Clearing Corporation merged with the Government Securities Clearing Corporation to form the FICC. For further information about the Government Securities Division and the Mortgage-Backed Securities Division, see www.ficc.com. composed of the Government Securities Division (GSD) and the Mortgage-Backed Securities Division (MBSD), compares and nets trades of U.S. Treasury securities, agency debt securities, and mortgage-backed securities. As the name implies, GSD clears and nets U.S. government securities and agency debt securities. MBSD provides automated post-trade comparison, netting, risk-management, and pool notification services to the mortgage-backed securities market. Securities eligible for MBSD clearing are mortgage-backed securities issued by the Government National Mortgage Association (GNMA), the Federal Home Loan Mortgage Corporation (FHLMC), and the Federal National Mortgage Association (FNMA).

FICC uses real time trade matching; trade details are compared and matched as soon as

trade information is submitted. Successfully compared trades result in binding and enforceable obligations for settlement. Unmatched trades may be revised to achieve a trade match.

Successfully matched trades of eligible securities, for FICC netting service participants, are netted against offsetting net-receive or net-deliver obligation of the same security. Once the government securities net positions are determined GSD interposes itself between the original trading parties and becomes the legal counter-party to FICC members for settlement purposes. Therefore, GSD members' net settlement obligations are delivered to or received from GSD. MBSD, however, engages in multilateral position netting and does not stand in the middle of transactions. Final net settlement obligations of GSD and MBSD participants are settled through the Fedwire Securities Service via participants' settlement bank.

Fedwire Securities Service

As fiscal agents of the United States, the Federal Reserve Banks act as the securities depository for all marketable U.S. Treasury securities, many federal agency securities, and certain mortgage-backed securities issued by GSEs.The Federal Reserve also acts as agent and depository for the securities of certain international organizations, such as the World Bank. U.S. government securities are issued in book-entry form through the Federal Reserve's Fedwire Securities Service using either an auction process or dealer syndicate mechanisms. The Federal Reserve's Fedwire Securities Service provides for the safekeeping and transfer of these securities. The safekeeping function involves the records of securities balances, and the transfer and settlement function involves the transfer of securities between parties.

When book-entry securities transfers are processed using Fedwire Security Service, the institution sending the transfer receives immediate credit in its Federal Reserve (funds) account for the payment associated with the transfer, and its securities account is correspondingly debited. The Federal Reserve (funds) account of the institution receiving a book-entry securities transfer is debited for the payment amount, and its securities account is credited. There are more than 9,000 participants in the system and they are largely composed of depository institutions.

The Federal Reserve's Fedwire Securities Service is supported by a real-time, delivery-versus-payment (DVP) gross settlement system that provides for the immediate, final, and simultaneous transfer of securities against the settlement of funds. This system, known as the National Book-Entry System (NBES), provides for the safekeeping and transfer of U.S. Treasury, government agency, and GSE securities as well as securities issued by certain international organizations. The safekeeping function involves the electronic storage of securities records in custody accounts, and the transfer and settlement function involves the transfer of securities between parties.

Financial institutions may access the Fedwire Securities Service via high-speed direct CI, FedLine, or with off-line telephone connectivity with a Federal Reserve Bank. Financial institutions may also access certain Fedwire Securities Service inquiry information via FedLine for the Web. On-line participants, using either a mainframe or FedLine PC connection to Fedwire Securities Service, require no manual processing by the Federal Reserve Banks. Off-line participants provide funds transfer instructions to their Federal Reserve Bank by telephone, and once authenticated, the Federal Reserve Bank enters the transfer instruction into the Fedwire Securities Service system for execution. The manual processing required for off-line requests makes them more costly

and suitable only for institutions processing a small number of funds transfer payment orders.

Corporate and Municipal Securities

Corporate equities and bonds, commercial paper, and municipal bonds are traded on various established exchanges and on over-the-counter markets. The primary securities exchanges in the United States are the New York Stock Exchange, the American Stock Exchange, and the primary over-the-counter dealer market is the National Association of Securities Dealers Automated Quotations (NASDAQ).

The commercial paper market warrants special mention as it is an important source of short term funding for financial corporations and municipal governments. Commercial paper is a money market instrument issued by prime-rated non-financial and financial companies with maturities ranging from one to 270 days. Commercial paper is issued through dealer placements or direct placements with investors. Although commercial paper is a negotiable instrument, secondary market trading is limited. Disruption in the issuance of commercial paper can cause significant liquidity and credit concerns for issuers, many of whom are depository institutions and other financial companies, and depository institutions that provide issuing and paying agent services to issuers.

National Securities Clearing Corporation (NSCC)

NSCC, established in 1976, provides clearing and settlement services for corporate equities, corporate debt, municipal securities, mutual funds, annuities, and unit investment trusts. NSCC is a registered clearing corporation regulated by the Securities and Exchange Commission (SEC). With roughly 250 full-service participants, NSCC handles all aspects of the clearing and settlement of trades between brokers and dealers in securities traded on the over-the-counter markets, the New York Stock Exchange, the American Stock Exchange, and other regional exchanges.

Executed trades are typically reported to NSCC on trade date. Trades are either reported to NSCC by an established exchange as matched (irrevocable) trades or by brokers and dealers as unmatched trades. Trades submitted by brokers and dealers are compared and matched within NSCC's Continuous Net Settlement (CNS) system. Following the comparison process, NSCC becomes the legal central counterparty and guarantees completion of all securities trades following through CNS. CNS functions as an automated book-entry accounting system that centralizes the settlement of compared security transactions and maintains an orderly flow of securities and money balances.Further information about NSCC's clearing processes can be found at www.nscc.com.

Similar to the FICC netting process, successfully matched trades of eligible securities are netted against offsetting net-receive or net-deliver obligation of the same security.

Settlement of securities takes place at the Depository Trust Company and funds settlement occur over the Fedwire Funds Service through settlement banks.

Depository Trust Company (DTC)

DTC is a New York limited purpose trust company, a member of the Federal Reserve System, and a clearing agency registered with the SEC. DTC, the central securities depository for corporate equities and bonds, municipal government securities, and money market instruments, provides safekeeping and transfer of these securities. DTC participants include securities brokers, dealers, institutional investors, and depository institutions acting on their own behalf as well as functioning as custodians, issuing and paying agents, and settling banks for their customers.

Like Fedwire Securities, the safekeeping function involves the electronic recordkeeping of securities balances for participants, and the transfer function involves the transfer of securities between parties. DTC transfers securities on a gross basis throughout the day, while settling funds obligations on a net basis at the end of the day. During the transfer process, DTC will limit its credit exposure through participants' net debit caps. Any net debit position incurred by participants must be fully collateralized. End of day funds settlement occur over the Fedwire Funds Service through participants' settlement banks.Seewww.dtc.org for more information on DTC.

Intrabank Payment and Messaging Systems

Internally Developed and Off-The-Shelf Funds Transfer Systems

Action Summary

Financial institutions require efficient systems for transferring funds internally, among themselves, and with their customers for large-dollar payments relating to financial market transactions and settling corporate and consumer payments.

Management and the board should:

- Establish dual controls and separation of duties for funds transfer systems;
- Monitor and log access to funds transfer systems, maintaining an audit trail of all sequential transactions; and
- Incorporate the funds transfer controls into the organization's information security program to ensure the integrity and confidentiality of customer information.

Financial institutions rely on internal funds transfer systems and networks to send payment instructions to their correspondents for the transfer of correspondent balances or to initiate Fedwire Funds Service or CHIPS payments. Large financial institutions have either developed their own funds transfer systems or relied on off-the-shelf funds transfer systems. In either case, the internal financial institution funds transfer systems interface with Fedwire Funds Service and CHIPS, supporting the interface and transaction format specifications for the transmission of payment orders. Off-the-shelf funds transfer systems typically support a variety of treasury, cash management, and straight-through-processing (STP) modules, which automate payment order processing.

The Federal Reserve Banks provide the Computer Interface Protocol Specifications (CIPS) that funds transfer and book-entry securities systems need to adopt in order to implement a CI connection successfully. The Federal Reserve provides a website with a list of vendors who have completed the Federal Reserve Banks' protocol certification process. [10] The Federal Reserve Banks do not endorse any specific software vendor or product. The Federal Reserve Banks make no warranties or representations with respect to any of the products offered by these vendors except that communication-level software correctly executes systems network architecture (SNA) commands as specified in the CIPS.

Payment Messaging Systems

Financial institutions, corporations, and other organizations employ wholesale payment message systems to originate payment orders, either for their own benefit or for a third party. These systems are indispensable components of funds transfer activities. Unlike payment systems, which transmit actual debit and credit entries, message systems process administrative messages and instructions to move funds. The actual movement of the funds is then accomplished by initiating the actual entries to debit the originating customer's account and credit the beneficiary's account at one or more financial institutions. If the beneficiary's account or the beneficiary institution's account is also with the originator's institution, the institution normally handles the transaction internally through a book transfer. If the beneficiary related accounts are outside the originating customer's institution, the parties will complete the transfer by use of a payments system such as Fedwire Funds Service or CHIPS. The means of arranging payment orders range from manual methods (e.g., memos, letters, telephone, fax, or standing instruction) to electronic methods using telecommunications networks. These networks may include those operated by the private sector, such as SWIFT or Telex, or operated internally by or for the institution. The internal networks can be for inter-company purposes only or connected to customer sites.

Since the payment order is the institution's authorization to act on behalf of the customer, it is imperative that a system is in place to establish the authenticity and time of receipt of the order. These two elements are the primary components cited by the Uniform Commercial Code Article 4A (UCC4A) in establishing responsibility for the execution of a payment order. Even though the transfers initiated through systems such as SWIFT and

Telex do not result in the immediate transfer of funds from the issuing institution, they do result in the issuing institution having an immediate liability, which is payable to the disbursing institution. Therefore, the physical and logical controls surrounding payments messaging systems should include:

- Physical controls limiting access to only those staff members assigned responsibility for managing the payment messaging system;
- Logical access controls restricting access on a need to know basis;
- Assigning access to payment messaging application and data based on functional job duties and requirements; and
- Identification and authentication controls used to authenticate access to payment messaging systems.

In-house Terminals

Some financial institutions employ terminals, connected via telecommunications networks with customers and the institutions' operating departments, to execute funds payment orders. These systems may be dial-up or dedicated lines and are often fully interfaced to the institution's funds payments system. The primary security method is the use of unique passwords for each user of the system. Since there is often no intervention by the funds payment operation, it is necessary to establish controls directly in the area employing the terminals. These controls should cover origination, data entry, and release, and should be the same as those associated with an independent funds payment function.

