

Electronic Funds Transfer Systems (EFTS) have become the primary method employed for large-dollar (wholesale) payments made by financial institutions and their business customers. It also is also an important and expanding element of retail payment systems. EFT is defined as any transfer of funds that is initiated through an electronic terminal, telephonic instrument, computer or magnetic tape to order, instruct, or authorize a financial institution to debit or credit an account. The ability of financial institutions to provide these services is a direct outgrowth of the rapidly improving computer and data communications technology.

EFT covers a wide-range of applications that, while for control purposes must be separate from direct IS activities, are often highly dependent on IS operations. Even systems not directly interfaced with a financial institution's IS operations, such as direct Fedwire and terminal connections with correspondent institutions, transmit data electronically. As a result, examiners familiar with information systems must be involved with the review of EFTS activities, since even non-IS related activities such as credit monitoring, payment authorization, and management reporting depend on systemically reliable and secure automated controls.

For U.S. financial institutions, the bulk of large-dollar payments are made through the Fedwire and CHIPS payments systems. While still primarily used for retail payments, an increasing number of large-dollar payments are made by means of automated clearing houses (see ACH Chapter 21). Other retail funds transfer services (see Chapter 20) include automated teller machines (ATMs), point-of-sale (POS) systems, telephone bill paying, and home banking systems, which are gaining widespread customer use.

Critical to any payments system is the method employed to generate payment instructions.

Payments systems are supported by a variety of electronic message networks that deliver payment instructions, including SWIFT, telex, and in-house data transmission terminals. Payment instructions also may be generated by partially electronic or manual sources including telephone, fax, letters, memos, and standing instructions.

In view of the potential for material loss through error, inadequate control, or fraud in EFT systems, it is imperative that financial institutions establish a strong internal control environment over these activities. Furthermore, senior management regularly should be made aware of inherent risks associated with the various systems together with any changes in the environment.

WHOLESALE OR LARGE-DOLLAR FUNDS TRANSFER SYSTEMS

FEDWIRE

Fedwire is the Federal Reserve System's nationwide electronic funds and securities transfer network. Fedwire links the 12 Federal Reserve Banks with a large number of depository institutions that maintain reserve or clearing accounts with the Federal Reserve. On a daily basis, Fedwire processes approximately \$1.4 trillion in funds and securities transfers. The Fedwire funds transfer system provides the electronic transfer of immediate and irrevocable payments between participating institutions and functions as both a clearing and settlement facility. The Fedwire book-entry securities transfer system provides for the transfer of U.S. government and federal agency securities that settle on the books of the Federal Reserve. The Fedwire service may be accessed by direct computer interface or off-line by telephone through a PC-based electronic delivery system named Fedline. Fedline was developed by the Reserve Banks and uses dial-up lines for network access. (See Chapter 19 Fedline EFT for additional information.)

The Fedwire fund transfer system is a credit transfer system. Each funds transfer is settled individually on the books of the Federal Reserve as it is processed, and is considered a final and irrevocable payment. A depository institution that sends a funds transfer irrevocably authorizes its Reserve Bank to debit (charge) its account for the transfer amount, and further authorizes the Reserve Bank of the receiving institution to give credit in the same amount to the payee. The Federal Reserve guarantees immediate availability of funds; once the Federal Reserve bank credits the receiving institution's account or delivers the advice of payment, the Federal Reserve Bank will not reverse credit for the payment. Therefore, there is no settlement risk to the recipient of a Fedwire Transfer. The Federal Reserve Bank assumes the risk if the sending bank overdraws its position at the Reserve Bank. The Federal Reserve's payments system risk policies are specifically designed to limit the risk that a sending bank fails with its reserve account overdrawn. Reserve Banks require that depository institutions continuously monitor and adjust their reserve account positions to ensure adequate funds are on hand, or that they are in compliance with established overdraft limits and collateral requirements. Other risks associated with Fedwire funds transfers include potential loss due to errors, omissions, and fraud.

CHIPS

The Clearing House Interbank Payment System (CHIPS) is a funds transfer network owned and operated by the New York Clearing House Association (NYCHA) to deliver and receive U.S. dollar payments between banks, domestic and foreign, that have offices located in New York City. The network is composed of a small number of settling participants (large U.S. chartered banks that settle end-of-day balances between each other) and a larger number of non-settling participants who maintain accounts with one of the settling banks. Settling participants settle for non-settling participants. The majority of CHIPS payments are for settlement of U.S. dollar foreign exchange contracts and Eurodollar investments.

