INTRODUCTION

One of the most important, if not the most important, means by which financial institutions can hope to avoid criminal exposure to the institution by ''customers'' who use the resources of the institution for illicit purposes is to have a clear and concise understanding of the ''customers' '' practices. The adoption of ''know your customer'' guidelines or procedures by financial institutions has proven extremely effective in detecting suspicious activity by ''customers'' of the institution in a timely manner.

Even though not presently required by regulation or statute, it is imperative that financial institutions adopt ''know your customer'' guidelines or procedures to ensure the immediate detection and identification of suspicious activity at the institution. The concept of ''know your customer'' is, by design, not explicitly defined so that each institution can adopt procedures best suited for its own operations. An effective ''know your customer'' policy must, at a minimum, contain a clear statement of management's overall expectations and establish specific line responsibilities. While the officers and staff of smaller banks, Edge corporations, and foreign branches or agencies may have more frequent and direct contact with customers than large urban institutions, it is incumbent upon all institutions to adopt and follow policies appropriate to their size, location, and type of business.

OBJECTIVES OF ''KNOW YOUR CUSTOMER'' POLICY

- A ''know your customer'' policy should increase the likelihood that the financial institution is in compliance with all statutes and regulations and adheres to sound and recognized banking practices.
- A ''know your customer'' policy should decrease the likelihood that the financial institution will become a victim of illegal activities perpetrated by its ''customers.''
- A ''know your customer'' policy that is effective will protect the good name and reputation of the financial institution.
- A ''know your customer'' policy should not interfere with the relationship of the financial institution with its good customers.

CONTENTS OF ''KNOW YOUR CUSTOMER'' POLICY

In developing an effective ''know your customer'' policy it is important to note that appearances can be deceiving. Potential customers of a financial institution may appear to be legitimate, but in reality are conducting illicit activities through the financial institution. Likewise, legitimate customers may be turned away from the institution because their activities are perceived to have a criminal tone. It is also important to realize that various influences on legitimate customers may transform such customers into wrongdoers.

At the present time there are no statutorily mandated procedures requiring a ''know your customer'' policy or specifying the contents of such a policy. However, in order to develop and maintain a practical and useful policy, financial institutions should incorporate the following principles into their business practices:

- Financial institutions should make a reasonable effort to determine the true identity of all customers requesting the bank's services;
- Financial institutions should take particular care to identify the ownership of all accounts and of those using safe-custody facilities;
- Identification should be obtained from all new customers;
- Evidence of identity should be obtained from customers seeking to conduct significant business transactions;
- Financial institutions should be aware of any unusual transaction activity or activity that is disproportionate to the customer's known business.

An integral part of an effective ''know your customer'' policy is a comprehensive knowledge of the transactions carried out by the customers of the financial institution. Therefore, it is necessary that the ''know your customer'' procedures established by the institution allow for the collection of sufficient information to

develop a "customer profile." The primary objective of such procedures is to enable the financial institution to predict with relative certainty the types of transactions in which a customer is likely to be engaged. The customer profile should allow the financial institution to understand all facets of the customer's intended relationship with the institution, and, realistically, determine when transactions are suspicious or potentially illegal. Internal systems should then be developed for monitoring transactions to determine if transactions occur which are inconsistent with the "customer profile." A "know your customer" policy must consist of procedures that require proper identification of every customer at the time a relationship is established in order to prevent the creation of fictitious accounts. In addition, the bank's employee education program should provide examples of customer behavior or activity which may warrant investigation.

IDENTIFYING THE CUSTOMER

As a general rule, a business relationship with a financial institution should never be established until the identity of a potential customer is satisfactorily established. If a potential customer refuses to produce any of the requested information, the relationship should not be established. Likewise, if requested follow-up information is not forthcoming, any relationship already begun should be terminated. The following is an overview of general principles to follow in establishing customer relationships:

Personal Accounts

1. No account should be opened without satisfactory identification, such as:
   - a driver's license with a photograph issued by the State in which the bank is located; or
   - a U.S. passport or alien registration card, together with:
   - a college photo identification card;
   - a major credit card (verify the current status);
   - an employer identification card;
   - an out-of-State driver's license; and/or
   - electricity, telephone.
2. Consider the customer's residence or place of business. If it is not in the area served by the bank or branch, ask why the customer is opening an account at that location.
3. Follow up with calls to the customer's residence or place of employment thanking the customer for opening the account. Disconnected phone service or no record of employment warrant further investigation.
4. Consider the source of funds used to open the account. Large cash deposits should be questioned.
5. For large accounts, ask the customer for a prior bank reference and write a letter to the bank asking about the customer.
6. Check with service bureaus for indications the customer has been involved in questionable activities such as kiting incidents and NSF situations.
7. The identity of a customer may be established through an existing relationship with the institution such as some type of loan or other account relationship.
8. A customer may be a referral from a bank employee or one of the bank's accepted customers. In this instance, a referral alone is not sufficient to identify the customer, but in most instances it should warrant less vigilance than otherwise required.

Business Accounts

1. Business principals should provide evidence of legal status (e.g. sole proprietorship, partnership, or incorporation or association) when opening a business account.
2. Check the name of a commercial enterprise with a reporting agency and check prior bank references.
3. Follow up with calls to the customer's business thanking the customer for opening the account. Disconnected phone service warrants further investigation.
4. When circumstances allow, perform a visual check of the business to verify the actual existence of the business and that the business has the capability of providing the services described.
5. Consider the source of funds used to open the account. Large cash deposits should be questioned.
6. For large commercial accounts, the following information should be obtained:

- a financial statement of the business;
- a description of the customer's principal line of business;
- a list of major suppliers and customers and their geographic locations;
- a description of the business's primary trade area, and whether international transactions are expected to be routine; and
- a description of the business operations i.e., retail versus wholesale, and the anticipated volume of cash sales.

LOAN TRANSACTIONS

It is important to realize that relationships with a financial institution that take a form other than deposit accounts can be used for illicit purposes. Loan transactions have become a common vehicle for criminal enterprises that wish to take advantage of the proceeds of their illegal activities. Therefore, prudent financial institutions should apply their "know your customer" policy to customers requesting credit facilities from the institution.

SUSPICIOUS CONDUCT AND TRANSACTIONS

In making a determination as to the validity of a customer, there are certain categories of activities that are suspicious in nature and should alert financial institutions as to the potential for the customer to conduct illegal activities at the institution. The categories, broadly defined, are:

- Insufficient, false, or suspicious information provided by the customer.
- Cash deposits which are not consistent with the business activities of the customer.
- Purchase and/or deposits of monetary instruments which are not consistent with the business activities of the customer.
- Wire transfer activity which is not consistent with the business activities of the customer.
- Structuring of transactions to evade recordkeeping and/or reporting requirements.
- Funds transfers to foreign countries.

The general categories, delineated above, can be broken down into various functions of the financial institution. Set forth below are more specific suspicious activities as related to the various functions of the financial institution:

Tellers and Lobby Personnel

- Customer is reluctant to provide any information requested for proper identification.
- Customer opens a number of accounts under one or more names and subsequently makes deposits of less than $10,000 in cash in each of the accounts.
- Customer is reluctant to proceed with a transaction after being informed that a Currency Transaction Report (CTR) will be filed, or withholds information necessary to complete the form.
- Customer makes frequent deposits or withdrawals of large amounts of currency for no apparent business reason, or for a business which generally does not involve large amounts of cash.
- Customer exchanges large amounts of currency from small to large denomination bills.
- Customer makes frequent purchases of monetary instruments for cash in amounts less than $10,000.
- Customers who enter the bank simultaneously and each conduct a large currency transaction under $10,000 with different tellers.
- Customer who makes constant deposits of funds into an account and almost immediately requests wire transfers to another city or country, and that activity is inconsistent with the customer's stated business.
- Customer who receives wire transfers and immediately purchases monetary instruments for payment to another party.
- Traffic patterns of a customer change in the safe deposit box area possibly indicating the safekeeping of large amounts of cash.
- Customer discusses CTR filing requirements with the apparent intention of avoiding those requirements or makes threats to an employee to deter the filing of a CTR.
- Customer requests to be included on the institution's exempt list.

Bookkeeping and Wire Transfer Operations

- Customer who experiences increased wire activity when previously there has been no regular wire activity.

- International transfers for accounts with no history of such transfers or where the stated business of the customer does not warrant such activity.
- Customer receives many small incoming wire transfers or deposits of checks and money orders then requests wire transfers to another city or country.
- Customer uses wire transfers to move large amounts of money to a bank secrecy haven country.
- Request from nonaccountholder to receive or send wire transfers involving currency from nonaccountholder near the $10,000 limit or that involve numerous monetary instruments.
- Nonaccountholder receives incoming wire transfers under instructions to the bank to "Pay Upon Proper Identification" or to convert the funds to cashier's checks and mail them to the nonaccountholder.