Non-automated Payment Order Origination

While in-house terminals are the primary sources for payment order origination, less complex institutions still rely heavily on memos, letters, telephone, fax, or standing instructions. (Note: standing instructions are normally maintained in the automated funds transfer system as recurring transfers and should be subject to the same input/ verification controls as wires when first entered into the system). It is imperative that an institution using these payment order methods has a viable security program, which includes:

- Maintaining signature lists for use with internally and externally generated memos, letters, or fax instructions. As noted in UCC4A Section 201, signature verification alone is not defined as a security procedure; however, institutions may use it with other security devices such as call backs or codes.
- Call back to authorized individuals for both internally and externally generated telephone instructions.
- Procedures covering standing instructions protecting against unauthorized change, periodic review to validate accuracy, and ensuring execution under the agreed

terms.

Funds Transfer Operations (Wire Room)

A financial institution's funds transfer operation (wire room) is responsible for originating, transmitting, and receiving payment orders. In less complex financial institutions, the wire room typically includes a FedLine PC. [11] Less complex institutions may also have a core banking package that includes a funds transfer module, which generates payment orders in a Fedwire Funds Service format for uploading to the FedLine PC. Staff assigned responsibility for these activities are generally responsible for other duties and are not typically dedicated full-time to the wire room function. In most financial institutions, funds transfer payment order volume does not justify the costs associated with a full time staff, and the sending and receiving of payment orders may be a part-time responsibility for one or more people. For less complex financial institutions, a complete separation of duties may be difficult to achieve, and compensating controls, including rotation of duties and internal review procedures covering those payment orders requiring officer review, should be considered.

Financial institutions generating significant payment order volume usually have a separate funds transfer department with dedicated staff. Financial institutions generating a large volume of high value Fedwire Funds Service payment orders typically use dedicated funds transfer software (developed in-house or purchased) connected via computer interface to the Federal Reserve Bank's Fedwire Funds Service application. The software used for wire transfers automatically posts transactions to the demand deposit account and general ledger. The automated function provides an efficient means to process a large number of payment orders supporting a variety of business lines.

Payment orders can be received from several different sources including business areas within the financial institution, as well as from corporate and individual customers. Payment orders can be initiated by phone, fax, and online systems. Individuals wishing to wire funds typically do so at the teller window or contact their loan officer or account representative. Payment order verification is an important safeguard, and institutions should, at a minimum, keep accurate records of all payment order requests, including those initiated by telephone. Institutions should record all phone calls initiating payment orders for security and audit reasons. The institutions should maintain the tapes for at least a 30-day period.

After receiving a payment order, the wire room operator keys the payment order into FedLine (or the payment order is generated through the use of a third-party software product funds transfer module). Before sending a payment order to the Federal Reserve Bank, a second staff member should verify it for accuracy and authorization. Most FedLine PCs have two printers attached, one that prints copies of all outgoing payment order Fedwire Funds Service messages and another that prints incoming Fedwire Funds Service payment order messages. Institutions should maintain a record of all payment orders for record keeping purposes. The unbroken printout sheet helps ensure a complete record of all messages; however, institutions should also verify the sequence numbers of the messages to identify missing records due to communication problems. The sequence number provides an audit trail for all funds transfers on the Fedwire Funds Service system.

The institution should have appropriate procedures in place to verify all processed payment orders. These procedures usually include the use of code words, call backs,

and corporate resolutions authorizing certain employees to send payment orders. Verification and security procedures are extremely important in light of the potential for fraud or errors.

A Fedwire Funds Service message is generated either by the application supporting the business line or by an authorized wire room employee who enters the message into an on-line terminal. Before transmitting the wire, it is sent to a second terminal for an independent employee to verify for accuracy as well as proper authorization. Only after a second staff member reviews the payment order should a financial institution send it to the Federal Reserve Bank for processing.

This separation of duties is important to ensure security. The institution's internal funds transfer system should maintain data on each day's transfers, including wires sent and received, wires listed by amount, wires listed by sequence number, and wires listed by account holder. Most software systems maintain the work of several previous days, often the last 5 to 7 days, to allow on-line access to trace errors and problems. After the 5 to 7 days, the data is typically archived.

Computer and Network Operations Supporting Funds Transfer

Wholesale funds transfer systems are high risk. Therefore, management should configure hardware and software components to control access and support effective monitoring. Management should develop change management procedures to ensure the integrity of the hardware configurations and applications software. Operations personnel should have the appropriate procedures to manage critical payment systems software.

Applications should employ strong user authentication, support user entitlement (information access and function controls) administration, and provide audit trails in sufficient detail to support the analysis or investigation of specific transactions. Management should enable funds transfer activity logs and designate independent staff members to monitor operations, applications support, system administration, and security administrators' activities associated with the funds transfer system.

Telecommunications systems employed for EFT can range from a dial-up connection between the institution and payments system (e.g., FedLine) to terminal connections with institution staff and customers that transmit institution's funds transfer system payment orders directly to Fedwire Funds Service via CI connection. An institution's information security program should include access, authentication, and transmission controls surrounding wire room activities and all terminal connections. Access and authentication controls may consist of personal identification numbers, passwords, or other identifying keys such as account numbers, balances, or other financial data. Financial institutions should use encryption as a means of protecting data throughout the EFT system. Encrypting data during transmission allows institutions to scramble the contents of message/payment orders during transmission and limit the value of the information to an interloper even if a transmission is intercepted. Nevertheless, financial institutions should monitor or prevent access to funds transfer activity by data processing personnel who

have access to communications equipment and can monitor and record data flowing in clear text from encryption devices.

Wholesale Payment Systems Risk Management

Payments System Risk (PSR) Policy

Given the role of payments and securities settlement systems as critical components of the nation's financial system, the Federal Reserve Board has developed a policy to foster the safety and efficiency of these systems.The regulatory agencies have also issued interagency and agency-specific policies on payments and payment system risk. The "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial Sys-tem," for example, identifies sound practices focusing on minimizing the immediate systemic effects of a wide-scale disruption to critical financial markets. The sound practices discussed in this paper supplement the agen-cies' respective policies and other guidance on business continuity planning. See http://www.federalreserve.gov/paymentsystems/psr_policy.htm

One major component of the Federal Reserve's policy addresses the extent to which institutions with Federal Reserve accounts are allowed to have daylight overdrafts in that account. Additional information about this aspect of the PSR policy is provided in Appendix E. A daylight overdraft occurs when an institution's Federal Reserve account is in a negative position during the business day. Negative balances typically occur when there are insufficient funds in an institution's account to cover outgoing Fedwire funds transfers, incoming book-entry securities transfers, or other payment activity processed by a Federal Reserve Bank. The PSR policy applies a series of limits and incentives to control the Federal Reserve Banks' exposures to the credit risk associated with these daylight overdrafts. Limits on net debit positions are sufficiently flexible to reflect the overall financial condition and operational capacity of each institution using Federal Reserve Bank payment services.

Institutions with the highest net debit caps are subject to an annual self-assessment process that is outlined in the "Guide to the Federal Reserve's Payments System Risk Policy."http://www.federalreserve.gov/paymentsystems/psr_policy.htm In addition to an analysis of the institution's general creditworthiness, institutions eligible for a self-assessed cap should manage and control their intraday funds positions, maintain credit policies and controls at the customer level, and employ operational controls and contingency plans. In particular, institutions with self assessed caps need to be able to monitor and control the intraday credit they extend to their customers. Such credit has the potential to result in Federal Reserve daylight overdrafts for the institution. The risks associated with customers' daylight overdrafts are discussed below.

Another major component of the PSR policy provides expectations for risk management in payments and securities settlement systems, and adopts international standards for systemically important systems.See http://www.federalreserve.gov/paymentsystems/psr_policy.htm for details and further references. This portion of the policy is directed at system operators, but contains key information about the risks that such systems present to system participants, and in some cases, requires covered systems to provide participants with clear information about these risks. Moreover, examined institutions may have an important role in the governance of wholesale payments and securities settlement systems, as many private sector systems are owned by their participant

financial institutions.

Reputation Risk

Reputation risk is the risk that potential negative publicity regarding a financial institution's business practices could cause a decline in the customer base, costly litigation, or revenue reductions. Reputation risk is relevant to wholesale payment systems because of the large dollar value of the transactions. Errors or fraud can have serious ramifications on the public perception of a financial institution.

Management can mitigate reputation risk for wholesale payment systems by having an effective public relations program, by developing and maintaining strong customer relationships, and by enacting adequate internal controls over all aspects of the wholesale payment system so that errors do not happen in the first place.

Strategic Risk

Credit Risk

Credit risk is the risk that a counter party will not settle an obligation for full value when due. In relation to wholesale payments and securities settlement systems, credit risk can take several forms and have multiple sources. Two of the most important sources, customer daylight overdrafts and settlement risks (including settlement lags, principal risk, and loss-sharing provisions), are discussed below. These forms of credit risk, as well as other forms of credit risk, should be appropriately monitored and managed. Information technology is often critical to such controls.

Customer Daylight Overdrafts

Financial institutions often permit their individual and corporate customers to incur intraday overdrafts by allowing customers to make payments without available balances. In most cases, overdrafts are eliminated with incoming funds transfers from other institutions (or outgoing securities transfers against payment) by the end of the business day.

Financial institutions engaging in this practice are extending credit to their customers. As such, they should monitor the credit position of individual customers; control the amount of intraday credit extended to each customer; and have guidelines to prevent exceeding approved intraday and overnight overdraft limits. These guidelines should include:

- Reviewing customer credit limits and the frequency and scope of internal credit reviews. In the absence of pre-authorized limits, institutions should have a process for management approval of daylight overdrafts. Authorization should be within the lending authority of approving officers.
- Reporting and approval procedures for payments exceeding established credit limits to ensure officers with sufficient lending authority make approvals.
- Reviewing intraday overdrafts incurred for compliance with established limits as well as approval and reporting requirements.
- Reviewing arrangements/agreements regarding collateralization of credit exposures.

To the extent that these guidelines give consideration to projected incoming payments, the financial institution should be aware of the risk that expected payments may not be received when expected. Moreover, as described below, institutions should also consider whether such payments have been or are expected to be made with finality.

Since daylight overdrafts constitute an extension of credit (no matter the period of time involved), financial institutions' credit policies should include provisions for approving and monitoring intraday credit lines to customers. Daylight overdrafts have the potential to become overnight overdrafts or overnight loans, and institutions should also have procedures to determine limits on overnight overdrafts. Both sets of procedures should be similar to loan portfolio credit analysis. Credit policies and procedures should include:

- Analyzing worthiness of all borrowers with amounts outstanding in excess of the credit line.
- Reviewing reporting and approval procedures for overdrafts and settlement credits exceeding established limits.
- Assessing reporting and approval procedures for payments against uncollected funds.