CHIPS is a multilateral net settlement payments system. Unlike Fedwire funds transfers, CHIPS

transfers are not settled at the time the payment instructions are delivered, but instead are settled at the end of the day through a net settlement arrangement established with the Federal Reserve Bank of New York. The Federal Reserve Bank of New York provides CHIPS with a special settlement account that is open to the settling participants only during the settlement period. Based on a net settlement report prepared by CHIPS at the end of each business day, CHIPS participants in a net debit position remit payments via Fedwire to the special account and, after all debit payments are received, the banks in a net credit position are paid.

Payment messages over the CHIPS network are irrevocable obligations of the participant. NYCHA has established rules that address the possibility of a participant failing to settle. Under these loss-sharing rules, all other participants are obligated to pay a share of the net debit balance of the failed participant. The rules are based on a defined formula that initially includes a pro-rata apportionment based on a participant's activity with the failed participant. This additional settlement obligation is collateralized in advance.

In order to limit the risk created by an individual participant, CHIPS adopted bilateral credit limits and net debit caps related to intraday net debit positions. Bilateral credit limits establish a limit on the net value of payments each participant is willing to receive from each of the other participants. The limit may be as high as 20 times the amount of collateral that the participant holds with CHIPS and may be revised on an intraday basis. The CHIPS system automatically rejects any payment in excess of the bilateral limit. Net debit caps are a function of the bilateral credit limits extended to a participant by all other participants and represent the maximum permissible debit position by a participant during the day. The net debit cap is 5 percent of the sum of all bilateral credit limits extended to a participant by other CHIPS participants and is set each morning. Payments that exceed the cap will be rejected.

CHIPS is not responsible for losses resulting from system errors. Such losses are settled by the participants. If a participant commits a fraud, that participant will bear the loss. CHIPS maintains

insurance coverage for possible fraud losses committed by employees. Losses exceeding CHIPS insurance coverage are shared on a pro rata basis of each participant's dollar amount of transfers for the preceding month.

Other Related Systems

Indispensable components of funds transfer activities are the message systems employed by customers to originate payment orders, either for their own benefit or payment to a third party. Unlike payments systems, message systems process instructions to move funds and administrative messages. The actual funds movement is accomplished by debiting the originating customer's account and crediting the beneficiary's account. If the beneficiary's account or the beneficiary bank's account also are with the originator's bank, the transaction is normally handled internally via book-entry. If the beneficiary related accounts are outside the originating customer's bank, the transfer may be completed by use of a payments system, such as Fedwire or CHIPS. The means of arranging payment orders range from manual methods (e.g., memos, letters, telephone, fax, or standing instruction) to 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 intercompany purposes only or connected to both intercompany and 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. UCC4A, which has been adopted by a majority of the states in the United States and incorporated into the Federal Reserve System's Regulation J, establishes liability for improper or untimely processing of a payment order, or cancellation, from initiation to final execution of the originator's instructions. Included in UCC4A is a requirement that a security agreement acceptable to both the financial institution and the customers be

established

Several phases exist in funds transfer operations where inappropriate or incorrect use of the system can occur. As a result, there is a need for a clearly defined authentication procedure throughout the process. Effective controls should be established over the following areas:

- The original instructions from the customer to the financial institution (e.g., account officer, branch manager, and terminal entry).
- Every transfer point of data for each step of the manual process (e.g., account officer, message receipt, authentication, data entry, and payment release).
- Every transfer point of data for each step of an automated process (e.g., SWIFT/telex, message preparation, data entry, and payment release).

The following is a summary of various message systems:

- *SWIFT* – Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a nonprofit cooperative of member banks serving as a worldwide interbank telecommunications network, based in Brussels, Belgium. SWIFT operates three fully redundant operating centers in Brussels; Amsterdam, Netherlands; and Culpepper, VA, that can function in a standalone mode. Unlike EFT systems, SWIFT only provides instructions to move funds. SWIFT does not have a settlement mechanism. The actual funds movement is accomplished via debits and credits to correspondent accounts maintained at participating institutions. SWIFT messages may be used to transmit instructions either domestically or internationally. Many high volume funds transfer institutions interface SWIFT directly with their automated payments system. As a result, entries pass through the system without human intervention unless programmed conditions (e.g., overdraft limit excesses) or message errors occur. SWIFT provides transaction reports necessary for system reconciliation. The SWIFT system employs dual passwords for data entry and release of certain messages (e.g., funds payment orders). Once properly

entered at the point of origination, the SWIFT network controls the integrity of the messages, thus there is no requirement for the receiver to reverify payment orders.