Loan Officers and Credit Administration Personnel

- Customer's stated purpose for the loan does not make economic sense, or customer proposes that cash collateral be provided for a loan while refusing to disclose the purpose of loan.
- Requests for loans to offshore companies, or loans secured by obligations of offshore banks.
- Borrower pays down a large problem loan suddenly, with no reasonable explanation of the source of funds.
- Customer purchases certificates of deposit and uses them as loan collateral.
- Customer collateralizes loan with cash deposit.
- Customer uses cash collateral located offshore to obtain loan.
- Loan proceeds are unexpectedly channeled off-shore.

INTRODUCTION

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 work, how these systems are used by money launderers, and how examiners should review a bank's wire transfers operations as part of the examination for compliance with the Bank Secrecy Act.

WIRE TRANSFER SYSTEMS

There are three wire transfer systems used in the United States by financial institutions—Fedwire, CHIPS, and S.W.I.F.T. All three systems share the same characteristics of high dollar value of the individual transfers, a real time system, and a widely distributed network of users. There are important differences, however, and these will be discussed below. In order to examine an institution's wire transfer function thoroughly, it is important to understand how the system(s) works. Each of the three wire transfer systems will be looked at below.

Fedwire

Fedwire is the funds transfer system operated by the Federal Reserve System. The Fedwire system may be used by any institution holding an account with a Federal Reserve Bank and it is principally domestic in orientation. It is a real-time system characterized by the instantaneous, irrevocable transfer of funds. As a ''wholesale'' wire transfer system, Fedwire is primarily used to transfer funds between financial institutions and their major corporate customers. There are no restrictions on the minimum dollar size of Fedwire transfers, and individuals and small businesses can and do use Fedwire by going through their financial institution.

A financial institution can originate a Fedwire message in one of two ways—''on-line'' or ''off-line.'' On-line institutions have an electronic connection to the Federal Reserve, and off-line institutions have no such connection and usually telephone the Federal Reserve to initiate a transfer. The large, high volume institutions use a direct computer-to-computer connection with Fed to originate funds transfers over Fedwire, and the other on-line institutions use a leased line connection or a telephone dial-up system to connect a PC to the Fedwire system. Because the settlement of all Fedwire transfers is made through reserve accounts maintained at the Federal Reserve Banks, all transfers go through a Reserve Bank for routing and settlement.

Off-line institutions usually telephone the Fed and give instructions over the phone using a prearranged codeword. The Fed verifies the codeword and enters the message into the electronic system for processing and sending to the receiving institution. Fedwire transfers sent to an off-line institution are credited immediately, and the institution is either notified by phone from the Fed or by copy of the Fedwire message sent to the institution the next day.

The actual transfer of funds in the Fedwire system takes place on the books of the Federal Reserve. For a transfer to an institution in the same Federal Reserve District, the Federal Reserve Bank, upon receiving the Fedwire instructions from the originating institution, debits the account of the originator and credits the account of the receiving institution. For interdistrict transfers, the ''local'' FR Bank debits the account of the originator and credits the account of the ''receiving'' FR Bank, which, in turn, credits the account of the receiving institution.

CHIPS

CHIPS (Clearing House Interbank Payments System) is a privately owned and operated funds transfer system. It is owned and operated by the New York Clearing House Association. CHIPS currently has 128 members who are primarily money center banks in New York, Chicago, and San Francisco as well as large international banks.

CHIPS has its own communications network and processes its own messages for member institutions. During the day CHIPS maintains

the net credit and debit positions of members while routing messages from sender to receiver. Although used primarily for international transfers, CHIPS is used to a small extent for domestic transfers between U.S. banks and can be used as an alternative to Fedwire if both the sending and receiving institutions are CHIPS members.

In CHIPS the transfer of funds does not occur with the sending of the message. Rather, at the end of each day any of the 30 CHIPS settlement participants that are in a net debit position wire funds by Fedwire to the CHIPS account at the New York Fed and CHIPS sends these funds to the banks in a net credit position by Fedwire. This end of day settlement feature is the biggest difference between Fedwire and CHIPS, and it also puts CHIPS participants at risk if a participating bank should fail or is unable to cover its position.

S.W.I.F.T.

SWIFT stands for the Society for Worldwide Interbank Financial Telecommunications. It is a cooperatively owned, non-profit organization which was founded in 1973 to serve the data processing and telecommunications needs of its members. SWIFT currently has members in most countries throughout the world. The membership base is very broad and includes commercial banks, investment banks, securities broker/dealers, and other financial institutions.

As its name implies, SWIFT handles all sorts of telecommunications for its member institutions. Transfers of funds are only one use of SWIFT, others being securities transfers, letters of credit, advices of collection, foreign exchange, and free format information messages. All messages are sent through the SWIFT network, SWIFT's privately owned, worldwide telecommunications network. Because of the availability of Fedwire and CHIPS, SWIFT is used almost exclusively by U.S. banks for international funds transfers and messages.

A SWIFT funds transfer message is simply notification that funds are being transferred. The actual movement of funds is independent of the message, and transfers are effected in two common ways. The first method is to transfer the funds by transferring balances through mutual correspondent banks, and the second method is to settle through Fedwire or CHIPS.

A bank's SWIFT operations are usually located in its international department, although additional terminals with SWIFT access could be located in the foreign exchange department or the securities trading department.

HOW A COMMERCIAL BANK'S WIRE ROOM WORKS

In order to examine the Fedwire operations of a commercial bank, it is important to understand how the ''wire room'' of a commercial bank operates. In the larger banks with a significant volume of wire traffic, there may be a department dedicated to this function. In most banks, however, the Fedwire volume does not justify a full time staff or person, and the sending and receiving of wires may be part-time responsibilities for one or several people. Every bank has its own procedures for handling wires, but there are enough features in common to allow for generic descriptions for large and small banks.

Large Banks

Large banks with a Fedwire volume of several hundred messages per day will most likely use dedicated computer resources for Fedwire—either part of the bank's host computer or a separate minicomputer. These banks utilize a computer-to-computer (computer interface) electronic link with the Fed, which allows for faster transmission of high volumes. The software used for wire transfers, either developed in-house or purchased from a vendor, allows for automatic posting to DDA and general ledger.

The wire room may receive payment orders from several different sources, including authorized personnel from within the bank and corporate customers who may either call the bank, fax instructions, or even have an on-line connection with the bank to send wire instructions and access other bank services. Phone calls to the wire room are recorded for security and audit reasons, and the tapes are usually maintained for a 30 day period. The bank should have procedures in place to verify payment orders. These procedures usually include the use of code words, call backs, and corporate resolutions authorizing certain employees to send wires. Verification and security procedures are

extremely important in light of the potential for high losses.

After a payment order is received, a Fedwire message is entered into the bank's system at an on-line terminal. Before the wire is sent to the Fed, it is sent to a second terminal to be verified for accuracy as well as proper authorization. Only after the payment order is reviewed by the second staff member is it sent to the Fed for processing. This separation of duties is extremely important to ensure security.

The bank's software will maintain data on each day's transfers in several different ways. These might include a listing by 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 for on-line access to trace errors and problems. After the 5 to 7 days, the data may be maintained on microfiche or paper listing.

Smaller Banks

Smaller banks with a low volume of Fedwire transactions will typically have one or several staff members handling the sending and receiving of wires over a connection from the bank's PC to the Fed's mainframe. The PC connection is called Fedline, and the software is supplied by the Fed. The basic procedures for sending and receiving wires are similar to those for the large banks, but the degree of sophistication and separation of duties is not as great. A financial institution should have other back-up controls in place if separation of duties is a problem. These controls can include rotation of duties and officer review of all transactions.

Payment orders to send a wire are received from bank personnel and corporate customers. Individuals who wish to wire funds usually go through their loan officer or account representative who notifies the wire room. Here again, verification is an important security procedure, and records should be kept of all payment order requests, by tapes of phone calls, written records of requests, or other means.

After receiving the payment order, the terminal operator keys the wire message into the PC. Before the message can be sent, it must be verified by a second person (this is the recommended procedure—some small banks allow the same person to key in the wire and verify for sending). Most on-line PC connections to the Fed have two printers attached, one which prints copies of the outgoing messages and the other which prints incoming messages. The bank should maintain the copies of these messages in the continuous paper form for recordkeeping purposes. The unbroken sheet ensures that all messages are accounted for; however, the sequence numbers of the messages should also be checked because messages can occasionally be skipped because of communication problems. In addition, each incoming and outgoing message is assigned a sequence number that also provides an audit trail ensuring that all messages are accounted for.

How Money Launderers Use the Wire System

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 U.S. Money laundering schemes uncovered by law enforcement agencies, for instance through Operation Polar Cap, 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 in countries such as Panama.