Depending on the creditworthiness of the customer and the nature of the activity, a financial institution should consider requiring customers to advise the institution of anticipated incoming securities transfers. Financial institutions should also consider requiring the customer to pre-fund all such anticipated transfers, with the understanding that any transfers not pre-funded may be reversed. To further mitigate credit risk, management should consider requiring customers to collateralize intraday overdrafts. As mentioned above, the control of customers' daylight overdrafts is one of several elements of the Self-Assessment process set out in the Board's PSR policy (see Appendix E).

Settlement Risk

In addition to the explicit provision of credit via daylight overdrafts, financial institutions also need to control their exposure to settlement risks incurred through the institutions' participation in interbank payment and settlement systems. In general, settlement risk is the possibility that the completion or settlement of individual transactions or settlement at the interbank funds transfer or securities settlement level more broadly, will not take place as expected. In addition to credit risk, settlement risk often includes elements of liquidity risk.

One important source of settlement risk is any time lag between the origination of the payment or securities settlement instructions and final settlement, and discharge of those instructions. This time difference between the delivery of payment details and payment finality, or settlement lag, creates the possibility that sending institutions could fail during the lag or at least not be able to settle their obligations when due, typically at the end of the day. If the receiving bank credits the anticipated payment proceeds to the customer's account before the payment is final, the receiving bank may be exposed to credit risk from the sending bank until final settlement occurs. As long as final settlement has not occurred, any credits or additional payment activity undertaken on the basis of "unsettled" payment messages results in credit risk.For more information, see "Real-time Gross Settlement Systems," Committee on Payment and Securities Settlement Systems, 1997 at www.bis.org/publ/

cpss22.pdf. Financial institutions should analyze and control this credit risk as they would any other extension of credit.

Real-Time Gross Settlement systems, such as Fedwire Funds Service, are not subject to this risk as payments credited to a receiver's account are final at the time of receipt. CHIPS payments were previously subject to this kind of risk. However, starting January 2001, CHIPS began sending payment details to the receiving bank only once a payment became final.Receiving banks may, however, request certain details about payments queued for their receipt. Such informa-tion should not be treated as a final payment. Securities settlements that occur at DTC may be subject to this kind of risk.

Another form of settlement risk is caused by a time-lag between the final settlement of two sides of a given trade or transaction (e.g., any difference in timing between the payment for and delivery of securities, or for foreign exchange transactions, the final delivery of one currency prior to the other). Such time lags can put the entire principle value of trades at risk. Several payments and securities settlement systems, including DTC and CLS Bank are designed to avoid this risk. Nonetheless, many foreign exchange transactions are not settled in CLS Bank, and may be subject to this type of settlement risk. Securities settlement systems in other countries in which U.S. institutions participate may also be subject to this form of risk.

Finally, many payments and securities settlement systems, especially those that rely on settlement lags, netting, or intraday credit, often implement various forms of risk controls that have important credit risk implications for system participants. In particular, systems often employ various types of loss-sharing and supplemental liquidity requirements in the event of settlement failures or disruptions. Participants in any payment or securities settlement system should understand the risks related to these settlement failure procedures and should be prepared to make any required supplemental payments of loss allocation assessments as described in the system rules. Financial institutions may also pre-arrange to serve as liquidity providers to payment or securities settlement systems in the event of a settlement disruption. These liquidity arrangements may involve committed lines of credit on either a secured or unsecured basis or foreign exchange swap facilities. Institutions should understand the nature of these special

commitments and be well-prepared to act on them.

Liquidity Risk

Liquidity risk involves the possibility that earnings or capital will be negatively affected by an institution's inability to meet its obligations when they come due. Liquidity risk is the risk that the financial institution cannot settle an obligation for full value when it is due (even if it may be able to settle at some unspecified time in the future). Liquidity problems can result in opportunity costs, defaults in other obligations, or costs associated with obtaining the funds from some other source for some period of time. In addition, operational failures may also negatively affect liquidity if payments do not settle within an expected time period. Until settlement is completed for the day, a financial institution may not be certain what funds it will receive and thus it may not know if its liquidity position is adequate. If an institution overestimates the funds it will receive, even in a system with real-time finality, then it may face a liquidity shortfall. If a shortfall occurs close to the end of the day, an institution could have significant difficulty in raising the liquidity it needs from an alternative source.

Systems that postpone a significant portion of their settlement activity (in dollar terms) toward the end of the day, such as CHIPS, may be particularly exposed to liquidity risk. These risks can also exist in RTGS systems such as Fedwire. As mentioned above, systems or markets that pose various forms of settlement risk also pose forms of liquidity risk. CLS Bank, while eliminating the bulk of principle risk through its payment-versus-payment design, retains significant liquidity risk, as funding is made on a net basis, and pay-in obligations may need to be adjusted in the event that a counterparty is unable to fund its obligations. Other systems, including securities settlement systems, may also be subject to liquidity risks.

To manage and control liquidity risk, it is important for financial institutions to understand the intraday flows associated with their customers' activity to gain an understanding of peak funding needs and typical variations. To smooth a customer's peak credit demands, a depository institution might consider imposing overdraft limits on all or some of its customers. Moreover, institutions must have a clear understanding of all of their proprietary payment and settlement activity in each of the payment and securities settlement systems in which they participate.

Legal (Compliance) Risk

Legal/compliance risk arises from an institution's failure to enact appropriate policies, procedures, or controls to ensure it conforms to laws, regulations, contractual arrangements, and other legally binding agreements and requirements. In particular, legal risks can result if a financial institution does not provide adequate attention to the operating circulars, procedures and rules of the payment and settlement systems in which it participates. Similarly, an institution's contractual relationships with customers, counterparties, and vendors must be sound and appropriate to the relevant legal framework(s) such as payment and bankruptcy frameworks. Contracts, among financial institutions, their customers, and counterparties are also important to allocate risk-sharing responsibilities applicable to payments. Finally, an institution must ensure it is in compliance with all applicable Federal and State laws and regulations governing payments activity, including the Bank Secrecy Act, the USA PATRIOT Act, and laws

regarding economic sanctions Appendix D provides details on the general legal framework for payments and securities settlement systems.

Office of Foreign Assets Control (OFAC)

The Office of Foreign Assets Control (OFAC), an agency of the U.S. Treasury, administers a series of laws imposing economic sanctions against targeted hostile foreign countries to further U.S. foreign policy and national security objectives. The U.S. government exercises economic sanctions through trade embargoes, blocked assets controls, travel bans, and other commercial and financial restrictions. The economic sanctions programs of the U.S. government are powerful foreign policy tools. Their success requires active participation and support of every financial institution. The Secretary of the Treasury manages the sanctions for the U.S. The U.S. Government mandates that all financial institutions located in the U.S., overseas branches of U.S. financial institutions, and, in certain instances, overseas subsidiaries of U.S. financial institutions, comply with economic sanctions and embargo programs administered under regulations issued by OFAC. In general, the regulations:

- Block accounts and other assets of countries identified as being a threat to national security by the President of the United States (this always involves accounts and assets of the sanctioned countries' governments; it may also involve nationals of the sanctioned countries). In addition, OFAC also blocks the accounts of individuals on OFAC's Specially Designated Nationals (SDN) listing who may not be associated with a sanctioned country.
- Prohibit unlicensed trade and financial transactions with such countries. U.S. law requires that assets and accounts be blocked when such property is located in the U.S., is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. The definition of assets and property is very broad and covers direct, indirect, present, future, and contingent interests. Certain individuals and entities located around the world that are acting on behalf of sanctioned country governments have been identified by the U.S. Treasury and must be treated as if they are part of the sanctioned governments. U.S. banks must block funds transfers that are remitted:

  - By, or on behalf of a blocked individual or entity;

  - To, or through a blocked entity; or

  - In connection with a transaction in which a blocked individual or entity has an interest.

Financial institutions receiving instructions to make a payment that falls into one of these categories are required to execute the payment order and place the funds into a blocked account. Customers cannot cancel or amend a payment order after the U.S. bank has received it. Once assets or funds are blocked, they may be released only by specific authorization from the U.S. Treasury. If OFAC compliance issues are found during an

examination, the examiner should follow up with the bank regulatory agency's compliance area to determine whether the financial institution needs to acquire subject matter expert support. [12]

Bank Secrecy Act (BSA)

Financial institutions should develop and provide for the continued administration of a program reasonably designed to ensure and monitor compliance with the record keeping and reporting requirements set forth in subchapter II of the Bank Secrecy Act. [13] The BSA requires a written compliance program that is approved by the board of directors. The board must note the approval in the board minutes. The compliance program must include, at a minimum:

- Provision for a system of internal controls to ensure ongoing compliance;
- Provision for independent testing for compliance to be conducted by institution personnel or by an outside party;
- Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance, and
- Provision for training for appropriate personnel.

USA PATRIOT Act

On October 26, 2001, the President signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. The USA PATRIOT Act contains strong measures to prevent, detect, and prosecute terrorism and international money laundering. The provisions of the USA PATRIOT Act that most affect financial institutions are those contained in Title III. Among other things, Title III amends the Bank Secrecy Act and provides the Treasury Department and federal agencies with enhanced authority to combat international money laundering and block terrorist access to the U.S. financial system.

The Act is far-reaching in scope, covering a broad range of financial activities and institutions. One such provision is section 312 - Due Diligence for Correspondent and Private Banking Accounts. Section 312 requires a U.S. financial institution that maintains a correspondent account or private banking account for a non-U.S. person to establish appropriate and, if necessary, enhanced due diligence procedures to detect and report instances of money laundering. Section 312 also describes specific enhanced due diligence standards for U.S. financial institutions that enter into correspondent banking relationships with foreign banks operating under offshore banking licenses or under banking licenses issued by countries that have been:

- Designated as non-cooperative with international anti-money laundering principles by an international body (such as the Financial Action Task Force) with the concurrence of the U.S. representative to that body, or
- The subject of special measures imposed by the Secretary of the Treasury under section 311 of the USA PATRIOT Act.

In addition, section 312 describes minimum anti-money laundering due diligence standards for the maintenance of private banking accounts by U.S. financial institutions for non-U.S. persons. The Treasury Department (Treasury) is authorized to issue regulations implementing section 312. The Act provides that the provisions of section 312 became effective July 23, 2002, whether or not final regulations were in place. Because of the complexity of the issues raised by the proposed rule, Treasury did not promulgate a final rule by July 23, 2002, but rather issued an interim final rule that was effective immediately. The interim final rule requires that insured depository institutions, U.S. branches and agencies of foreign banks, and Edge and Agreement corporations comply with the statutory requirements of section 312.