- *Telex* – Several private telecommunications companies offer worldwide or interconnected services that provide a printed record of each message transmitted. Telex is the primary message system for institutions that do not have access to SWIFT. Access to Telex systems can be by dial-up or dedicated line connections through teleprinters. Some systems are monitored by computer around the clock, seven days a week and are fully redundant with automatic switch over and recovery capability. The companies which process the majority of volume include Western Union, RCA Globe, ITT World Communications, and Money Gram. The Telex systems do not include built-in security features. Users of Telex exchange security codes and senders numerically number messages sent to another given institution. It is the responsibility of the sending institution to incorporate a test key in all instructions to a receiver to execute a payment order. The receiver is responsible for the safekeeping of the unique test code keys of each sender and the decoding of each test message. This function must be clearly separated from the Telex operating area and funds payment function. Due to the lack of uniformity and the uniqueness of the various test codes, only a few institutions employ fully automated interface of Telex with their funds payments systems. However, such interfaces are increasing.
- *In-house Terminals* – Several institutions employ terminals, connected via telecommunications networks with customers' and the institution's 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 the aforementioned systems are the primary sources for payment order origination, smaller institutions, and some operations in larger institutions (e.g., private banking) 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 utilizing these payment order methods have a viable security program, including:
 - Signature lists to be maintained and used for 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, it may be used with other security devices such as call backs or codes.
 - Call back to authorized individuals for both internally and externally generated telephone instructions; and
 - Procedures covering standing instructions protecting against unauthorized change, periodic review to validate accuracy, and ensuring execution under the agreed terms.

CONTROLLING PAYMENT TRANSFER RISKS

Depository institutions, their primary regulators, and the Federal Reserve have been focusing increased attention on the credit risks inherent in large-dollar funds transfer systems. Credit risk is the risk that a party to a funds transfer will fail to settle for the transfer. This risk arises when a financial institution or a Federal Reserve Bank executes a payment order before it has received covering payment from its customer, i.e., when the transfer results in a daylight overdraft in the account of the sending customer. Many depository institutions incur intraday, or daylight, overdrafts in their accounts held at the Federal Reserve as a result of Fedwire funds transfers sent and book-entry

securities received against payment. Similarly, institutions often permit their corporate customers to incur intraday overdrafts.

In principle, an institution engaging in this practice is extending credit to its customer. In most cases, the overdraft is eliminated with incoming funds transfers from other institutions (or outgoing securities transfers against payment) by the end of the business day. Since daylight overdrafts constitute an extension of credit – no matter the period of time involved – institutions' credit policies should include provisions for approving and monitoring intraday credit lines to customers.

Intraday overdrafts also may result in disruption of the settlement process for private large-dollar wire transfer systems (e.g., CHIPS). In fact, the failure of one participant to settle on a given day could create settlement problems for other participants who may be relying on credits from the failed institution to settle their own position. As noted above, CHIPS has instituted several controls to alleviate this potentiality, including bilateral credit limits, net debit caps, and collateralization.

The Board of Governors of the Federal Reserve System's payment system risk reduction program (FRRS 9-1005) is designed to control and reduce the intraday credit risks to depository institutions and the Federal Reserve. The policy establishes intraday payments system cap procedures based on a financial institution's own self-assessment and defines the role that the Federal Reserve and other financial institution supervisors will perform in monitoring, examining and counseling depository institutions regarding these matters.

EXAMINATION CONCERNS

There are three primary wholesale EFT examination objectives:

- To minimize systemic risk from payment activities.
- To identify weaknesses in payments operations that could jeopardize the condition of the bank.
- To assure that proper records are available to assist law enforcement authorities pursuing illegal payments activities.

Examiners should be aware of the various levels of

risk in funds transfer operations, the potential effect of such risk on the examined institution, and the associated regulatory policies established to control these risks. Funds transfer examination procedures should include evaluations of credit risks, operational controls, communications controls, and audit activities. Also refer to the *Guide to the Federal Reserve's Payments System Risk Policy* for additional guidance.

Evaluation of Credit Risks

Financial institutions should be able to monitor and control their overall position across all payment systems in which they participate. Institutions also should monitor the position of individual customers and control the amount of intraday credit extended to each customer within approved credit limits. Guidelines should be established regarding payments that may exceed approved intraday and overnight overdraft limits, including the consideration that is given to projected incoming payments.

The examination procedures applied to these credit exposures should include:

- Review of established customer credit limits and of the frequency and scope of internal credit reviews. In the absence of preauthorized limits, examiners should determine the process for management approval of daylight overdrafts. Authorization should be within the lending authority of approving officers.
- Review of reporting and approval procedures for payments exceeding established credit limits to ensure that approvals are made by officers with sufficient lending authority.
- Review of intraday overdrafts incurred for compliance with established limits, approval and reporting requirements.
- Review of arrangements/agreements regarding collateralization of credit exposures.