Unlike cash transactions, which are 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 of the likelihood that transactions will be processed with little or no scrutiny.

HOW TO READ A 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 the purposes of these examination procedures, 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 backslash.

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 backslash 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 backslash 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	error-intercept
PRODUCTION		FT	INCOMING	MSG
rcvr	type			
121000358	1040			
sndr	ref #	amt		
021000089	4092	$1,000,000.00		

CITIBANK NYC/ORG=J.DOE, LONDON OGB=BANK OF THE NORTH, LONDON

BANK AMER SF/CTR/IBK=B OF A LOS ANGELES BBK=BK OF SAN PEDRO, CA

BNF=H.L. INDUSTRIES/AC-12-34567/PHN/(415)555-1212 RFB=INV8123

OBI=EQUIP PURCH

imad	omad
0504 B1Q0216K 209 05041233 FTB1	0504 L1Q11339K 1391 05041235

This Fedwire message shows a transfer from Citibank, NYC, to Bank of America, San Francisco, for $1,000,000.00. Under the "rcvr" heading is Bank of America's routing number,

and under the ''sndr'' is Citibank's routing number. The transfer was originated by J. Doe in London through his bank (the originating bank), the Bank of the North, London. Bank of the North sent the funds to Citibank, which in turn sent the funds to Bank of America. The funds will be sent to the intermediary bank, Bank of America's Los Angeles bank for credit to the bank of the beneficiary, Bank of San Pedro, San Pedro, CA. The beneficiary of the transfer is H. L. Industries, and the message contains instructions to credit the amount to H. L. 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 8123, 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 the 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.

Amendment to Regulation H
Procedures for Monitoring Bank Secrecy Act Compliance—February 1987*

Effective January 27, 1987, section 208.14 is added to read as follows:

SECTION 208.14—PROCEDURES FOR MONITORING BANK SECRECY ACT COMPLIANCE

(a) *Purpose*. This section is issued to ensure that all state member banks establish and maintain procedures reasonably designed to ensure and monitor their compliance with the provisions of subchapter II of chapter 53 of title 31, United States Code, the Bank Secrecy Act, and the implementing regulations promulgated thereunder by the Department of Treasury at 31 CFR part 103, requiring recordkeeping and reporting of currency transactions.[13]

(b) *Establishment of compliance program*. On or before April 27, 1987, each bank shall develop and provide for the continued administration of a program reasonably designed to ensure and monitor compliance with the recordkeeping and reporting requirements set forth in subchapter II of chapter 53 of title 31, United States Code, the Bank Secrecy Act, and the implementing regulations promulgated thereunder by the Department of Treasury at 31 CFR part 103. The compliance program shall be reduced to writing, approved by the board of directors, and noted in the minutes.

(c) *Contents of compliance program*. The compliance program shall, at a minimum—

(1) provide for a system of internal controls to ensure ongoing compliance;

(2) provide for independent testing for compliance to be conducted by bank personnel or by an outside party;

(3) designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance, and

(4) provide training for appropriate personnel.

---

* The complete regulation as amended effective January 27, 1987, consists of—
- a regulation pamphlet dated May 1942 and
- this slip sheet.

13. Recordkeeping requirements contained in this section have been approved by the Board under delegated authority from the Office of Management and Budget under the provisions of chapter 35 of title 44, United States Code, and have been assigned OMB No. 7100–0196.

Essential to the financial institution's ability to comply with the rules and regulations of the Bank Secrecy Act and ensure that the institution does not become involved in illicit activities, is an effective internal compliance program. It should be noted that, by statute (12 U.S.C. 1818(s)), Federal banking agencies are required to issue orders requiring an institution to ''cease and desist from its violation'' when an institution has failed to establish and maintain adequate internal compliance procedures or an institution has failed to correct any problem with the internal compliance procedures that were previously identified as being deficient.

At a minimum, an internal compliance program must:

- Provide for a system of internal controls to ensure ongoing compliance;
- Provide for independent testing of compliance;
- Designate an individual responsible for day-to-day coordination and monitoring of compliance; and
- Provide training for appropriate personnel.

These items are the basic elements of a good compliance program. In order to maintain a program that ensures compliance on an ongoing basis and helps to prevent abuse of the institution by those who might wish to use the institution for illegal purposes, financial institutions must involve several areas of operation and administration.

SENIOR MANAGEMENT

Senior management must show a commitment to compliance by the financial institution by:

- Establishing a strong compliance plan that is fully implemented and approved by the board of directors of the institution;
- Requiring that senior management be kept informed of compliance efforts, audit reports and any compliance failures with corrective measures instituted;
- Including regulation compliance within the job description and job performance evaluation of institution personnel; and
- Conditioning employment on regulation compliance.

INTERNAL AUDITORS

An internal auditing department within the financial institution should be established with responsibilities which include:

- Performing transaction testing to ensure that the institution is following proscribed regulations;
- Performing testing of employees to assess knowledge of regulations and procedures;
- Reviewing written procedures and training programs for completeness and accuracy; and
- Reporting all findings to senior management.

LARGE CURRENCY INTERNAL CONTROL

Financial institutions should have the ability to detect and monitor large currency transactions occurring at the financial institution to ensure that such transactions are not being conducted for illegitimate purposes. With the advent of the ''$3,000 rule'' imposing recordkeeping requirements for cash purchases of certain monetary instruments of between $3,000 and $10,000, the same principles of currency transaction monitoring should be applied to this function, as well.

EXEMPTION PROCEDURES

For those financial institutions that maintain exemptible customers from the CTR reporting requirements under the existing rules (as opposed to the interim exemption rule), it is imperative that regular monitoring of the exemption process be undertaken. The institution must be able to ensure that exempted customers are complying with the limitations of their exemption and that, on a regular basis, exempted customers transactions are reviewed. Any abnormalities in the exemption process by the institution or the customer should be readily identifiable through the internal compliance program.

TRAINING

Financial institution personnel should be trained in all aspects of regulatory and internal policies

and procedures. An effective training program should include:

- All compliance officers, audit and/or independent review personnel and other customer contact personnel, including tellers, customer service representatives, lending officers and private or personal banking officers, should be trained regarding policies and procedures, as well as common money laundering schemes and patterns;

Continuous and updated training to ensure personnel is provided with the most current and up to date information.

COMPLIANCE RESPONSIBILITY

An individual should be designated as a compliance contact, with day-to-day responsibility for the compliance program.

The Bank Secrecy Act and Money Laundering Statutes were passed by Congress to help facilitate the identification and prosecution of individuals involved in illegal activities for profit. In 1984, the Detroit Computing Center (DCC) was chosen to collect, perfect and input to the CBRS Data Base, millions of documents required to be furnished under the laws. These documents consist of the following: **Currency Transaction Reports (CTR's - Form 4789)** required to be filed by Financial Institutions on cash transactions over $10,000; **Currency Transaction Reports by Casinos (CTRC - Form 8362)** required to be filed by casinos on cash transactions over $10,000; **Report of Cash Payments Received in a Trade or Business (Form 8300)** to be filed by anyone in a trade or business receiving payments in cash totalling $10,000 or more in a single or related transaction; **Report of Foreign Bank and Financial Accounts (FBAR - TDF 90-22.1)** required to be filed annually by any U.S. citizen having financial interest in or signature authority over any foreign bank account exceeding $10,000 in total value at any time during the calendar year, or multiple accounts that in the aggregate exceed $10,000; **Report of International Transportation of Currency or Monetary Instrument Reports (CMIR - Form 4790)** are loaded from tapes received from U.S. Customs Service, these documents are filed when amounts greater than $10,000 in cash or monetary instruments are taken across any U.S. Borders; **Suspicious Activity Report (SAR)** are filed by Financial Institutions on any unusual or suspicious cash transactions of any amount; and **Form CF-7501 Entry Summary** is received from Customs electronically for any commodity subject to Excise Tax. In early 1994, the **Information Return for Federal Contract Document (Form 8596)** was added to the CBRS. This Collection document allows for tracking of contracts being issued by different Federal Agencies. As of the end of January 1996, the CBRS Data Base contained over 90,000,000 information documents.

The CBRS Data Base can be accessed by special agents, revenue agents and revenue officers through portable computers through a telephone system or CDN lines. There are approximately 15,000 user-id/passwords assigned to users of the CBRS, including staff of the Board of Governors of the Federal Reserve System. Additionally, tapes of all documents, except 8300s, are furnished to U.S. Customs and subsequently added to the Treasury Enforcement Communications Service's (TECS) data base for use by law enforcement agencies. Tape files are also sent to the states of California, Arizona, New York, Florida, Illinois and Texas for CTR documents filed in their respective states. Project GATEWAY has been established to allow selected officials from all states to have hands-on access to the query data base.