The interim final rule also provides compliance guidance to financial institutions. This guidance, which is set forth in supplementary information and not as a regulation, indicates what Treasury would consider as "reasonable" due diligence policies and procedures pending the issuance of a final rule. According to Treasury's guidance, these policies and procedures include (1) focusing on accounts that pose the highest risk of money laundering, (2) according priority to those accounts opened on or after July 23, 2002, and (3) complying with existing best practice standards for banks, such as those issued by the Wolfsberg Group in May 2002, the Clearing House in March 2002, and the Bank for International Settlements in October 2001. Treasury noted that it would be reasonable for an institution not to apply every best practice standard if it has a justifiable basis for not adopting a particular practice.

Until Treasury issues a final rule implementing section 312, examiners should make certain covered banking organizations are aware of the specific provisions of the law and have reasonable policies and procedures in place to assure and monitor compliance. Also, in accordance with existing practices concerning anti-money laundering related matters, examiners should ensure that a banking organization is in compliance with the terms of section 312.

Operational (Transaction) Risk

In the context of payment systems, operational risk is the risk of loss resulting from inadequate or failed internal processes, systems, and staff, or from external events. Operational risk includes various physical and information security risks. Institutions should address operational risk by adopting the appropriate internal and operating controls, information security policies and controls, operational resiliency policies and resources, and by comprehensively and effectively auditing these policies, controls, and resources. Institutions should ensure all policies, controls, and resources are sufficient to meet all regulatory expectations. [14]

Internal and Operational Controls

Management should consider implementing a variety of specific measures to mitigate or limit operational risks, such as authentication and encryption techniques to ensure the authenticity of the payer and payee as well as prevent unauthorized access to information in transit; and edit checks and automated balancing to verify the integrity of the information relative to the payment order and funds transfer transaction. Additional controls include the use of certified tamper resistant equipment, logical access controls to verify transactions, verification of account balances, and the logging of all transactions and attempts to make a transaction.

Additional internal control measures that management should employ to mitigate wholesale payment system risk include:

- Dual custody and separation of duties for critical payment transaction processing and accounting tasks;
- Payment data verification;
- Clear error processing and problem resolution procedures; and
- Confidential and tamper resistant mailing procedures for bankcards and other sensitive material.

The operational controls for funds transfer operations require clearly defined procedures establishing a control environment which provides for the authorization and authentication of transactions. Financial institutions should establish effective operational controls that identify and document:

- The original payment instructions from the corporate or individual customer to the financial institution and other pertinent information (e.g., account officer, branch manager, terminal entry identity, automated interface identification);
- Every transfer point of data for each step of the manual process (e.g., account officer, message receipt, authentication, data entry, and payment release); and
- Every transfer point of data for each step of an automated process (e.g., SWIFT and Telex, message preparation, data entry, and payment release).

Basic internal controls should be in effect to maintain overall integrity for any funds transfer operation. However, depending on the complexity and volume of operations, certain steps may not be applicable for some institutions. Recommended control objectives for a wholesale funds transfer system include:

- Verifying the accuracy and completeness of the outgoing instruction;

- Protecting original instructions from loss or alteration;
- Authenticating the identity and authority of the sender;
- Ensuring collected balances are available and held for the outgoing payments;
- Ensuring the original unaltered outgoing instruction is entered into the internal accounting system;
- Maintaining a physically secure environment; and
- Maintaining appropriate separation of duties for employees involved in the payment process.

Financial institutions should have funds transfer policies and procedures addressing both the processing of funds transfer messages and the related standards for creating and maintaining source documents. Policies and procedures should include documentation describing all interfaces between the funds transfer application and other back office and customer-related banking processes, and should address the controls relating to crediting, debiting, and reconciling customer and institution account balances. Policies and procedures should also document institution specific compliance requirements to address federal and state regulations including OFAC verification procedures.

Audit

A financial institution's internal auditors should conduct periodic independent reviews of the funds transfer operation, including all pertinent internal policies and procedures. An external audit can supplement or replace internal audit procedures. Financial institution audits should verify the effectiveness of the funds transfer control environment and identify funds transfer deficiencies for correction.

Examiners should perform an evaluation of the institution's audit function to determine whether audit activities related to funds transfer operations are comprehensive and effective. Examiners also should review the auditor's opinion of the adequacy of accounting records and internal controls for funds transfer operations. The review of audit procedures should focus on:

- The scope and frequency of the internal funds transfer audit program;
- The effectiveness of audit procedures in determining any control/operating problems disclosed since the previous examination and what corrective measures management has taken;
- Audit work papers to ensure they document adherence to prescribed audit procedures;
- IT audit coverage of new system enhancements and development projects; and
- External audit findings and recommendations.

Information Security

A financial institution's information security program should include an effective risk assessment methodology that includes an evaluation of risks relating to performing high-risk activities such as funds transfer and other payment-related activities. Management should use risk assessments based on a periodic review of high-risk activities to develop effective standards for adequate separation of duties, physical security, and logical access controls based on the concept of "least possible privilege." Refer to the IT Handbook's Information Security Booklet for more detail.

Management should establish logical access controls on the funds transfer application that assign appropriate access levels to staff members working in the wire room or funds transfer operation. Inappropriate access levels provide the opportunity to create and transmit unauthorized funds transfer messages. The risk is greater without adequate separation of duties. Management should ensure no employees have access to more than one assigned user code unless the code is under dual control. Management should configure message verification rights to ensure adequate separation of duties between employees initiating and employees verifying and sending funds transfer messages.

Business Continuity Planning (BCP)

Financial institutions should recognize their role in supporting systemic financial market processes (e.g., inter-bank payment systems and key market clearance and settlement activities) and understand that service disruptions at their institution may significantly affect the integrity of key financial markets. Critical markets include, but are not limited to, the markets for federal funds, foreign exchange, commercial paper, and government, corporate, and mortgage-backed securities. Firms that play significant roles in critical financial markets are those that participate in sufficient volume or value such that their failure to perform critical activities by the end of a business day could present systemic risk (see Appendix F).

In addition, financial institutions should coordinate BCP development and testing with all applicable third parties. All financial institutions, especially those that play a major role in critical financial markets, are expected to have sufficient business continuity plans, commensurate with their funds transfer activities. Financial institutions should also coordinate testing with other industry participants. Refer to IT Handbook's Business Continuity Planning Booklet for more detail.

Vendor and Third-Party Management

Some financial institutions rely on third party service providers and other financial institutions for wholesale payment system products and services either to enhance the services performed in-house or to offer wholesale payment services that are otherwise not cost effective.

Financial institutions should have adequate due diligence processes, appropriate contract provisions, and service provider monitoring procedures to ensure they conduct wholesale payment operations appropriately. Effective monitoring should include the review of select wholesale payment transactions to ensure they are accurate, reliable,

and timely. The integrity and accuracy of wholesale payment transactions depend on the use of proper control procedures throughout all phases of processing, including outsourced functions.

Regardless of whether the financial institution's control procedures are manual or automated, internal controls should address the areas of transaction initiation, data entry, computer processing, and distribution of output reports. Financial institutions should also maintain effective control over service provider access to customer and financial institution information consistent with GLBA 501(b). Contractual provisions should define the terms of acceptable access and potential liabilities in the event of fraud or processing errors. Refer to IT Handbook's Outsourcing Technology Services Booklet for more detail.

Endnotes

[1]	For further information on these topics, refer to the Committee on Payment and Settlement Systems (CPSS) "Recommendation for Central Counterparties," at www.bis.org.
[2]	FedLine® is a registered trademark of the Federal Reserve Banks.
[3]	In addition, FedwireFedwire® is a registered service mark of the Federal Reserve Banks. See http://www.frbservices.org/ for fur-ther information on Fedwire Funds and Securities Service, and NSS.
[4]	CHIPS is a private multilateral settlement system operated by CHIP Co., a subsidiary of The Clearing House (formerly known as the New York Clearing House Association).
[5]	See Appendix D for a discussion of the general legal framework for interbank payment systems.
[6]	CHIP Co., using a formula based on the latest transaction history of each participant, establishes the amount of a participant's opening position requirement.
[7]	X.25 is the software that SWIFT provides to its users for access capability to SWIFT's core FIN application.
[8]	rnment-sponsored enterprises (GSEs) are publicly-traded corporations created by Congress to address public policy concerns about the ability of members of certain groups to borrow sufficient funds at affordable rates. GSEs do not receive federal funds and rely primarily on debt financing for their day-to-day operations. GSE securities are not government securities; however, market participants rate and price GSE securities similar to U.S. government-issued securities.
[9]	Primary dealers are designated trading counterparties for the Federal Reserve Bank of New York in its execu-tion of market operations to carry out US monetary policy. Currently there are 23 designated primary dealers.
[10]	Refer to http://www.frbservices.org/Wholesale/ ProtocolCertVendors.cfm for a list of protocol certified ven-dors.
[11]	See the IT Handbook's, "FedLine Booklet."
[12]	For a complete discussion of legal requirements, consult 31 CFR Part 500 et seq.
[13]	Chapter 53 of title 31, United States Code, the Bank Secrecy Act, and the implementing regulations promul-gated by the Department of Treasury at 31 CFR part 103.
[14]	See Appendix F for a discussion of the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System."

[15]	See SR Letter 03-9, dated May 28, 2003, Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, for further information. The agencies included the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.
[16]	Federal Reserve Operating Circulars are available at http://www.frbservices.org/OperatingCirculars/index.html.
[17]	See http://www.federalreserve.gov/paymentsystems/psr/default.htm.
[18]	See IT Handbook "Retail Payment Systems Booklet" for additional information on NSS and PSR policy.
[19]	See SR Letter 03-9, dated May 28, 2003, Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, for further information. The agencies included the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.

Appendix A: Examination Procedures

Tier I Examination Objectives and Procedures

EXAMINATION OBJECTIVE: Examiners should use the Wholesale Payment Systems Examination Procedures to determine the adequacy of the financial institution's payment system risk policies and wholesale payment business processes, including personnel and internal control systems used to mitigate the risks associated with wholesale payment systems. Wholesale payment system services include Fedwire Funds Servicefunds transfer and book-entry securities; CHIPS; SWIFT; payment messaging systems; net settlement, clearing and settlement systems; internally developed and off-the-shelf funds transfer systems; and web-based payment systems. The examiner's assessment of risk and risk management practices relating to a financial institution's wholesale payment system service should help determine the extent of testing and which procedures to perform. The assessment should consider the effectiveness of formal policies and procedures as well as the financial institution's underlying internal control environment including information security, business continuity and disaster recovery, and management of wholesale payment services outsourced to third parties.