Overnight overdrafts should be reviewed as part of the appraisal of the examined institution's loan portfolio. The examination procedures applied to these transactions should include:

- Analysis of credit worthiness of all borrowers with amounts outstanding in excess of the credit line selected for the overall examination. The credit evaluation procedures should be the same as those applied to any other form of short-term credit.
- Review of reporting and approval procedures for overdrafts and settlement credits exceeding established limits.
- Assessment of reporting and approval procedures for payments against uncollected funds.

Private Netting System

The Federal Reserve has instituted minimum risk management standards for private multilateral large-dollar payments networks and their participants (FRR 9-1021). In order to satisfy these standards, the Federal Reserve expects that individual large-dollar multinational netting systems will utilize the following risk management measures, or their equivalent:

- Each participant must establish bilateral net credit limits – the maximum value of transfers it is willing to receive in excess of the value sent on that network.
- Net debit caps should be established for each participant in the network and monitored in real time.
- The network must develop and implement a system that would not allow the participant to breach either its bilateral net credit limit or sender net debit cap.
- The network must establish liquidity resources, such as cash or collateral, at least equal to the largest single net position.
- The network must establish rules and procedures for the sharing of credit losses among network participants.

Evaluation of Operational and Communications Controls

The evaluation of an institution's operational controls relating to funds transfer activities should be coordinated with the overall examination efforts

for the institution to avoid duplication of effort. For example, separate funds transfer and payment systems risk reviews are performed, outside the IS examination, in some institutions. The objective of such reviews is to determine that the internal controls in these areas are effective in minimizing the possibility of fraudulent transfers and losses due to errors and omissions resulting from a poor operating environment. The following sections discuss recommended operational and communications controls for funds transfer activities.

Operational Controls

Basic internal control routines must be in effect for any funds transfer operation to ensure that overall integrity is maintained. However, depending on the size of operations, certain steps may not be applicable for some institutions. The Board of Governors of the Federal Reserve System has issued a *Funds Transfer Activities Uniform Examination Procedures Manual* that includes an Internal Control Questionnaire. In addition, the Bank Administration Institute (BAI) published *Process and Control Guidelines for Wholesale Funds Transfer Systems*, which provides control guidelines. The BAI publication divides the scope of funds transfer operations into three general categories: outgoing transactions, transfer system processing, and incoming credit transactions.

Outgoing Transaction Guidelines:

Recommended control objectives for a wholesale funds transfer system:

- Ensure that an outgoing instruction is recorded accurately and that the original instruction is protected from loss or alteration.
- Authenticate the identity and authority of the sender and ensure the accuracy and completeness of the outgoing instruction.
- Ensure that collected balances are available and that they are held for the outgoing instruction. Any deviations must be considered a credit decision.
- Ensure that the original unaltered outgoing instruction is entered into the internal accounting

].

- Maintaining a physically secure environment.
- Implementation of a comprehensive disaster recovery program.
- Standards for developing or purchasing funds transfer systems software and hardware acquisition.
- Personnel hiring and dismissal policies.
- Organizational reporting controls.
- Audit reviews of funds transfer activities.
- Provisions for maintaining compliance with regulatory reporting and review procedures.

Communications Controls

Telecommunications systems employed for EFT can range from a simple connection between the institution and payments system (e.g., Fedline) to terminal connections with customers that pass through the institution's funds transfer system directly to the payments systems. A data security program must be in place that covers each interface and storage point of the system. These may consist of personal identification numbers, passwords or other identifying keys. Also, it may include account numbers, balances, and financial data relating to transactions.

Financial institutions should use encryption as a means of protecting data throughout the EFT system. Encrypting data during transmission allows the institution to scramble the contents of message/payment orders during transmission and limit the value of that information to an interloper even if a transmission is successfully intercepted. Nevertheless, financial institutions should exercise control over data processing personnel who have access to communications equipment and can monitor and record data flowing in clear text from encryption devices.

Disaster Recovery

In view of the criticality of funds transfer operations for the financial institution, its customers

and the related financial community, it is imperative that continuity of operations be maintained. A comprehensive and tested disaster recovery plan must be in effect for each financial institution covering all phases of the operation including:

- Computer equipment.
- Message systems (e.g., SWIFT, telex, telephones, terminals etc.).
- Data entry/receipt terminals (e.g., internal, customers, funds transfer networks, etc.).
- Communications equipment (e.g., terminals, telephone, etc.).
- Communications lines.
- Personnel.
- Physical plant.
- Supplies.
- Transportation.