The system can be used to identify bank accounts, secret cash, leads to assets and foreign bank accounts, and a myriad of other useful information for compliance and other law enforcement personnel. For example, Federal Reserve staff utilize the data base to verify timely filings by financial institutions.

The CBRS Data Base is maintained at the DCC, where the processing of the data is controlled. Three branches comprise the working group for the project: Systems, Edit/Error Resolution, and the Compliance Branch. The Compliance Branch has the overall responsibility of providing authoritative information and assistance in person, by telephone, or by correspondence to financial institutions and their representatives as they apply to the provisions of the Bank Secrecy Act.

Banks, as defined in the regulations, have the authority to exempt from reporting transactions of certain types of entities specifically enumerated in the regulations. These entities are maintained on bank exempt lists. The Compliance Branch corresponds with banks to obtain these exempt lists and conducts a limited review on such lists once received.

If a bank believes that certain circumstances warrants the exemption of an entity not specifically enumerated in the regulation, it must request a ''Special Exemption'' from IRS. These requests for ''Special Exemptions'' are granted or denied by the Compliance Branch.

Research of various data bases and files is done so that certified transcripts/documents can be prepared by use in grand jury investigations and criminal/civil court cases. Periodically, the employees may be called upon to serve as witnesses (court testifiers) to introduce these documents as evidence during a trial.

Also, as a part of the document processing function, many documents are perfected by telephone contact and/or correspondence. Telephone contact is made with financial institutions when an unsatisfactory response is received as a result of computer generated correspondence on an incomplete Currency Transaction Report. The objective is to make the Form 4789 processable. If the telephone contact is unsuccessful, the Form 4789 is deemed unsatisfactory and thus forwarded to Treasury for further review.

BSA COMPLIANCE BRANCH, DETROIT COMPUTING CENTER

The BSA Compliance Branch of the Currency Reporting & Compliance Division has been delegated responsibility for providing authoritative information on certain provisions of the Bank Secrecy Act (''BSA''). This guidance is provided in person, by telephone or through correspondence to financial institutions and their representatives.

The BSA Compliance Branch will verify receipt of CTRs at the request of a financial institution. There is a research fee charged for this service of $20.00 for up to ten documents and $2.00 for each additional document. To receive copies, add 15 cents per document requested.

A synopsis of the duties of the BSA Compliance Branch as follows:

Outreach Program:

- Speakers for Banking/Professional Seminars

Financial Institution Services

- Customer service lines for answering technical and form completion questions
- Grant/deny request for special exemptions
- Process requests for backfiling determinations
- Review bank Exemption Lists
- Provide verification of receipt and copies of CTRs
- Staff a toll-free suspicious transaction reporting hot line

CID Agents, IRS and Other Law Enforcement Services

- Copies of BSA/Title 26 documents including true copy certifications for court
- Research and certification of ''negative'' or ''no document filed'' results
- Testify at trials as Custodian of the Record

BSA Compliance Branch—Contact Points

BSA Compliance Branch Office
David Gooding, *Chief*
Tamika Brown, *Secretary*
P.O. Box 32063
Detroit, Michigan 48232-0063
Voice (313) 234-1576
Fax (313) 234-1614

BSA Compliance Review Group

Candace Walls, *Chief*	(313) 234-1597
Vergary Fortune, *Secretary*	
Outside Customers (financial institutions)	(313) 234-1613
IRS Employees/law enforcement	(313) 234-1597

Lead BSA Representative

Marion Formigan	(313) 234-1602

BSA Representatives (BSAR)

Freda Allen	(313) 234-1610
Phyllis Brown	(313) 234-1599
Yvonne Covington	(313) 234-1600
Lyndon Ford	(313) 234-1601
Wanda Hampton	(313) 234-1612
Elva Jackson	(313) 234-1603
Elizabeth Johnson	(313) 234-1604
Ronald Kaczynski	(313) 234-1605
Marian Kirkland	(313) 234-1607
Linda Krych	(313) 234-1608
Annie McCarty	(313) 234-1609
Marie Morris	(313) 234-1610
Linda Townsend	(313) 234-1611

BSA Support Group I

Chief, Yvonne Davis	(313) 234-1594

Tax Examining Assistants (TEA)

Minnie Blair	(313) 234-1580
Cynthia Drew	(313) 234-1590
Sharon McMorris	(313) 234-1585

Mary Rogers	(313) 234-1586
Linda Taylor	(313) 234-1588

Other Numbers/Addresses of Interest

Jim Bahnke *Chief, Tax Systems Division*	(313) 234-1066
Pat Donaldson *Chief, CTR Branch*	(313) 234-1401 (voice) (313) 234-1402 (fax)
Henry James *Chief, Currency Rep. & Compl. Div.*	(313) 234-1062
Derrick Moore *Chief, Edit/Error Res. Br.*	(313) 234-1636
CTR Corrective Correspondence	(313) 234-1657
Ben McMakin *CID Coordinator*	(313) 234-1077
Cathy Swickle *Public Affairs Officer*	(313) 234-1052
Magnetic Media Hotline	(313) 234-1445
Suspicious Transaction Hotline	(800) 800-2877
Bank Secrecy Act (BSA) Bulletin Board	(313) 234-1453
IRS Forms (including Form 4789)	(800) 829-3676
IRS Taxpayer Service Toll-Free	(800) 829-1040

LOGON CODES

Each organization is required to use specified Client and Office codes in the Accounting Data field when logging into the CBRS. Federal Reserve System staff must first obtain an authorizaion code in order to access the CBRS system. Each Reserve Bank has established a Bank Secrecy Act contact to access the CBRS system. Additional requests for logon i.d.'s should be mailed to:

Mr. Richard Small
Special Counsel
Board of Governors of the Federal Reserve System
Mail Stop 173
Washington, D.C. 20551

SPECIAL REQUEST PROCEDURE (REPORTS AND/OR TAPE)

In situations where on-line or download data is insufficient for your needs, a special report or data tape may be requested from the DCC. Non-IRS personnel should mail requests to the Special Assistant for Financial Enforcement at the DCC. For Federal Reserve System staff, the request should be routed through the Special Counsel at the Federal Reserve Board.

INTRODUCTION

Pursuant to Federal Reserve regulations, all institutions supervised by the Federal Reserve are required to report suspicious transactions using the Suspicious Activity Report (''SAR''). The SARs are maintained in a computerized database that is managed by the Internal Revenue Service. All Reserve Banks have on-line access to the SAR database.

REVIEW OF SUSPICIOUS ACTIVITY REPORTS

Prior to the start of an examination, the SAR database should be reviewed as to all SARs related to the financial institution to be examined. This review should be an integral part of the examination preparation, as it can provide valuable information to assist in developing the appropriate scope of the review.

SEARCHING THE SAR DATABASE

Instructions for accessing the SAR database can be found in the ''Internal Revenue Service User's Guide.'' Additional guidance on the use of the SAR database can be obtained from the Bank Secrecy Act coordinator at each Reserve Bank.

IDENTIFICATION OF SIGNIFICANT SUSPICIOUS ACTIVITY

When suspicious activity involving senior current or former officials or highly unusual activity is identified, the Board's Special Investigations and Examinations Section should be notified at 202-452-3168.

FAST TRACK CRIMINAL REFERRAL ENFORCEMENT PROGRAM

Effective April 14, 1995, as detailed in the Board's supervisory directive SR 95-23, the Federal Reserve implemented a Fast Track Criminal Referral[1] Enforcement Program (the ''Fast Track Program'') that uses expedited, streamlined enforcement procedures to obtain consent orders of prohibition from banking officials and employees whose cases have been declined by law enforcement agencies and have already admitted to criminal acts involving amounts up to $100,000. When needed, it will also be used to seek restitution from the individuals through consent cease and desist orders. The Fast Track Program also involves the expeditious issuance of appropriate notices in those instances where individuals do not consent to the orders presented to them. Detailed below are the procedures that Federal Reserve staff should follow in utilizing the Fast Track Program.

Procedures

1. Each Federal Reserve Bank should review all SARs on an on-going basis and, in connection therewith, should implement the Fast Track Program to identify those SARs where law enforcement agencies have declined to prosecute institution-affiliated parties who have admitted guilt involving criminal activities with associated losses of less than $100,000.
2. For those SARs involving losses of under $100,000, in which an institution-affiliated party has admitted guilt through a signed confession, an oral admission to a banking organization official that is recorded, or otherwise, designated Federal Reserve Bank personnel should contact federal law enforcement agencies and, where necessary, state or local law enforcement agencies, or reconfirm prior contacts, to determine the status of any criminal investigation or prosecution involving the individual. The Federal Reserve Bank should ascertain whether the individual has already been prosecuted and sentenced through a U.S. Attorney's or state equivalent

1. Effective April 1, 1996, the Criminal Referral Form was replaced with the Suspicious Activity Report form.

"Fast Track" system or otherwise,[2] whether the matter is under active investigation, or whether the matter has been declined for prosecution.