Financial institutions are exposed to numerous credit, liquidity, reputation, legal, and operational risks in provisioning wholesale payment system services to counter parties and performing related processing, clearance, and settlement functions in-house and with third parties. Depending on the financial risks, IT related operational (transactional) risks, compliance risks, and complexity of wholesale payment system activity, the examination may require an integrated team approach that includes the knowledge and skills of safety and soundness examiners and IT examiners.

Examiners may incorporate the Examination Procedures as part of either an IT or safety and soundness examination. The Examination Procedures can also be used in its entirety, or can be used in modular fashion, focusing on particular wholesale payment system products or business lines. Depending on the size and complexity of the financial institution or service provider, examiners may tailor the use of the examination procedures. In many cases, they can eliminate certain procedures and still arrive at a conclusion regarding the quality of risk management practices and performance. The examination procedures are structured as follows:

- Tier I objectives and procedures, which evaluate the effectiveness of the financial institution and service provider's wholesale payment systems, internal controls, and risk management processes that may be relied on for the purpose of identifying and managing risks.
- Tier II objectives and procedures, which provide additional validation as warranted by the risks to verify the effectiveness of the financial institution and service provider's wholesale payment systems function.

Objective 1: Determine the scope and objectives of the examination of the wholesale

payment systems function.

1. Review past reports for comments relating to wholesale payment systems. Consider:

- Regulatory reports of examination.
- Internal and external audit reports.
- Regulatory reports on and, audit, and information security reports from/on service providers.
- Trade group, card association, interchange, and clearing house documentation relating to services provided by the financial institution.
- Supervisory strategy documents, including risk assessments.
- Examination work papers.

2. Review past reports for comments relating to the institution's internal control environment and technical infrastructure. Consider:

- Internal controls including logical access controls, data center operations, and physical security controls.
- Wholesale EFT network controls.
- Inventory of computer hardware, software, and telecommunications protocols used to support wholesale EFT transaction processing.

3. During discussions with financial institution and service provider management:

- Obtain a thorough description of the wholesale payment system activities performed, including transaction volumes, transaction dollar amounts, and scope of operations, including Fedwire Funds Service, CHIPS, SWIFT, and all wholesale payment messaging systems in use.
- Review the financial institution's payment system risk policy and evaluate its compliance with net debit caps and other internally generated self-assessment factors.
- Identify any wholesale payment system functions performed via outsourcing relationships and determine the financial institution's level of reliance on those services.
- Identify any significant changes in wholesale payment system policies, personnel, products, and services since the last examination.

4. Review the financial institution's response to any wholesale payment systems issues raised at the last examination. Consider:

- Adequacy and timing of corrective action.
- Resolution of root causes rather than specific issues.
- Existence of outstanding issues.

Objective 2: Determine the quality of oversight and support provided by the board of directors and management.

1. Determine the quality and effectiveness of the financial institution's wholesale payment systems management function. Consider:

- Data center and network controls over backbone networks and connectivity to counter parties.
- Departmental controls, including separation of duties and dual control procedures, for funds transfer, clearance, and settlement activities.
- Compliance with the Federal Reserve's Payment System Risk policies and procedures.
- Physical and logical security controls designed to ensure the authenticity, integrity, and confidentiality of wholesale payments transactions.

2. Assess management's ability to manage outsourcing relationships with service providers and software vendors contracted to provide wholesale payment system services. Evaluate the adequacy of terms and conditions, and whether they ensure each party's liabilities and responsibilities are clearly defined. Consider:

- Adequacy of contract provisions including service level and performance agreements.
- Compliance with applicable financial institution and third party (e.g. Federal Reserve, CHIPS, SWIFT) requirements.
- Adequacy of contract provisions for personnel, equipment, and related services.

3. Evaluate the adequacy and effectiveness of financial institution and service provider contingency and business recovery plans. Consider:

- Ability to recover transaction data and supporting books and records based on wholesale payment system business line requirements.
- Ability to return to normal operations once the contingency condition is over.
- Confidentiality and integrity of interbank and counter party data in transit and storage.

4. Evaluate wholesale payment system business line staff. Consider:

- Adequacy of staff resources.
- Hiring practices.
- Effective policies and procedures outlining department duties.
- Adequacy of accounting and financial controls over wholesale payment processing, clearance, and settlement activity.

5. Review the disaster recovery plan for the funds transfer system (FTS) to ensure it is reasonable in relation to the volume of activity, all units of the FTS are provided for in the plan, and the plan is regularly tested.

Objective 3: Determine the quality of risk management and support for Payment System Risk policy compliance.

1. Review policies and procedures in place to monitor customer balances for outgoing payments to ensure payments are made against collected funds or established intraday or overnight overdraft limits and payments resulting in excesses of established uncollected or overdraft limits are properly authorized.

2. Review a sample of contracts authorizing the institution to make payments from customers' accounts to ensure they adequately set forth responsibilities of the institution and the customer, primarily regarding provisions of the Uniform Commercial Code Article 4A (UCC4A) related to authenticity and timing of transfer requests.

Objective 4: Determine the quality of risk management and support for internal audit and the effectiveness of the internal audit program for wholesale payment systems.

1. Review the audit program to ensure all functions of the FTS are covered. Consider:

- Payment order origination (funds transfer requests).
- Message testing.

- Customer agreements.
- Payment processing and accounting.
- Personnel policies.
- Physical and data security.
- Contingency plans.
- Credit evaluation and approval.
- Incoming funds transfers.
- Federal Reserve's Payment Systems Risk Policy.

2. Review a sufficient sample of supporting audit work papers necessary to confirm that they support the execution of procedures established in step 1 above.

3. Review all audit reports related to the FTS and determine the current status of any exceptions noted in the audit report.

CONCLUSIONS

1. Determine the need to proceed to Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. From the procedures performed, including any Tier II procedures performed:

- Document conclusions related to the quality and effectiveness of the retail payment systems function.
- Determine and document to what extent, if any, the examiner may rely upon wholesale payment systems procedures performed by internal or external audit.

3. Review your preliminary conclusions with the EIC regarding:

- Violations of law, rulings, regulations, and third party agreements.
- Significant issues warranting inclusion as matters requiring board attention or recommendations in the report of examination.

- Potential impact of your conclusions on URSIT composite and component ratings.

4. Document your conclusions in a memo to the EIC that provides report ready comments for all relevant sections of the FFIEC Report of Examination and guidance to future examiners.

5. Organize work papers to ensure clear support for significant findings and conclusions.

Tier II Examination Objectives and Procedures

Overall Objective: The Tier II examination procedures for Wholesale Payment Systems provide for additional verification procedures to evaluate the effectiveness of the financial institution's internal control processes over its wholesale payment systems, including Fedwire Funds Service funds transfer and book entry securities, CHIPS, SWIFT, payment messaging systems, net settlement, clearing and settlement systems, internally developed and off-the-shelf funds transfer systems, and web-based payment systems. These procedures are designed to assist in achieving examination objectives, and may be used in their entirety or selectively. Examiners should coordinate this coverage with other examiners involved in assessing the institution's information systems, operations, and information security effectiveness to ensure there is an adequate understanding of the control environment as it pertains to the bank's wholesale payment systems.

Objective 1: Determine if management and the board have enacted sufficient controls over funds transfer activity.

1. Determine if management and the board provide administrative direction for the funds transfer function. Ascertain whether:

- The directors and senior management are informed regarding the nature and magnitude of risks with the institution's funds transfer activities.
- Management is informed of new systems designs and available hardware for the wire transfer system.
- The board of directors and/or senior management regularly review and approve any funds transfer limits, and if so, when the limits were last reviewed.
- Senior management and the board monitor customers with large intraday or overnight overdrafts and analyze the overdrafts along with all other credit exposure to the customer.

2. Determine if the board and management have developed sufficient policies and procedures to ensure that the following are reviewed:

- Transaction volumes.
- Adequacy of personnel and equipment.
- Customer creditworthiness.
- Funds transfer risk.

3. Determine if the board and senior management develop and support adequate user access procedures and controls for funds transfer requests. Assess whether the institution:

- Maintains a current list of employees approved to initiate funds transfer requests.
- Has developed and approved an organization plan that shows the structure of the funds management department and limits the number of employees who can initiate or authorize transfer requests.
- Has a list of authorized employee signatures maintained in a secure environment.
- Regularly reviews staff compliance with credit and personnel procedures, operating instructions, and internal controls.
- Requires its senior management receive and review activity and quality control reports which disclose unusual or unauthorized activities and access attempts

4. Determine if management maintains authorization lists from its customers that use the funds transfer system. Verify:

- Management advises customers to limit the number of authorized signers.
- There are dual controls or other protections over customer signature records.
- The authorization list also identifies authorized sources of requests (e.g., telephone, fax, memo, etc.).
- The customer authorization establishes limits over the amount each signer is authorized to transfer.

5. Determine if the institution has dual control procedures that pro-hibit persons who receive transfer requests from transmitting or ac-counting for those requests.

Objective 2: Determine the adequacy of the internal and external audit reviews of the funds transfer area.

1. Review the internal and external audit function to determine if the scope and frequency of audit review for the funds transfer area is adequate. Review:

- Whether internal auditors have expertise or training in funds transfer operations and controls.
- The frequency and scope of internal and external audit reviews of the funds transfer function.
- Whether the internal and external audits provide substantive testing or quantitative measurements of the following areas:

  - Personnel policies.

  - Operating policies (including segregation of duty and dual controls).

  - Customer agreements.

  - Contingency plans.

  - Physical security.

  - Logical security (user access, authentication, etc.).

  - Sample tests for message and recordkeeping accuracy.

  - Processing.

  - Balance verification and overdraft approval.

2. Obtain and review internal and external audit reports to ensure they provide an adequate appraisal of the funds transfer function to management.

3. Review management's response to audit reports to ensure the institution takes prompt and appropriate corrective action. Ensure there is adequate tracking and resolution of outstanding exceptions.

Objective 3: Determine if there are adequate written documents outlining the funds transfer operating procedures.