Backup of EFT Systems

In the event that a financial institution's primary system becomes inoperable, the financial institution should have backup procedures commensurate to the significance and volume of the system. The procedures should cover temporary and long-term conditions as well as conditions related to the network and in-house operations. While reestablishing communications is an important factor, immediate concerns should center on the recovery and settlement of transactions in process and ensuring that security and confidentiality of customer data, PINs, account numbers, and balances are not breached. EFT systems backup should be included in financial institutions' overall emergency procedures and disaster recovery plans. Backup plans should be periodically evaluated and tested for adequacy and feasibility.

Insurance

Although computer related employee defalcations are normally covered, financial institution blanket

bond policies normally exclude certain types of electronic funds transfer activities from standard coverage. Separate coverage for ATM, POS and other EFT systems are available and should be suggested to management, particularly if potential risk exposure exists. A decision to self insure an EFT network should be made by the board of directors only after a briefing on the level of exposure. Coverage that can be obtained through riders include:

- Electronic Data Processor Coverage – This is an optional coverage that extends the definition of employee to include outside data processors of personnel.
- Electronic Funds Transfer Coverage – This optional rider covers fraud losses assumed as the result of the debiting or crediting a customer's account based on any electronic instructions, including an EFT system, originating from:
 - Another financial institution.
 - An automated clearing house.
 - Fedwire.
 - CHIPS.
 - SWIFT.

This rider contains a clarifying clause that excludes voice communication by telephone.

- ATM and POS Coverage – The use of ATMs also may require the attachment of a restrictive rider which may exclude any loss due to the unauthorized use of access cards. Each ATM location must be covered by specific amounts of insurance. Regarding POS transactions, many fidelity bonds, covering retailers, have similar exclusions for EFT which will, in effect, leave the store clerks unbonded. However, specialized EFT insurance providing coverage for ATM and POS systems is available. Coverage may be extended to include impostor terminals and errors and omissions through telephone bill paying and automatic transfers.

Audit Activities

An evaluation of the institution's audit function must be performed 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 should focus on:

- The scope and frequency of the internal audit program with regard to funds transfer activities.
- The adequacy of the audit program in relation to the Examination Work Program.
- Audit reports to determine any control/operating problems disclosed since the previous examination and what corrective measures were taken by management.
- Audit workpapers to ensure that they document adherence to prescribed audit procedures.
- IS audit coverage of new system enhancements and development projects.
- External audit findings and recommendations.

Regulations Governing EFT Transactions

The Electronic Funds Transfer (EFT) Act is the primary federal law governing consumer rights in an EFT transaction involving a consumer asset account. This law requires that the consumer be provided an initial disclosure statement, a periodic disclosure statement, and terminal receipts for all EFT transactions. It also provides for consumer protection for preauthorized debits or credits to an account. It imposes limits on consumer liability for unauthorized transactions and restricts the ability of financial institutions to issue unsolicited EFT access devices (plastic cards). A consumer's right to have the financial institution investigate and resolve billing errors and limitations on the compulsory use of EFT systems also are included in the EFT act. Regulation E, issued by the Federal Reserve, implements the EFT Act.

Section 205.3 of the EFT Act excludes certain transfers from its coverage, including:

- Transfers made through wholesale wire transfer systems, such as Fedwire and CHIPS.
- Securities transfers.

-
- Certain automatic transfers between a consumer's accounts at the same institution.
 - Telephone transfers not made pursuant to a written agreement.

Also, many states have statutes regulating EFT transactions, which are generally patterned after federal legislation. State EFT laws are not preempted except to the extent that they are inconsistent with federal law. However, they are not preempted if they provide more protection than the federal statute.

As previously noted, rules for wholesale wire transfers regarding the rights, obligations, and liabilities of the parties to funds transfers are established by UCC4A and Fedwire funds transfers are governed by the Federal Reserve's Regulation J, Subpart B, which incorporates the provisions of UCC4A. Fedwire book-entry securities transfers are governed principally by federal regulations promulgated by the Department of the Treasury and the various agencies whose securities are held on the books of the Federal Reserve Banks. In addition, most states have adopted the revised Uniform Commercial Code Article 8, which addresses securities safekeeping and transfer arrangements that do not directly involve the Federal Reserve Banks.

MONEY LAUNDERING AND WIRE TRANSFER ISSUES

As financial institutions, law enforcement agencies, and financial regulators have increased their scrutiny of cash transactions, money launderers have become more sophisticated in using all services and tools available to launder cash and move funds, including the wire transfer systems. This section will provide some background and information on how the different wire transfer systems are used by money launderers, and what IS examiners should consider when reviewing a financial institution's wire transfers operations with regard to the Bank Secrecy Act (BSA). In all cases where an overview by an IS examiner surfaces BSA or Office of Foreign Asset Controls (OFAC) related concerns a reference should be made back through the EIC or the area BSA subject matter expert for additional support.