3. If law enforcement has declined to prosecute the individual subject to the SAR, the Federal Reserve Bank should:
   a. Gather from the law enforcement agency, or the banking organization filing the SAR, or both, all appropriate documents related to the SAR, including a copy of the signed confession, records relating to any admission made to banking officials, and any other pertinent supporting materials, such as affidavits and investigatory reports;
   b. contact the appropriate banking organization representative to ascertain whether any civil action has been taken by the organization against the individual, and whether the financial institution has obtained any restitution, either through the voluntary cooperation of the individual or by means of a court judgment;
   c. determine the current home address of the individual, if possible; and
   d. determine whether the individual is currently employed by a banking organization, if possible.
4. When requested information is received and the Federal Reserve Bank determines with certainty that the appropriate federal, state, or local law enforcement agency will not prosecute the institution-affiliated party, designated Federal Reserve Bank personnel should make a determination regarding whether a prohibition order, or cease and desist order seeking restitution, or a combination of both should be pursued under the Fast Track Program.
5. In the event a Federal Reserve Bank recommends an institution-affiliated party for inclusion in the Fast Track Program, it should forward to the Board's Division of Banking Supervision and Regulation's Deputy Associate Director responsible for enforcement matters the following:
   a. The completed portion of the Fast Track Program checklist[3] identified as "Federal Reserve Bank Responsibilities," along with a copy of the SAR; and
   b. documentation supporting the recommendation, such as the signed confession, or a bank's record of an individual's admission.
6. Upon the submission of a Federal Reserve Bank's recommendation and completed checklist, designated staff of the Division of Banking Supervision and Regulation, in coordination with the Board's Legal Division, will:
   a. Obtain the necessary approvals of senior Board staff required for the initiation of an enforcement action using the Fast Track Program checklist in the place of a standard "final approval" memorandum;
   b. notify the other federal financial institutions supervisory agencies regarding the proposed enforcement action under current interagency notification procedures;
   c. in consultation with Federal Reserve Bank staff, finalize a proposed order, using preapproved formats, and send it to the individual for his or her consideration of entering into the order on a consent basis by means of a cover letter signed by the Deputy Associate Director, which designates an Enforcement Section attorney as the contact person for discussions regarding the consent order;
   d. upon receipt of a signed consent order, obtain the necessary senior Board staff approvals, have the order executed by the Board's Secretary, prepare and send all necessary interagency notification letters, and, in consultation with the Board's public information office, prepare an appropriate press release; and
   e. in the event the individual does not agree to the consensual issuance of an order of prohibition, or cease and desist order, or a combined order, where necessary, coordinate with designated Federal Reserve Bank staff in order to prepare the appropriate notice under existing Federal Reserve enforcement procedures.

2. In those cases where an individual has already been prosecuted and sentenced, Federal Reserve Banks should follow current procedures and ensure that the individual receives a letter from the Federal Reserve Bank explaining the restrictions and limitations contained in section 19 of the Federal Deposit Insurance Act, as amended (12 U.S.C. 1829).

3. Not included in this Manual. Refer to SR Letter 95-23 for a copy of the checklist.

These are internal procedures for the Federal Reserve's Fast Track Program. They do not create or confer any substantive or procedural rights on third parties, which would be enforceable, in any manner, in a proceeding of any nature.

QUESTIONS

For questions regarding the use of the SAR database you may telephone the Board's Special Investigations and Examinations Section at 202-452-3168.

The Federal Reserve supervises the following entities and has the statutory authority to take formal enforcement actions against them:

- State member banks
- Bank holding companies
- Nonbank subsidiaries of bank holding companies
- Edge and agreement corporations
- Branches and agencies of foreign banking organizations operating in the U.S. and their parent banks
- Officers, directors, employees, and certain other categories of individuals associatied with the above banks, companies and organizations (referred to as ''institution affiliated parties'')

Generally, the Federal Reserve takes formal enforcement actions against the above entities for violations of laws, rules, or regulations, unsafe or unsound practices, breaches of fiduciary duty, and violations of final orders. Formal actions include cease and desisit orders, written agreements, removal and prohibition orders, and orders assessing civil money penalties. Such actions can include those for entities who fail to develop and implement compliance programs designed to detect, deter and report suspicious activities possibly associated with money laundering or to meet other technical reporting and recordkeeping requirements under the Bank Secrecy Act.

For information regarding enforcement actions taken by the Federal Reserve, the reader may refer to the Federal Reserve's home page at the following address:

http://www.bog.frb.fed.us/boarddocs/enforcement

From time to time as deemed necessary, the Financial Crimes Enforcement Network ("FinCEN") will provide advisories to the banks, regulators and the general public concerning money laundering matters, trends and patterns, or amendments/clarifications to the Bank Secrecy Act. Access to the Fincen home page to obtain the advisories and other information can be found at the following address:

http://www.ustreas.gov/treasury/bureaus/fincen/advis.html

Other communications can be directed to FinCEN:

Phone (703) 905-3773
Facsimile (703) 905-3885
Address: 2070 Chain Bridge Road, Vienna, Virginia 22182

Federal Reserve Examination Staff is advised that any questions regarding a FinCEN matter should be directed first to the Board's Special Investigations and Examinations Section at (202) 452-3168.

Check List to Identify Potential Abuses

The following is a list of transactions that could be considered unusual or suspicious and possibly linked to money laundering or other financial crime activities. The list is not intended to be all inclusive.

MONEY LAUNDERING

- Increase in cash shipments that is not accompanied by a corresponding increase in the number of accounts.
- Cash on hand frequently exceeds limits established in security program and/or blanket bond coverage.
- Large volume of wire transfers to and from offshore banks.
- Large volume of cashier's checks, money orders or travelers checks sold for cash.
- Accounts have a large number of small deposits and a small number of large checks with the balance of the account remaining relatively low and constant. Account has many of the same characteristics as an account used for check kiting.
- A large volume of deposits to several different accounts with frequent transfers of major portion of the balance to a single account at the same bank or at another bank.
- Loans to offshore companies.
- A large volume of cashier's checks or money orders deposited to an account where the nature of the account holder's business would not appear to justify such activity.
- Large volume of cash deposits from a business that is not normally cash intensive.
- Cash deposits to a correspondent bank account by any means other than through an armored carrier.
- Large turnover in large bills or excess of small bills from bank and demand for large bills by bank which would appear uncharacteristic for the bank.
- Cash shipments which appear large in comparison to the dollar volume of currency transaction reports filed.
- Dollar limits on the list of the bank customers exempt from currency transaction reporting requirements which appear unreasonably high considering the type and location of the business. No information is in the bank's files to support the limits set.
- Currency transaction reports, when filed, are often incorrect or lack important information.
- List of exempted customers appears unusually long.
- High volume of sequentially numbered traveler's checks or postal money orders addressed to same payee.

OFFSHORE TRANSACTIONS

- Loans made on the strength of a borrower's financial statement reflects major investments in and income from businesses incorporated in bank secrecy haven countries.
- Loans to offshore companies.
- Loans secured by obligations of offshore banks.
- Transactions involving an offshore ''shell'' bank whose name may be very similar to the name of a major legitimate institution.
- Frequent wire transfers of funds to and from bank secrecy haven countries.
- Offers of multimillion dollar deposits at below market rates from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank through a letter, telex, or other ''official'' communication.
- Presence of telex or facsimile equipment in a bank where the usual and customary business activity would not appear to justify the need for such equipment.

WIRE TRANSFERS

- Indications of frequent overrides of established approval authority and other internal controls.
- Intentional circumvention of approval authority by splitting transactions.
- Wire transfers to and from bank secrecy haven countries.
- Frequent or large wire transfers for persons who have no account relationship with bank.
- In a linked financing situation, a borrower's request for immediate wire transfer of loan proceeds to one or more of the banks where the funds for the brokered deposits originated.
- Large or frequent wire transfers against uncollected funds.

- Wire transfers involving cash where the amount exceeds $10,000.
- Inadequate control of password access.
- Customer complaints and/or frequent error conditions.

LINKED FINANCING/BROKERED TRANSACTIONS

- Out-of-territory lending.
- Loan production used as a basis for officer bonuses.
- Evidence of unsolicited attempts to buy or recapitalize the bank where there is evidence of a request for large loans at or about the same time by persons previously unknown to the bank. Promise of large dollar deposits may also be involved.
- Promise of large dollar deposits in consideration for favorable treatment on loan requests. (Deposits are not pledged as collateral for the loans.)
- Brokered deposit transactions where the broker's fees are paid for from the proceeds of related loans.
- Anytime a bank seriously considers a loan request where the bank would have to obtain brokered deposits to be able to fund the loan should be viewed with suspicion.
- Solicitation by persons who purportedly have access to multi-millions of dollars, from a confidential source, readily available for loans and/or deposits in U.S. financial institutions. Rates and terms quoted are usually more favorable than funds available through normal sources. A substantial fee may be requested in advance or the solicitor may suggest that the fee be paid at closing but demand compensation for expenses, often exceeding $50,000.
- Prepayment of interest on deposit accounts where such deposit accounts are used as collateral for loans.