1. Obtain the institution's written procedures for employees in the incoming, preparation, data entry, balance verification, transmission, accounting, reconciling and security functions of the funds transfer area. Determine if management reviews and approves the

procedures periodically. Determine if the procedures address:

- Control over test words, signature lists, and opening and closing messages.
- Origination of funds transfer transactions and the modification and deletion of payment orders or messages.
- Review of rejected payment orders or messages.
- Verification of sequence numbers.
- End of day accounting for all transfer requests and message traffic.
- Controls over message or payment orders received too late to process in the same day.
- Controls over payment orders with future value dates.
- Supervisory review of all adjustments, reversals, reasons for reversals and open items.

Objective 4: Determine the adequacy of institution controls over funds transfer requests.

1. Determine if institution personnel use standard, sequentially numbered forms to initiate funds transfer requests.

2. Determine if the institution has an approved request authentication system.

3. Determine if the institution has adequate security procedures for requests received from customers via telex, on-line terminals, telephone, fax, or written instructions. Determine if management:

- Developed policies and procedures to verify the authenticity of requests (e.g., call backs, customer authentication, signature verification).
- Maintains a current record of authorized signers for customer accounts.

4. Determine if the institution records incoming and outgoing telephone transfer requests. Also determine if the institution notifies the customer that calls are recorded (e.g., through written contracts, audible signals).

5. Determine if the institution maintains sequence control internally for requests processed by the funds transfer function.

- Review a sample of incoming and outgoing messages to determine if they are time

stamped or sequentially numbered for control. If not, determine if the institution maintains an unbroken copy of all messages received via telex or other terminal printers during a business day.

- Determine if the sequence records and unbroken copies are reviewed and controlled by an employee independent of the equipment operations.

6. Ascertain whether the financial institution records transfer requests in a log or another bank record prior to execution.

- Review the logs to determine if supervisory personnel review the record of transfer requests daily.
- Select a sample of the transfer request log entries and compare them to funds transfer requests for accuracy.

7. Determine if the institution has guidelines for the information to be obtained from a customer making a funds transfer request. The request should contain:

- The account name and number.
- A sequence number.
- The amount to be transferred.
- The person or source initiating the request.
- The time and date.
- Authentication of the source of the request.
- Instructions for payment.
- Bank personnel authorization for large dollar amounts.

Objective 5: Determine if there are adequate controls over the institution's use of test keys for authentication.

1. Determine if all message and transfer requests that require testing are authenticated with a test key. If so determine whether:

- The institution maintains an up-to-date test key file.
- An agreement between the bank and the customer stipulates that test key formulas incorporate a variable (e.g., sequence number).

- There is a procedure in place for an employee (independent of testing the authenticity of transfer requests) to issue and cancel test keys.
- Test codes are verified by an employee who does not receive the initial transfer request.

2. Obtain and review management's test key user access list to determine if:

- There are dual controls or other protections over files containing test key formulas.
- Only authorized personnel have access to the test key area or to terminals used for test key purposes.

Objective 6: Determine if agreements concerning funds transfer activities with customers, correspondent banks, and service providers are adequate and clearly define rights and responsibilities.

1. Obtain any material agreements or contracts concerning funds transfer services between the financial institution and correspondent banks, service providers and operators (e.g., Federal Reserve Bank and CHIPS). Review the agreements to determine if they:

- Establish responsibilities and accountability among all parties.
- Establish recovery time objectives in the event of failure.
- Outline the other party's liability for actions of its employees.

2. Obtain a sample of customer agreements regarding funds transfer activity and review it for compliance with applicable sections of the Uniform Commercial Code. Consider if:

- Agreements adequately describe security procedures as defined by UCC Article 4A Sections 201 and 202.
- The bank obtains written waivers from its customers if they choose security procedures that are different from what is offered by the bank, as indicated in UCC Article 4A Section 202(c).
- Agreements with customers establish cut-off times for receipt and processing of payment orders and canceling or amending payment orders as noted in UCC Article 4A Section 106.

Objective 7: Review the institution's payment processing and accounting controls to determine the integrity of funds transfer data and the adequacy of the separation of duties.

1. Review the institution's reconcilement policies and procedures as they relate to the funds transfer department. Determine if:

- The funds transfer department prepares a daily reconcilement of funds transfer activity (incoming and outgoing) by dollar amount and number of messages.
- The funds transfer department performs end-of-day reconcilements for messages sent to and received from intermediaries (e.g., Federal Reserve Bank, servicers, correspondents, and clearing facilities).
- The daily reconcilements account for all pre-numbered forms, including cancellations.
- Supervisory personnel review the reconcilements of funds transfer and message requests on a daily basis.
- The staff responsible for balancing and reconciling daily activity is independent of the receiving, processing, and sending functions.
- The funds transfer department verifies that work sent to and received from other institution departments agree with its totals.
- The institution accepts transfer requests after the close of business or with a future value date, and whether there are appropriate processing controls.

2. Determine if the institution's daily processing policies and procedures are adequate to ensure data integrity and independent review of funds transfer activity. Determine if:

- Supervisory personnel and the originator initial all general ledger tickets or other supporting documents.
- The institution reviews all transfer requests to determine that they have been properly processed.
- Independent wire transfer personnel verify key fields before transmission.
- Staff members independent of entering the messages release funds transfer messages.
- Employees not involved in the receipt, preparation, or transmittal of funds review all reject and/or exception reports.

3. Determine if there is adequate oversight of the funds transfer department. Ensure:

- An independent institution department (e.g., accounting or correspondent banking) reviews and reconciles the Federal Reserve Bank, correspondent bank, and clearing house statements used for funds transfer activities to determine if:

  - They agree with the funds transfer departments records.

  - They identify and resolve any open funds transfer items.

- Open statement items, suspense accounts, receivables/payables, and inter-office accounts related to funds transfer activity are controlled outside of the funds transfer operations.

- Management receives periodic reports on open statement items, suspense accounts, and inter-office accounts that include:

  - Aging of open items.

  - The status of significant items.

  - Resolution of prior significant items.

- An officer reviews and approves corrections, overrides, open items, reversals, and other adjustments.

4. Determine if the institution has documented any operational or credit losses that it has incurred, the reason the losses occurred, and actions taken by management to prevent future loss occurrences.

5. Determine if the institution maintains adequate records as required by the Currency and Foreign Transactions Reporting Act of 1970 (also known as the Bank Secrecy Act) and the USA PATRIOT Act.

Objective 8: Determine the adequacy of the institution's personnel policies governing the funds transfer function.

1. Obtain and review the institution's personnel policies to assess the procedures and controls over hiring new employees. Determine if:

- The bank conducts screening and background checks on personnel hired for sensitive positions in the funds transfer department.

- The bank prohibits new employees from working in sensitive areas of the funds transfer operation without close supervision.

- The institution limits or excludes temporary employees from working in sensitive areas without close supervision.

2. Assess management's personnel policies regarding current employees in the funds transfer department. Determine if:

- Management obtains statements of indebtedness of employees in sensitive positions of the funds transfer function.
- Employees are subject to unannounced rotation of responsibilities.
- Relatives of employees in the funds transfer function are precluded from working in the institution's bookkeeping, audit, data processing, and/or funds transfer departments.
- The institution enforces a policy that requires employees to take a minimum number of consecutive days as part of their annual vacation.
- There are policies and procedures to reassign departing employees from sensitive areas of the funds transfer function and to remove user access profiles of terminated employees as soon as possible.

Objective 9: Determine if the institution has enacted sufficient physical and logical security to protect the data security of the funds transfer department.

1. Obtain, review, and test the policies and procedures regarding the physical security of the funds transfer department. Determine if:

- Management restricts access to the funds transfer area to authorized personnel. Identify and assess the physical controls (e.g., locked doors, sign-in sheets, terminal locks, software locks, security guards) that prevent unauthorized physical access.
- There is an up-to-date funds transfer area visitors log and whether visitors are required to sign in and be accompanied while in restricted areas.
- There are adequate controls over the physical keys used to access key areas and key equipment within the funds transfer department.

2. Obtain and review policies and procedures regarding wire transfer password controls to determine if they are adequate. Consider whether:

- Management requires operators to change their passwords at reasonable intervals.
- Management controls access to master password files ensuring that no one has access to employee passwords.
- Passwords are suppressed on all terminal displays.
- Policy requires that passwords meet certain strength criteria so they are not easily

guessed.

- Management maintains required generic system account passwords under dual control.
- Terminated or transferred employees access is removed as soon as possible.
- Access levels and who has passwords is periodically reviewed for appropriateness.

3. Review funds transfer system user access profiles to ensure that:

- User access levels correspond to job description.
- Management appropriately limits user access to the funds transfer system and periodically reviews the access limits for accuracy.
- There are adequate separation of duties and access controls between funds transfer personnel and other computer areas or programs.

4. Review the institution's access controls to determine if terminals in the funds transfer area are shut down or locked out when not in use or after business hours. Determine:

- The adequacy of time out controls.
- The adequacy of time of day controls.
- Whether supervisory approval is required for access during non-work hours.

5. Determine if the institution's training program adequately protects the integrity of funds transfer data. Ensure:

- The institution conducts training in a test environment that does not jeopardize the integrity of live data or memo files.
- There are adequate controls to protect the confidentiality of data housed in the test environment.
- There are procedures and controls to prevent the inadvertent release of test data into the production environment, thus transferring live funds over the system.

Objective 10: Review the adequacy of backup, contingency, and business continuity plans for the funds transfer function.

1. Obtain the institution's written contingency and business continuity plans for Obtain

the institution's written contingency and business continuity plans for partial or complete failure of the systems and/or communication lines between the bank and correspondent bank, service provider, CHIPS, Federal Reserve Bank, and data centers. Consider if:

- The procedures, at a minimum, ensure recovery by the opening of the next day's processing depending on the criticality of this function to the institution.
- The contingency plans are reviewed and tested regularly.
- Management has distributed these plans to all funds transfer personnel.
- There are procedures to secure sensitive information and equipment before evacuation (if time permits) and security personnel adequately restrict further access to the affected areas.
- The plan includes procedures for returning to normal operations after a contingency.

2. Review the institution's policies and procedures regarding back-up systems. Assess whether:

- The institution maintains adequate back-up procedures and supplies for events such as equipment failures and line malfunctions.
- Supervisory personnel approve the acquisition and use of back-up equipment.

Objective 11: Determine if the institution adequately monitors intraday and overnight overdrafts. Ensure that management applies appropriate credit standards to customers that incur overdrafts.

1. Determine if management has developed procedures to approve customer use of daylight or overnight overdrafts including assigning appropriate approval authority to officers. Obtain and review a list of officers authorized to approve overdrafts and their approval authority, a current list of borrowers authorized to incur daylight and overnight overdrafts, and a sample of overdraft activity. Determine if:

- Management has established limits for each customer allowed to incur intraday and overnight overdrafts.
- The institution has assigned overdraft approval authority to officers with appropriate credit authority. Ensure that:

  - Payments that exceed the established limits are referred to an officer with appropriate credit authority for review and approval before release.