While there are many ways for money launderers to use the wire system, the objective for most money launderers is to aggregate funds from different accounts and move those funds through accounts at different banks until the origins of the funds cannot be traced. Most often this involves moving the funds out of the country, through a bank account in a country with strict bank secrecy laws, and possibly back into the United States. Money laundering schemes uncovered by law enforcement agencies show that money launderers use the wire system to aggregate funds from multiple accounts at the same bank, wire those funds to accounts held at other U.S. banks, consolidate funds from these larger accounts, and ultimately wire the funds to offshore accounts.

Unlike cash transactions, which are more closely monitored, Fedwire transactions and banks' wire rooms are designed to quickly process approved transactions. Wire room personnel usually have no knowledge of the customer or the purpose of the transaction. Therefore, once cash has been deposited into the banking system, money launderers use the wire system because it is more likely that the transactions can be processed with little or no scrutiny.

BSA RECORDKEEPING FOR FUNDS TRANSFER ACTIVITIES

Recent changes to the Financial Recordkeeping and Reporting of Currency and Foreign Transactions – 31 CFR 103, specifies certain reporting and recordkeeping requirements for wire transactions of \$3,000 or more.

In addition to these regulatory changes, the Federal Financial Institutions Examination Council issued a policy statement addressing the use of large-value funds transfer for money laundering. The revised regulation and the FFIEC encourages financial institutions to support law enforcement efforts in this area by including, to the extent practical, complete originator and beneficiary information when sending payment orders, including those sent through Fedwire, CHIPS and SWIFT.

These amendments to 31 CFR 103 require each financial institution involved in wire transfer

activity to collect and maintain certain information on the payment order for five years. This additional information includes the name, address, and account number of the originator, and the name, address, and account number of the beneficiary where practical. If the originator or beneficiary are not customers of the institutions, the banks shall attempt to verify the identification information.

WIRE TRANSFER CONTROL CONCERNS

The following list of wire transfer related activities/transactions in a financial institution warrants further attention by management. The appearance of a transaction with these characteristics or features on the list does not mean that it necessarily involves illicit activity, only that it requires closer scrutiny. Many, if not most, listed transactions may be found upon closer inspection to reflect legitimate business activity. However, a financial institution must know its customer to make an informed decision as to the suspicious nature of a transaction. Also a transaction may be suspicious for reasons other than those previously listed.

- Sending and receiving wire transfers (to/from bank secrecy haven countries), without an apparent business reason or when they are inconsistent with the customer's business or history.
- Periodic wire transfers from a personal account(s) to bank secrecy haven countries.
- Frequent or large volume of wire transfers to and from offshore institutions (banking centers).
- Deposits of funds into several accounts, usually in amounts below a specified threshold, and then consolidated into one master account and transferred outside of the country.
- Large volume of deposits to several different accounts with frequent transfer of major portions of the balances to a single account at the same or another institution.
- Instructions to a financial institution to wire

transfer funds abroad and to expect an incoming wire transfer of funds (in an equal amount) from other sources.

- Regular deposits or withdrawals of large amounts of cash, using wire transfers to, from, or through countries that are either known sources of narcotics or whose bank secrecy laws enable money laundering.
- Cash/funds or proceeds of a cash deposit wire transferred to another country without changing the form of currency.
- Many small incoming wire transfers of funds received or deposits made using checks and money orders, and all but a token amount almost immediately wire transferred to another city or country, in a manner inconsistent with the customer's business or history.
- Wire transfers received and monetary instruments purchased immediately for payment to another party.

The internal policies developed by management should address *all* business units of the financial institution including: teller and currency operations, sale of monetary instruments, wire transfers, private and correspondent banking, and the fiduciary, loan, international, credit card, and discount brokerage departments, as appropriate.

WIRE TRANSFER MESSAGE

A wire transfer message contains, by design, a minimal amount of information. As discussed in more detail below, Fedwire messages must contain primary information consisting of the sender's and receiver's name and ABA routing number, the amount of the transfer, a reference number, and certain other control information. These messages may contain certain supplementary information, such as the name of the originating party, the name of the beneficiary, the beneficiary's account number, a reference message for the beneficiary, and other related information.

For purposes of an examination, it is important to be able to identify certain information on the message. The supplementary information is identified using three letter codes. These codes

are identified below, but not all information will appear in all messages. In some messages, there may not be any supplementary information at all.