THIRD PARTY OBLIGATIONS

- Incomplete documentation on guaranties.
- Loans secured by obligations of offshore banks.
- Lack of credit information on third party obligor.
- Financial statements reflect concentrations of closely held companies or businesses that lack audited financial statements to support their value.

CREDIT CARDS AND ELECTRONIC FUNDS TRANSFERS

- Lack of separation of duties between the card issuing function and issuance of personal identification number (PIN).
- Poor control of unissued cards and PINs.
- Poor control of returned mail.
- Customer complaints.
- Poor control of credit limit increases.
- Poor control of name and address changes.
- Frequent malfunction of payment authorization system.
- Unusual delays in receipt of card and PINs by the customers.
- Bank does not limit amount of cash that a customer can extract from an ATM in a given day.
- Evidence that customer credit card purchases have been intentionally structured by a merchant to keep individual amount below the ''floor limit'' to avoid the need for transaction approval.

MISCELLANEOUS

- Indications of frequent overrides of internal controls or intentional circumvention of bank policy.
- Unresolved exceptions or frequently recurring exceptions on exceptions report.
- Out-of-balance conditions.
- Purpose of loan is not recorded.
- Proceeds of loan are used for a purpose other than the purpose recorded.
- A review of checks paid against uncollected funds indicates that the customer is offsetting checks with deposits of the same or similar amount and maintains a relatively constant account balance, usually small in relation to the amount of activity and size of the transactions.

FEDERAL RESERVE press release

For immediate release **February 5, 1996**

The Federal Reserve Board today announced a final rule to simplify the process for reporting suspected crimes and suspicious activities by banking organizations supervised by the Federal Reserve.

The final rule is effective April 1, 1996.

The rule was developed by the Federal Reserve, the other federal banking agencies, and the Financial Crimes Enforcement Network of the U.S. Department of the Treasury (FinCEN).

The rule significantly reduces reporting burdens, while at the same time enhancing the ability of law enforcement authorities to investigate and prosecute criminal offenses involving our Nation's financial institutions.

The new suspicious activity reporting rule:

- **combines the current criminal referral rules of the Federal Reserve and the other federal banking agencies with FinCEN's suspicious activity reporting requirements relating to money laundering offenses;**
- **creates a uniform reporting form and instructions--the new "Suspicious Activity Report" or "SAR"--for use by banking organizations to report all violations;**
- **requires the filing of only one form with FinCEN;**
- **enables a filer, through computer software that will be provided by the Federal Reserve to all of the domestic and foreign banking organizations it supervises, to prepare a SAR on a computer and file it by magnetic media, such as a computer disc or tape;**

(more)

- raises the thresholds for mandatory reporting in two categories and creates a threshold for the reporting of suspicious transactions related to money laundering and violations of the Bank Secrecy Act in order to reduce the reporting burdens of banking organizations; and
- emphasizes recent changes in the law that provide a safe harbor from civil liability to banking organizations and their employees for reporting of known or suspected criminal offenses or suspicious activities.

Substantially identical suspicious activity reporting rules are being issued by FinCEN, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration.

The Board's notice is attached.

-0-

Attachment

FEDERAL RESERVE SYSTEM

12 CFR Parts 208, 211 and 225

[Regulations H, K and Y; Docket No. R-0885]

Membership of State Banking Institutions in the Federal Reserve System; International Banking Operations; Bank Holding Companies and Change in Control; Reports of Suspicious Activity under the Bank Secrecy Act

AGENCY: Board of Governors of the Federal Reserve System.

ACTION: Final Rule.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) is amending its regulations on the reporting of known or suspected criminal and suspicious activities by the domestic and foreign banking organizations supervised by the Board. This final rule streamlines reporting requirements by providing that such an organization file a new Suspicious Activity Report (SAR) with the Board and the appropriate federal law enforcement agencies by sending a SAR to the Financial Crimes Enforcement Network of the Department of the Treasury (FinCEN) to report a known or suspected criminal offense or a transaction that it suspects involves money laundering or violates the Bank Secrecy Act (BSA).

EFFECTIVE DATE: April 1, 1996.

FOR FURTHER INFORMATION CONTACT: Herbert A. Biern, Deputy Associate Director, Division of Banking Supervision and Regulation, (202) 452-2620, Richard A. Small, Special Counsel, Division of Banking Supervision and Regulation, (202) 452-5235, or Mary Frances Monroe, Senior Attorney, Division of Banking

Supervision and Regulation, (202) 452-5231. For the users of Telecommunications Devices for the Deaf (TDD) only, contact Dorothea Thompson, (202) 452-3544, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, N.W., Washington, D.C. 20551.

SUPPLEMENTARY INFORMATION:

Background

The Board, the office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) (collectively, the Agencies) have issued for public comment substantially similar proposals to revise their regulations on the reporting of known or suspected criminal conduct and suspicious activities. The Department of the Treasury, through FinCEN, has issued for public comment a substantially similar proposal to require the reporting of suspicious transactions relating to money laundering activities.

The Board's proposed regulation (60 FR 34481, July 3, 1995) noted that the interagency Bank Fraud Working Group, consisting of representatives from the Agencies, the National Credit Union Administration, law enforcement agencies, and FinCEN, has been working on the development of a single form, the SAR, for the reporting of known or suspected federal criminal law violations and suspicious activities. The Board's proposed regulation, as well as those proposed by the OCC, FDIC, OTS and FinCEN, attempted to simplify and clarify reporting requirements

and reduce banking organizations, reporting burdens by raising mandatory reporting thresholds for criminal offenses and by requiring the filing of only one report with FinCEN.

The Board's final rule adopts its proposal with a few additional changes that have been made in response to the comments received. The changes will result in burden reductions even greater than those that were proposed. The Board's, the other Agencies', and FinCEN's final rules relating to the reporting of suspicious activities are now substantially identical, and they:

(1) Combine the current criminal referral rules of the federal financial institutions regulatory agencies with the Department of the Treasury's suspicious activity reporting requirements;

(2) create a uniform reporting form, the new Suspicious Activity Report or SAR, for use by banking organizations in reporting known or suspected criminal offenses, or suspicious activities related to money laundering and violations of the BSA;

(3) provide a system whereby a banking organization need only refer to the SAR and its instructions in order to complete and file the form in conformance with the Agencies' and FinCEN's reporting regulations;

(4) require the filing of only one form with FinCEN;

(5) eliminate the need to file supporting documentation with a SAR;

(6) enable a filer, through computer software that will be provided by the Board to all of the domestic and foreign banking organizations it supervises, to prepare a SAR on a computer and file it by magnetic media, such as a computer disc or tape;

(7) establish a database that will be accessible to federal and state financial institutions regulators and law enforcement agencies;

(8) raise the thresholds for mandatory reporting in two categories and create a threshold for the reporting of suspicious transactions related to money laundering and violations of the BSA in order to reduce the reporting burdens on banking organizations; and

(9) emphasize recent changes in the law that provide a safe harbor from civil liability to banking organizations and their employees for reporting of known or suspected criminal offenses or suspicious activities, by filing a SAR or by reporting by other means, and provide criminal sanctions for the unauthorized disclosure of such report to any party involved in the reported transaction.

Section-by-Section Analysis

Under the Board's final rule, state member banks, bank holding companies and their nonbank subsidiaries, most U.S. branches and agencies and other offices of foreign banks, and Edge and Agreement corporations need only follow SAR instructions

for completing and filing the SAR to be in compliance with the Board's and FinCEN's reporting requirements. The following section-by-section analysis correlates the specific SAR instruction number with the applicable section of the Board's final rule:

Section 208.20(a) (Instruction No. 1 on the SAR) provides that a state member bank must file a SAR when it detects a known or suspected violation of federal law or a suspicious activity pertinent to a money laundering offense.

Section 208.20(b) provides pertinent definitions.

Sections 208.20(c)(1), (2), and (3) (Instructions 1 a., b., and c. on the SAR) instruct a state member bank to file a SAR with FinCEN in order to comply with the requirement to notify federal law enforcement agencies if the bank detects any known or suspected federal criminal violation, or pattern of violations, committed or attempted against the bank, or involving one or more transactions conducted through the bank, and the bank believes it was an actual or potential victim of a crime, or was used to facilitate a crime. If the bank has a substantial basis for identifying one of its insiders or other institution-affiliated parties in connection with the known or suspected crime, reporting is required regardless of the dollar amount involved. If the bank can identify a non-insider suspect, the applicable transaction threshold is $5,000. In cases in which no suspect can be identified, the applicable transaction threshold is

$25,000. These sections were not changed from the proposed regulations published for public comment in July 1995.