  - Payments made in anticipation of the receipt of covering funds are approved by an officer with appropriate authority.

- Management assesses all of a customer's credit facilities and affiliated relationships in determining overdraft limits.
- The institution routinely reviews and updates the institution and customer limits as well as officer approval authority.

2. Review the institution's policies and procedures regarding overdrafts to ensure it prohibits transfers of funds against accounts that do not have collected balances or preauthorized credit availability. Determine if:

- Supervisory personnel monitor funds transfer activities during the business day to ensure that payments in excess of approved limits are not executed without proper approval.
- An intraday record is kept for each customer showing opening collected and uncollected balances, transfers in and out, and whether the collected balances are sufficient at the time payments are released.
- The cause of any violations of overnight overdraft limits is identified and documented.
- Intraday exposures are limited to amounts expected to be received the same day.
- Adequate follow-up is made to obtain the covering funds in a timely manner.

3. If required as a participant of a net settlement system, determine whether management sets and approves bi-lateral credit limits on a formal credit analysis.

4. If the institution is an Edge Act Corporation, determine whether intraday and overnight overdrafts comply with Regulation K.

Objective 12: Review and determine the adequacy of the institution's controls over incoming funds transfers.

1. Review policies and procedures regarding incoming funds transfers. Select a sample of incoming funds transfers and review them to determine if:

- The institution maintains separation of duties over receipt of instructions, posting to a customer's account, and mailing customer credit advices.
- OFAC verification is performed.
- There are adequate audit trails maintained from receipt through posting the transfer to a customer's account.
- Procedures ensure accuracy of accounting throughout the process.

- Customer advices are issued in a timely manner.
- Any funds transfer requests received via telex, telephone or fax are authenticated prior to processing.

Objective 13: Determine if the institution complies with the Federal Reserve Policy Statement on Payments System Risk.

1. Determine if the institution incurs overdrafts in its Federal Reserve account. If so, consider if:

- The institution has reviewed and complied with the Payment System Risk program (i.e., the institution selected an appropriate net debit cap).
- The institution has elected a de minimis or self-assessed net debit cap and ensure that the examination evaluates the adequacy of records supporting the accuracy of the de minimis or self-assessed rating.

Objective 14: Review the institution's policies and procedures regarding the release of payment orders to assess the adequacy of controls.

1. Determine whether all incoming and outgoing payment orders and messages are received in the funds transfer area.

2. Obtain a sample of payment orders. Determine if the payment orders are:

- Logged as they enter the funds transfer department.
- Time stamped or sequentially numbered for control.
- Reviewed for signature authenticity.
- Reviewed for test verification, if applicable.
- Reviewed to determine whether personnel who initiated each funds transfer have the authority to do so.

3. Determine if current lists of authorized signatures are maintained in the wire transfer area. Ensure the lists indicate the amount of funds that individuals are authorized to release.

4. Assess whether there are adequate dual controls over the review of payment orders

and message requests. Determine whether an independent employee reviews the requests for the propriety of the transaction and for future dates, especially on multiple transaction requests.

Objective 15: Coordinate the review of wholesale payment systems with examiners in charge of reviewing other information technology risks.

1. In discussion with other examiners, ensure that management applies corporate-wide, information technology policies and procedures (i.e. development and acquisition, operational security, environmental controls, etc.) to the funds transfer department. If any discrepancies exist, determine their severity and document any corrective actions.

Appendix B: Glossary

Aggregate Short Position - The sum of a Settlement Member's short positions, each such short position expressed in its base currency equivalent and adjusted by the applicable haircut.

Aggregate Short Position Limit - In respect of a Settlement Member, the maximum aggregate short position that such Settlement Member is permitted to incur at any time.

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

Automated Clearing House (ACH) - An electronic clearing system in which a data processing center handles payment orders that are exchanged among financial institutions, primarily via telecommunications networks. ACH systems process large volumes of individual payments electronically. Typical ACH payments include salaries, consumer and corporate bill payments, interest and dividend payments, and Social Security payments.

Automated Teller Machine (ATM) - An electronic funds transfer (EFT) terminal that allows customers using a PIN-based debit (ATM) card to initiate transactions (e.g., deposits, withdrawals, account balance inquiries).

Bankcard - A general-purpose credit card, issued by a financial institution under agreement with the bankcard associations (Visa and MasterCard), which customers can use to purchase goods and services and to obtain cash against a line of credit established by the bankcard issuer.

Bilateral Key Security - A multi-level data encryption system, based on the exchange of Bilateral Keys, allowing users of SWIFT to create, send, and receive SWIFT messages. Bilateral Keys are unique authenticator keys possessed by only the two parties (either the provider or recipient of a message) involved and provide confirmation in both directions of the legitimacy of a message sent via SWIFT.

Check - A written order from one party (payer) to another (payee) requiring the payer's financial institution to pay a specified sum on demand to the payee or to a third party specified by the payee

Clearance - The process of transmitting, reconciling, and in some cases, confirming payment orders or financial instrument transfer instructions prior to settlement.

Consumer - Usually refers to an individual engaged in non-commercial transactions.

Correspondent Bank - An institution, acting on behalf of other institutions, that can settle the checks they collect for other institutions (respondents) by using accounts on their books or by sending a wire funds transfers. Generally, a provider of banking and payment services to other financial institutions.

Credit Card - A card indicating the holder has been granted a line of credit. It enables the holder to make purchases or withdraw cash up to a prearranged ceiling. The credit granted can be settled in full by the end of a specified period or can be settled in part, with the balance taken as extended credit. Interest is charged based on the terms of the credit card agreement and the holder is sometimes charged an annual fee.

Currency Balance - As at the time calculated, the current amount (positive or negative) of a particular eligible currency included in an account, as indicated on the books and records of CLS Bank. A currency balance is not a separate account.

Daylight overdraft - A daylight overdraft occurs at any point in the business day when the balance in an institution's account becomes negative. Daylight overdrafts can occur in accounts at Federal Reserve Banks as well as at private financial institutions. Daylight credit can also arise in the form of net debit positions of participants in private payment systems. A daylight overdraft occurs at a Federal Reserve Bank when there are insufficient funds in an institution's Federal Reserve Bank account to cover outgoing funds transfers or incoming book-entry securities transfers. An overdraft can also be the result of other payment activity processed by the Federal Reserve Bank, such as check or automated clearinghouse transactions.

Depository - An institution that holds funds or marketable securities for safekeeping. Depositories may be privately or publicly operated and allow securities transfers through book-entry and offer funds accounts permitting funds transfers as a means of payment.

Electronic Funds Transfer Act (EFTA) - The Electronic Funds Transfer Act and Regulation E are designed to ensure adequate disclosure of basic terms, costs, and rights relating to electronic fund transfer (EFT) services provided to consumers. Institutions offering EFT services must disclose to consumers certain information, including: initial and updated EFT terms, transaction information, periodic statements of activity, the consumer's potential liability for unauthorized transfers, and error resolution rights and procedures. EFT services include automated teller machines, telephone bill payment, point-of-sale transfers in retail stores, fund transfers initiated through the Internet, and pre-authorized transfers to or from a consumer's account.

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

Extensible Markup Language (XML) - XML (Extensible Markup Language) is a "metalanguage", a language for describing other languages – which lets you design your own customized markup languages for different types of documents. It is designed to improve the functionality of the Web by providing more flexible and adaptable information identification.

Federal Reserve Banks - The Federal Reserve Banks provide a variety of financial services including retail and wholesale payments. The Federal Reserve Bank operates a nationwide system for clearing and settling checks drawn on depository institutions located in all regions of the United States.

Fedwire Funds Service - The Federal Reserve Banks' high-speed electronic funds transfer system. As a real-time gross settlement system, the Fedwire® Funds Service processes and settles individual payments between participants immediately in central bank money. Once processed, these payments are final.

Fedwire Securities Service - The Federal Reserve Banks' high-speed electronic payments system for maintaining securities accounts and for effecting securities transfers. The Fedwire® Securities Service provides a real-time, delivery-versus-payment (DVP), gross settlement system that allows for the immediate, simultaneous transfer of securities against payment. Once processed, securities transfers are final.

FIN (Financial Application) - The SWIFT application within which all SWIFT user-to-user messages are input and output.

Finality - Irrevocable and unconditional transfer of payment during settlement.

Haircut - With respect of an eligible currency, the percentage increase of a negative currency balance or reduction of a positive currency balance and is based on (a) the volatility of the historic foreign exchange movements in the applicable eligible currency determined by CLS Bank and (b) an add-on component.

Instruction - Means (i) any instruction submitted by a Member through the submission process directing CLS Bank to settle certain payment entitlements and obligations arising pursuant to an FX transaction eligible for settlement in CLS Bank and (ii) any instructions resulting from the split of Settlement Eligible Instructions.

Internet - The global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide.

Large value funds transfer system - A wholesale payment system used primarily by financial institutions in which large values of funds are transferred between parties. Fedwire® and CHIPS are the two large-value transfer systems in the United States.

Long position - In respect of a currency balance that is greater than zero, the amount by which such currency balance is greater than zero. A position that appreciates in value if market prices increase. When one buys a currency, their position is long.

Matched instructions - Two Instructions in which the information set forth in a specific CLS Bank Rule is matched in accordance with the parameters and procedures set forth in the CLS Bank Rules.

Matching - With respect to compared and non-compared transactions, the process of comparing the trade or settlement details provided by counterparties to ensure they agree with respect to the terms of the transaction. Also called comparison checking.

National Settlement Service (NSS) - Also referred to as Deferred Net Settlement. The Federal Reserve Banks' multilateral settlement service. NSS is offered to depository institutions that settle for participants in clearinghouses, financial exchanges, and other clearing and settlement groups. Settlement agents acting on behalf of those depository institutions electronically submit settlement files to the Federal Reserve Banks. Files are processed on receipt, and entries are automatically posted to the depository institutions' Reserve Bank accounts. Entries are final when posted.

Net debit cap - The maximum dollar amount of uncollateralized daylight overdrafts that an institution is authorized to incur in its Federal Reserve account. The net debit cap is generally equal to an institution's capital times the cap multiple for its cap category.

Office of Foreign Asset Control (OFAC) - The Office of Foreign Assets Control, United States Department of the Treasury, administers and enforces economic sanctions programs primarily against countries and groups of individuals such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

Open market operations - The buying and selling of government securities in the open market in order to expand or contract the amount of money in the banking system.