Product Codes These codes identify the type of transfer and are followed by a slash.

- BTR/ *Bank Transfer*, the beneficiary is a bank.
- CTR/ *Customer Transfer*, the beneficiary is a non-bank.
- DEP/ *Deposit to Sender's Account*.
- DRW/ *Drawdown*
- FFR/ *Fed Funds Returned*
- FFS/ *Fed Funds Sold*

Field Tags These codes identify certain supplementary information about the transfer and consist of three letters followed by an equals sign.

- ORG= *Originator*, initiator of the transfer.
- OGB= *Originator's Bank*, bank acting for the originator of the transfer.
- IBK= *Intermediary Bank*, the institution(s) between the receiving institution and the beneficiary's institution through which the transfer must pass, if specified by the sending institution.
- BBK= *Beneficiary's Bank*, the bank acting as financial agent for the beneficiary of the transfer.
- BNF= *Beneficiary*, the ultimate party to be credited or paid as a result of a transfer.
- RFB= *Reference for the Beneficiary*, reference information enabling the beneficiary to identify the transfer.
- OBI= *Originator to Beneficiary Information*, information to be conveyed from the originator to the beneficiary.
- BBI= *Bank to Bank Information*, miscellaneous information pertaining to the transfer.
- INS= *Instructing Bank*, the institution that instructs the sender to execute the transaction.

Identifier Codes Two letter codes preceded by a slash and followed by a hyphen used to identify or designate a number important to the transfer.

- /AC- Account number.
- /BC- Bank identifier code
- /CH- CHIPS universal identifier.
- /CP- CHIPS participant identifier.
- /FW- Federal Reserve routing number.
- /SA- SWIFT address.

Advice Method Codes Three letter codes preceded by a slash used to identify the method of advising the beneficiary of transfer.

- /PHN Advise by telephone.
- /LTR Advise by letter.
- /WRE Advise by wire.
- /TLX Advise by telex.+

The following sample message illustrates the format of a Fedwire message and the use of the above codes:

Mode	Status	Mdc
PRODUCTION	FT	INCOMING
Error-Intercept	Rcvr	Type
MSG	123456789	1040
Sndr	Ref #	Amt
987654321	40922	\$1,000,000.00

Sample message text block

ANYBANK NYC/ORG=J.DOE, OSLO
 OGB=BANK OF NORWAY, OSLO AMER NB
 SF/CTR/IBK=AMER NB LOS ANGELES
 BBK=BK OF SOUTH CA, MARIETTA, CA
 BNF = A . B . I N D U S T R I E S / A C - 8 9 -
 34567/PHN/(415)555-5555 RFB=INV0123
 OBI=EQUIP PURCH

Imad
 DATE A1B2345C 678 DATE 1234 DEF5

Omad
 DATEGH67890I 1234 5679012

This Fedwire message shows a transfer from Anybank New York City, to American National Bank, San Francisco, for \$1,000,000.00. Under the *Rcvr* reading is American's routing number. The transfer was originated by J. Doe in Oslo through his bank (the originating bank), the Bank of Norway, Oslo. Bank of Norway sent the funds

to Anybank, which in turn sent the funds to American National Bank. The funds will be sent to the intermediary bank, American National Bank's Los Angeles bank for credit to the bank of the beneficiary, Bank of Southern California, Marietta, CA. The beneficiary of the transfer is A. B. Industries, and the message contains instructions to credit the amount to A. B. Industries' account and advise the company by phone of receipt of the transfer. Mr. Doe sends information that the wire is for payment of invoice number 0123, which was for the purchase of equipment. The *Imad* and *Omad* numbers at the bottom of the message are added by the Fed and identify the date, time, and receiving and sending terminal. For purposes of examining for money laundering, most of the important information will be contained in the supplementary portion of the message with the field tags. Bank personnel can help decipher messages.

INTERNATIONAL ENFORCEMENT

On December 8, 1992, the Federal Financial Institutions Examination Council (FFIEC) issued the following interagency policy statement to address the problem of the use of large-value international funds transfers for money laundering. The law enforcement community both within the United States and abroad has a growing interest in money laundering through funds transfer systems. The FFIEC supports law enforcement's efforts to identify and prosecute money laundering activities involving large-value funds transfer systems. The FFIEC encourages financial institutions to support law enforcement efforts in this area by including, to the extent practical, complete originator and beneficiary information when sending payment orders, including payment orders sent through Fedwire, CHIPS, and SWIFT.