Section 208.20(c)(4) (Instruction 1 d. on the SAR) instructs a state member bank to file a SAR with FinCEN in order to comply with the requirement to notify federal law enforcement agencies and the Department of the Treasury of transactions involving $5,000 or more in funds or other assets when the bank knows, suspects or has reason to suspect that the transaction: (i) involves money laundering, (ii) is designed to evade any regulations promulgated under the Bank Secrecy Act, or (iii) has no business or apparent lawful purpose or is not the sort in which the particular customer normally engages and, after examining the available facts, the bank knows of no reasonable explanation for the transaction. Section 208.20(c)(4) has been modified in the final rule to reflect comments received on the proposal. Most notably, the circumstances under which a transaction should be reported under this section were clarified, and a reporting threshold of $5,000 was added.

Section 208.20(c)(4) recognizes the emerging international consensus that the efforts to deter, substantially reduce, and eventually eradicate money laundering are greatly assisted by the reporting of suspicious transactions by banking organizations. The requirements of this section comply with the recommendations adopted by multi-country organizations in which the United States is an active participant, including the Financial Action Task Force of G-7 nations and the Organization

of American States, and are consistent with the European Community's directive on preventing money laundering through financial institutions.

Section 208.20(d) (Instruction 2 on the SAR) provides that SARs must be filed within 30 calendar days of the initial detection of the criminal or suspicious activity. An additional 30 days is permitted in order to enable a bank to identify a suspect, but in no event may a SAR be filed later than 60 days after the initial detection of the reportable conduct. The Board and law enforcement must be notified in the case of a violation requiring immediate action, such as an on-going violation. These reporting requirements were not changed from the July 1995 proposal, with the exception of the addition of the requirement that the Board be notified about on-going offenses requiring immediate notification to law enforcement authorities.

Section 208.20(e) encourages a state member bank to file a SAR with state and local law enforcement agencies. This section is unchanged from the July 1995 proposal.

Section 208.20(f) (Instruction 3 on the SAR) provides that a state member bank need not file a SAR for an attempted or committed burglary or robbery reported to the appropriate law enforcement agencies. In addition, a SAR need not be filed for missing or counterfeit securities that are the subject of a report pursuant to Rule 17f-1 under the Securities Exchange Act of 1934. This section of the final rule was not modified from the version published for public comment in July 1995.

8

Section 208.20(g) requires that a state member bank retain a copy of the SAR and the original or business record equivalent of supporting documentation for a period of five years. The section also requires that a state member bank identify and maintain supporting documentation in its files and that the bank make available such documentation to law enforcement agencies upon their request. The Board made three changes to this section from the version published for public comment in July 1995. First, the record retention period was shortened from 10 years to five years. Second, provision was made for the retention of business record equivalents of original documents, such as microfiche and computer imaged record systems, in recognition of modern record retention technology. The third change involves the clarification of a state member bank's obligation to provide supporting documentation upon request to law enforcement officials. Supporting documentation is deemed filed with a SAR in accordance with this section of the Board's final rule; as such, law enforcement authorities need not make their access requests through subpoena or other legal processes.

Section 208.20(h) requires the management of a state member bank to report the filing of all SARs to the board of directors of the bank, or a designated committee thereof. No change was made from the July 1995 proposal.

Section 208.20(i) reminds a state member bank and its institution-affiliated parties that failure to file a SAR may

expose them to supervisory action. No change from the July 1995 proposal was made.

Section 208.20(j) provides that SARs are confidential. Requests for SARs or the information contained therein should be declined. The final rule also adds a requirement that a request for a SAR or the information contained therein should be reported to the Board. With the exception of the added requirement that requests for SARs be reported to the Board, no changes were made to this section from the July 1995 proposal.

Section 208.20(k) sets forth the safe harbor provisions of 31 U.S.C. 5318(g). This new section, which was added to the final rule as the result of many comments concerning this important statutory protection for banking organizations, states that the safe harbor provisions of the law are triggered by a report of known or suspected criminal violations or suspicious activities to law enforcement authorities, regardless whether the report is made by the filing of a SAR in accordance with the Board's rules or for other reasons by different means.

Sections 211.8, 211.24(f), and 225.4(f) of the Board's rules relating to the activities of foreign banking organizations and bank holding companies have not been changed in a substantive manner. Only the references in the sections to ''criminal referral forms'' have been changed to reflect the new name for the reporting form, the SAR. The SAR filing requirements, as well as the safe harbor and notification prohibition provisions of

31 U.S.C. 5318(g), continue to be applicable to all foreign banking organizations and bank holding companies and their nonbank subsidiaries supervised by the Federal Reserve through these provisions.

Comments Received

The Board received letters from 44 public commenters. Comments were received from 15 community banks, 13 multinational or large regional banks, eight trade and industry research groups, seven Federal Reserve Banks and one law firm.

The large majority of commenters expressed general support for the Board's proposal. None of the commenters opposed the proposed new suspicious activity reporting rules. A number of suggestions and requests for clarification were received. They are as follows.

Criminal Versus Suspicious Activities. Many commenters expressed confusion over the difference between the known or suspected criminal conduct that would be subject to the dollar reporting thresholds (provided such conduct does not involve an institution-affiliated party of the reporting entity) and the suspicious activities that would be reported regardless of dollar amount. Section 208.20(c)(4) has been revised to add a $5,000 reporting threshold and to clarify that the suspicious activity must relate to money laundering and Bank Secrecy Act violations. A threshold for the reporting of suspicious activities was added to reduce further the reporting burdens on banking organizations.

11

Reporting of Crimes Under State Law. A number of commenters requested clarification of whether activities constituting crimes under state law, but not under federal law, should be reported on the SAR. The Board continues to encourage banking organizations to refer criminal and suspicious activities under both federal and state law by filing a SAR. Under the new reporting system designed by the Board, the other Agencies, and FinCEN, state chartered banking organizations should be able to fulfill their state reporting obligations by filing a SAR with FinCEN.

Safe Harbor Protections; Potential Liability Under Federal and State Laws. Some commenters expressed the concern that banking organizations and their institution-affiliated parties could be liable under federal and state laws, such as the Right to Financial Privacy Act, for filing SARs with respect to conduct that is later found not to have been criminal. Another concern was that the filing of SARs with state and local law enforcement agencies would subject filers to claims under state law. Both of these concerns are addressed by the scope of the safe harbor protections provided in 31 U.S.C. 5318(g).

The Board is of the opinion that the safe harbor statute is broadly defined to include the reporting of known or suspected criminal offenses or suspicious activities, by filing a SAR or by reporting by other means, with state and local law enforcement authorities, as well as with the Agencies and FinCEN.

A few commenters requested that the Board make explicit the safe harbor protections of 31 U.S.C. 5318(g)(2) and (3) on the SAR. They are included in new Section 208.20(k) of this rule and on the form.

Record Retention. Several commenters expressed the view that the 10-year period for the retention of records in Section 208.20(g) was excessive, especially in light of a five-year record retention requirement for records that is contained in the Bank Secrecy Act. The 10-year period in the Board's proposed regulation would have continued the Board's existing record retention requirement for criminal referral forms. However, in recognition of the potential burden of document retention on financial institutions, the Board has limited the record retention period to five years.

Dollar Thresholds. A few commenters encouraged the Board to raise the dollar thresholds for known or suspected criminal conduct by non-insiders, or to establish a dollar threshold for insiders. The Board has considered these comments, but at this time it believes that the thresholds meet and properly balance the dual concerns of prosecuting criminal activity involving banking organizations and minimizing the burden on banking organizations. With respect to the suggestion that the Board adopt a dollar threshold for insider violations, it is noted that insider abuse has long been a key concern and focus of enforcement efforts at the Board. With the development of a new sophisticated automated database, the Board and law

enforcement agencies will have the benefit of a comprehensive and easily accessible catalogue of known or suspected insider wrongdoing. The Board does not wish to limit the information it receives regarding insider wrongdoing. Some petty crimes, for example, repetitive thefts of small amounts of cash by an employee who frequently moves between banking organizations, may warrant enforcement action or criminal prosecution.

One commenter suggested an indexed threshold, based on the regional differences in the various dollar thresholds below which the federal, state, and local prosecutors generally decline prosecution. While the Board recognizes that there may be regional variations in the dollar amount of financial crimes generally prosecuted, the Board's concern is to place the relevant information in the hands of the investigating and prosecuting authorities. The prosecuting authorities then may consider whether to pursue a particular matter. In the Board's view, the dollar thresholds proposed and adopted in this final rule best balance the interests of law enforcement and banking organizations. The Board also believes that indexed thresholds could create more confusion than benefit to banking organizations.