Originating depository financial institution (ODFI) - A participating financial institution that originates entries at the request of and by agreement with its originators in accordance with the provisions of the NACHA rules.

Originator - A person that has authorized an ODFI to transmit a credit or debit entry to the deposit account of a receiver at an RDFI.

Payment - A transfer of value.

Payment system - The mechanism, the rules, institutions, people, markets, and agreements that make the exchange of payments possible.

Payments System Risk Policy (PSR) - The Federal Reserve's Payments System Risk (PSR) policy addressing the risks that payment systems present to the Federal Reserve Banks, the banking system, and to other sectors of the economy.

Real time gross settlement (RTGS) System - A type of payments system operating in real time rather than batch processing mode. It provides immediate finality of transactions. Gross settlement refers to the settlement of each transfer individually rather than netting. FedwireÒ is an example of a real time gross settlement system.

Receiver - An individual, corporation, or other entity that has authorized a company or an originator to initiate a credit or debit entry to a transaction account belonging to the receiver held at its RDFI.

Receiving depository financial institution (RDFI) - Any financial institution qualified to receive debits or credits through its ACH operator in accordance with the ACH rules.

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

Reserve account - A non-interest-earning balance account institutions maintain with the Federal Reserve Bank or with a correspondent bank to satisfy the Federal Reserve's reserve requirements. Reserve account balances play a central role in the exchange of funds between depository institutions.

Retail payments - Payments, typically small, made in the goods and services market.

Security procedure agreement - An agreement between a financial institution and a Federal Reserve Bank whereby the financial institution agrees to certain security procedures if it uses an encrypted communications line with access controls for the transmission or receipt of a payment order to or from a Federal Reserve Bank.

Settlement - The final step in the transfer of ownership involving the physical exchange of securities or payment. In a banking transaction, settlement is the process of recording the debit and credit positions of the parties involved in a transfer of funds. In a financial instrument transaction, settlement includes both the transfer of securities by the seller and the payment by the buyer. Settlements can be "gross" or "net." Gross settlement means each transaction is settled individually. Net settlement means parties exchanging payments will offset mutual obligations to deliver identical items (e.g., dollars or EUROS), at a specified time, after which only one net amount of each item is exchanged.

Settlement eligible instructions - See "Matched Instructions".

Short position - In respect of a currency balance that is less than zero, the amount by which such currency balance is less than zero. An investment position that benefits from a decline in market price. When one sells a currency their position is short.

Short position limit - In respect of an eligible currency, the maximum short position a Settlement Member may have at any time in that eligible currency and, unless otherwise reduced pursuant to the CLS Bank Rules, shall equal (i) the total amount of all available committed liquidity facilities in such eligible currency (or such lesser amount that CLS Bank may determine from time to time) minus (ii) the amount of the largest available committed liquidity facility among such liquidity facilities (after taking into account any amounts already drawn.

Spot - The most common foreign exchange transaction. Spot or spot date refers to the spot transaction value date that requires settlement within two business days, subject to value date calculation.

Test key - Internal controls used to verify the authenticity of incoming wire requests involve the use of test keys. A test key is a formula used to develop or interpret test codes or test words. Test codes or words consist of a series of numbers signifying different types of information and usually precede the text of the message. As an example, a test code may contain a bank number, the amount of the transaction, and a number indicating the day and week of the month. As an additional precaution, many test codes contain a variable (sequence number) based on the number of messages received.

Appendix C: Laws, Regulations and Guidance

Laws

- 12 USC: 248 (i), (j), and (o): Federal Reserve Act (N/A)
- 12 USC: 342: Federal Reserve Act (N/A)
- 12 USC: 360: Federal Reserve Act (N/A)
- 12 USC: 464: Federal Reserve Act (N/A)
- 12 USC: 4001-4010: Federal Reserve Act (N/A)

Federal Reserve Board

- 12 CFR Part 210, Subpart B: Funds Transfers Through Fedwire (Regulation J) (N/A)

Appendix D: Legal Framework for Interbank Payment Systems

State and federal statutes, regulations, and case law govern the payment systems in the United States. The relevant legal principles depend on the method of payment (paper-based or electronic) and in some cases the status of parties to a payment (consumer, merchant, or financial institution). Several federal laws apply to payment activities, particularly in the consumer sector. At the state level, the Uniform Commercial Code (UCC) establishes a set of model statutes governing certain commercial and financial activities, including some banking and securities market transactions. Articles of the UCC pertinent to payment and settlement activities are the following: Article 3 (negotiable instruments), Article 4 (bank deposits and collections), Article 4A (funds transfers, including wholesale ACH credit transfers) and Article 8 (investment securities). [15]

Every state has incorporated these Articles, sometimes with local variations, into the state laws. In addition, the rules and membership agreements of private clearing and settlement arrangements provide a contractual framework for payment activity within the relevant governing law.

Fedwire Funds Service

The Federal Reserve's Regulation J governs payment transactions using the Fedwire Funds Service and incorporates the requirements of Article 4A of the UCC. The Regulation, in particular subpart B, defines the rights and responsibilities of financial institutions that use Fedwire, as well as the rights and responsibilities of the Federal Reserve Bank. Federal Reserve Bank Operating Circular 6 covers items such as Fedwire operating hours, security, authentication, fees, and certain restrictions. [16] It also contains time schedules, holidays, and guidelines pertaining to the extension of Fedwire hours.

Under subpart B of Regulation J and Operating Circular 6, the Federal Reserve Banks can impose conditions on an institution's use of Fedwire. In particular, the regulation and operating circular require each Fedwire participant to enter into a security procedure agreement with its Federal Reserve Bank and includes institution responsibilities for information security, business continuity, and related administrative information.

Federal Reserve Regulation CC, Availability of Funds and Collection of Checks, also regulates the time within which a depository institution receiving a Fedwire or CHIPS funds transfer on behalf of a customer must make those funds available to its customer.

National Settlement Service (NSS)

Federal Reserve Bank Operating Circular 12 establishes the terms and conditions under which participants using NSS submit settlement files to the Federal Reserve Banks. The

provision of intraday settlement finality is similar to the Fedwire Funds Service and enables the Federal Reserve Banks to manage and limit settlement risk by incorporating risk controls on extensions of daylight credit.

Messaging Systems

Payment messaging systems allow financial institutions to initiate payment orders, providing that the institution is authorized to act on behalf of its customers. It is important for financial institutions to establish the authenticity and time of receipt of payment order messages. UCC4A establishes responsibility for the execution of a payment order and requires financial institutions to agree to the terms and conditions established by the responsible messaging system with respect to security procedures.

CHIPS

Funds transfers made through CHIPS are subject to CHIPS rules and procedures. The CHIPS rules stipulate that the laws of the state of New York, which include Article 4A of the UCC, also apply to CHIPS transactions. CHIP Co. is not responsible for losses resulting from system errors. Each participant agrees to indemnify and to hold harmless CHIPS from such losses. Any participant losses are settled by a loss sharing agreement, and if a participant commits a fraud, that participant will bear the loss. CHIP Co. maintains a financial institution bond for possible employee fraud. Losses exceeding CHIPS's bond coverage are shared on a pro rata basis of each participant's average daily CHIPS usage for the 30-day calendar period preceding the notice of loss to the underwriters of the bond.

Appendix E: Federal Reserve Board Payment System Risk Policy: Daylight Overdrafts

Similar to financial institutions offering retail payment services to customers, the Federal Reserve Banks are exposed to credit risk when they process payments for financial institutions holding reserve accounts. The Federal Reserve Banks guarantee payment finality for financial institutions using their systems for Fedwire Funds, NSS, and ACH credit originations. Due to this payment guarantee, the Federal Reserve Banks may incur losses when institutions fail with overdrafts in their accounts.

An integral component of the Federal Reserve's Payments System Risk (PSR) policy controls and reduces the use of Federal Reserve Banks' daylight overdrafts and the Federal Reserve Banks' associated credit risk. [17] The PSR policy addresses daylight overdrafts that occur in accounts at Federal Reserve Banks as well as at financial institutions. A daylight overdraft occurs when an institution's Federal Reserve Bank account is in a negative position during the business day.

To control daylight overdrafts, the PSR policy establishes limits, or net debit caps, on the amount of Federal Reserve Bank daylight credit that a depository institution may use during a single day and over a two-week reserve maintenance period. These limits are sufficiently flexible to reflect the overall financial condition and operational capacity of each institution using Federal Reserve Bank payment services. The policy also permits the Federal Reserve Banks to protect themselves from the risk of loss by unilaterally reducing net debit caps, imposing collateralization or clearing-balance requirements, rejecting or delaying certain transactions until sufficient balances exist, or prohibiting an institution from using Federal Reserve Bank payment services.

The PSR policy established daylight overdraft fees to provide a financial incentive for institutions to control their use of Federal Reserve Bank intraday credit and to recognize the risks inherent in the provision of intraday credit. Daylight overdraft fees induce financial institutions to make business decisions concerning the amount of Federal Reserve Bank intraday credit they are willing to use based on the cost of using that credit. The daylight overdraft measurement method, which incorporates a set of nearly real time transaction posting rules, also supports institutions in controlling their use of Federal Reserve Bank intraday credit.

The Federal Reserve Banks use the Account Balance Monitoring System (ABMS) to monitor financial institution accounts intraday. For a limited number of institutions, the system is also used to prevent those institutions from incurring daylight overdrafts in their Federal Reserve Bank accounts beyond a certain threshold (often set to zero) for Fedwire Funds, NSS, and ACH credit origination transactions. In this situation, credit ACH transactions are required to be prefunded, including those settled on behalf of any respondents. If there are insufficient funds available in the account, the batch will reject and a notice will be sent to the ACH sending point and to the settlement financial institution. [18]

Appendix F: Payment System Resiliency

The "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" identifies sound practices focusing on minimizing the immediate systemic effects of a wide-scale disruption to critical financial markets. The sound practices focus on the appropriate back-up capacities necessary for recovery and resumption of clearance and settlement activities for material open transactions in wholesale financial markets. [19]

The agencies, in promoting resiliency, have identified four broad sound practices for core clearing and settlement organizations and firms that play significant roles in critical financial markets. The practices involve:

- Identifying clearing and settlement activities in support of critical financial markets.
- Determining appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets.
- Maintaining sufficient geographically dispersed resources to meet recovery and resumption objectives.
- Routinely using or testing recovery and resumption arrangements.

The sound practices discussed in this paper supplement the agencies' respective policies and other guidance on business continuity planning.