FATF Background

The President of the United States has joined with the leaders of other nations to sponsor a Financial Action Task Force (FATF).¹ The FATF is primarily charged with developing international guidelines to facilitate the identification and prosecution of money laundering activities.

Historically, law enforcement efforts to curtail money laundering activities have focused on the

identification and documentation of currency-based transactions; however, recent investigations have focused on the use of funds transfer systems. The FATF has developed recommendations to provide more complete information about the parties to a funds transfer. This information is useful for law enforcement investigations.

FATF Recommendations

The FATF recommends that the text of every payment order include: the name, address, and account number of the person who initiated the first payment order in the funds transfer (the originator); the beneficiary's name and address, and when possible, account number also should be provided in the message text. The FATF also recommends that the identity of the first bank that accepts a payment order from a nonbank should be noted and retained through all subsequent processing of the funds transfer. (The FATF recognizes that the originator and beneficiary information specified in its recommendations may not be provided in transfers originated in some countries because of provisions contained in local laws.)

In this context, SWIFT and CHIPS have recently issued statements encouraging their participants to include the information specified by the FATF recommendations in funds transfers processed through those systems. The Bank of England has also encouraged financial institutions in the United Kingdom to provide complete originator and beneficiary information when using national, international, and proprietary message transfer systems.

To the extent practical, the council encourages all domestic banking offices to implement the FATF recommendations when sending a payment order over any funds transfer system, including Fedwire, CHIPS, SWIFT, and any proprietary networks.

¹ The FATF was formed as a direct initiative by the heads of state of governments of seven major industrialized countries and the President of the European Communities during an economic summit in July 1989. The total membership of FATF now stands at 28 countries, with the primary representation being law enforcement.

With respect to Fedwire, the council recognizes that the Fedwire format limits the amount of information that can be included in a Fedwire funds transfer. While the Federal Reserve System is exploring changes to the Fedwire format, those changes would require time to implement. In the interim, the FFIEC encourages originating banks to ensure that the nonbank originator, beneficiary, and any instructing bank information is included in each Fedwire funds transfer to the extent possible given the limited size of the Fedwire format and the need to give priority to information necessary for payment processing.

Information concerning the originator and beneficiary may be recorded in the payment order text. For example, if an originator requests depository bank A to transfer funds over Fedwire to a beneficiary of depository bank B, and either the originator or beneficiary information is exceeds the space fields specified for originator or beneficiary information.

When a payment order is received by a bank through one funds transfer system and then executed through another funds transfer system; to the extent practical, information on the originator of the payment order received by the intermediary bank should be included in the payment order sent by the intermediary bank. For example, when a SWIFT message is received by an intermediary bank and subsequently sent to the beneficiary's bank via Fedwire, the originator information on the SWIFT message should be carried forward as space permits to the Fedwire message. If the originator information is lengthy and exceeds the space available in the specified fields, to the extent practical, the remaining information may be included in the message text in optional fields that otherwise will not be used for that payment order.

THE OFFICE OF FOREIGN ASSETS CONTROLS (OFAC)

Another area of consideration which the examiner should address during the review of a wholesale EFT area relates to the Office of Foreign Assets Control (OFAC). This is an agency of Treasury that administers a series of laws that impose economic sanctions against targeted hostile

foreign countries to further U.S. foreign policy and national security objectives. 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 use of economic sanctions goes back to the earliest days of the Republic through trade embargoes, blocked assets controls, travel bans, and other commercial and financial restrictions. There has recently been a dramatic increase in the use of such sanctions on a multinational level through such organizations as the United Nations and the Organization of American States. Management of sanctions on the U.S. side is entrusted to the Secretary of the Treasury.

The U.S. Government mandates that all banks located in the U.S., overseas branches of U.S. banks, and, in certain instances, overseas subsidiaries of U.S. banks, comply with economic sanctions and embargo programs administered under regulations issued by OFAC. In general, such 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).
- 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.
- Are remitted to or through a blocked entity.

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

If a U.S. bank receives instructions to make a payment that falls into one of these categories, it is required to execute the payment order and place the funds into a blocked account. A payment order cannot be canceled or amended 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.

This is not intended to be a comprehensive discussion of the sanctions programs. In all cases

where a non-compliance examiner is reviewing the Wholesale EFT activities of an institution and issues relating to OFAC compliance are discovered contact should be made with the EIC or the agency's Compliance area to determine whether subject matter expert support is necessary. For a complete discussion of legal requirements, consult 31 CFR Part 500 et seq. Users requiring further information or seeking a Treasury authorization should contact the: Office of Foreign Assets Control, Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Washington, D.C. 20220. Phone: (202) 622-2490, or 1-800-540-6322. Fax: (202) 622-1657.