Commenters also suggested the creation of a dollar threshold for the reporting of suspicious activities relating to money laundering offenses. A $5,000 threshold has been established for reporting of such suspicious activities.

14

Questions were raised regarding the permissibility of filing SARs in situations in which the dollar thresholds for known or suspected criminal conduct or suspicious activity are not met and the applicability of the safe harbor provisions of 31 U.S.C. 5318(g) to such non-mandatory filings. It is the opinion of the Board that the safe harbor provisions of 31 U.S.C. 5318(g) cover all reports of suspected or known criminal violations and suspicious activities to law enforcement authorities, regardless of whether such reports are filed pursuant to the mandatory requirements of the Board's regulations or are voluntary.

Notification of On-Going Violations and of State and Local Law Enforcement Authorities. Proposed Section 208.20(d) required a banking organization to notify immediately the law enforcement authorities in the event of an on-going violation. Section 208.20(e) encourages the filing of a copy of the SAR with state and local law enforcement agencies in appropriate cases. This requirement and guidance were found by some commenters to be unclear as to when immediate notification or the filing of the SAR with state and local authorities would be required. The Board wishes to clarify that immediate notification is limited to situations involving on-going violations, for example, when a check kite or money laundering has been detected and may be continuing. It is impossible for the Board to contemplate all of the possible circumstances in which it might be appropriate for a banking organization to advise state and local law enforcement authorities. Banking organizations should use their best

judgment regarding when to alert them regarding on-going criminal offenses or suspicious activities.

Supporting Documentation. The proposed requirements that an institution maintain ″related″ documentation and make ″supporting″ documentation available to the law enforcement agencies upon request were criticized as inconsistent and vague. One commenter questioned whether the Board intended a substantive difference in meaning between ″related″ and ″supporting.″ As a substantive difference is not intended, the Board has referred to ″supporting″ documentation in the final rule in reference both to the maintenance and production requirements. The Board believes that the use of the word ″supporting″ is more precise and limits the scope of the information which must be retained to that which would be useful in proving that the crime has been committed and by whom it has been committed. As to the criticism that the meaning of ″related″ or ″supporting″ documentation is vague, it is anticipated that banking organizations will use their judgment in determining the information to be retained. It is impossible for the Board to catalogue the precise types of information covered by this requirement, as it necessarily depends upon the facts of a particular case.

Scope of Confidentiality Requirement. One commenter correctly noted that the proposed regulation is unclear as to whether the confidentiality requirement applies only to the information contained on the SAR itself, or whether the requirement extends to the ″supporting″ documentation. The Board

takes the position that only the SAR and the fact that supporting documentation to a SAR exists are subject to the confidentiality requirements of 31 U.S.C. 5318(g). The supporting documentation itself is not subject to the confidentiality provisions of 31 U.S.C. 5318(g). The safe harbor provisions of 31 U.S.C. 5318(g), however, apply to the SAR and supporting documentation, as set forth in Section 208.20(k).

Provisions of Supporting Documentation to Law Enforcement Authorities Upon Request. Many commenters noted that the guidance provided in the Board's proposed regulation regarding giving supporting documentation to law enforcement agencies upon their request after the filing of a SAR was unclear or contrary to law. Some questioned whether law enforcement agencies would still need to subpoena relevant documents from a banking organization. The Board's regulation requires banking organizations filing SARs to identify, maintain and treat the documentation supporting the report as if it were actually filed with the SAR. This means that subsequent requests from law enforcement authorities for the supporting documentation relating to a particular SAR does not require the service of a subpoena or other legal processes normally associated with providing information to law enforcement agencies.

Civil Litigation. The Board was encouraged to adopt regulations that would make SARs undiscoverable in civil litigation in order to avoid situations in which a banking organization could be ordered by a court to produce a SAR in

civil litigation and could be confronted with the prospect of having to choose between being found in contempt or violating the Board's rules. In the opinion of the Board, 31 U.S.C. 5318(g) precludes the disclosure of SARs. The final rule requires a banking organization that receives a subpoena or other request for a SAR to notify the Board so that the Board may, if appropriate, intervene in litigation or seek the assistance of the U.S. Department of Justice.

Maintenance of Originals. Proposed Section 208.20(g) required the maintenance of supporting documentation in its original form. A number of commenters noted that electronic storage of documents is becoming the rule rather than the exception, and that requiring the storage of paper originals would impose undue burdens on financial institutions. Moreover, some records are retained only in a computer database. The proposed regulation reflected the concerns of the law enforcement agencies that the best evidence be preserved. However, upon further consideration, the Board wishes to clarify that the electronic storage of original documentation related to the filing of a SAR is permissible. In addition, the Board recognizes that a banking organization will not always have custody of the originals of documents and that some documents will not exist at the organization in paper form. In those cases, preservation of the best available evidentiary documents, for example, computer disks or photocopies, should be acceptable. This has been reflected in the final rule by changing the

reference to original documents to "original documents or business record equivalents."

Investigation and Proof Burdens. One commenter expressed the concern that a banking organization would need to establish probable cause before reporting crimes for which an essential element of the proof of the crime was the intent of the actor. The Board does not intend that banking organizations assume the burden of proving illegal conduct; rather, banking organizations are required to report known or suspected crimes or suspicious activities in accordance with this final rule.

Supplementary or Corrective Information; Reporting of Multiple Crimes or Suspects. Material information that supplements or corrects a SAR should be filed with FinCEN by means of a subsequent SAR. The first page of the SAR provides boxes for the reporter to indicate whether the report is an initial, a corrected or a supplemental report.

One commenter requested guidance on the reporting of multiple crimes or related crimes committed by more than one individual. The instructions to the SAR contemplate that additional suspects may be reported by means of a supplemental page. Likewise, multiple crimes committed by a suspect may be reported by means of multiple check-offs on the SAR, or if needed, by a written addendum to the SAR. In the event that related crimes have been committed by more than one person, a description of the related crimes may be made by addendum to the SAR. The Board encourages filers to make a complete report of

19

all known or suspected criminal or suspicious activity. The SAR may be supplemented in order to facilitate a complete disclosure.

Calculation of Time Frame for Reporting. A number of commenters requested that the Board clarify the application of the deadline for filing SARs. The Board's proposed regulation used the broadest possible language to set the time frames for the reporting of known or suspected criminal offenses and suspicious activities in order to best guide reporting institutions. Absolute deadlines for the filing of SARs are important to the investigatory and prosecutorial efforts of law enforcement authorities. It is expected that banking organizations will meet the filing deadlines once conduct triggering the reporting requirements is identified. Further clarification of the time frames is not needed in the Board's view.

Board Notification Requirements. Several commenters expressed general support for the modification of the reporting requirement that permits reporting of SARs to a committee of the board. As a matter of clarification, notification of a committee of the board relieves the banking organization of the obligation to disclose the SARs filed to the entire board. It would be expected, however, that the appointed committee, such as the audit committee, would report to the full board at regular intervals with respect to routine matters in the same manner and to the same extent as other committees report at board meetings. With respect to serious crimes or insider malfeasance, the

appointed committee likely should consider it appropriate to make more immediate disclosure to the full board.

Some larger banking organizations expressed the view that prompt disclosure of SARs to the board or a committee would impose a serious burden because larger organizations typically file a larger number of criminal referral forms (now, SARs). While the Board acknowledges that larger institutions may have more SARs to report to the board or a committee, this does not alter the directors' fiduciary obligation to monitor, for example, the condition of the institution and to take action to prevent losses. The final regulation does not dictate the content of the board or committee notification, and, in some cases, such as when relatively minor non-insider crimes are to be reported, it may be completely appropriate to provide only a summary listing of SARs filed. The Board expects the management of banking organizations to provide a more detailed notification to the boards or committees of SARs involving insiders or a potential material loss to the institutions.

Information Sharing. Commenters suggested that the final regulations should somehow facilitate the sharing of information among banking organizations in order to better detect new fraudulent schemes. It is anticipated that the Treasury Department, through FinCEN, and the Agencies, will keep reporting entities apprised of recent developments and trends in banking-related crimes through periodic pronouncements, meetings, and seminars.

21

Single Filing Requirement; Acknowledgement of Filings. Some commenters requested clarification of the single form filing requirement. The Board reiterates that the filing of a SAR with FinCEN is the only filing that is required. Federal and state law enforcement and bank supervisory agencies will have access to the database created and maintained by FinCEN on behalf of the Agencies and the Department of Treasury; thus, a single filing with FinCEN is all that is required under the new reporting system.

Commenters also requested that the final rule permit the filing of SARs via telecopier. Such filings are not compatible with the system developed by the Agencies and FinCEN. Banking organizations can file the SAR via magnetic media using the computer software to be provided to all banking organizations by the Board and each of the other Agencies with respect the institutions they supervise. Larger banking organizations that currently file currency transaction reports via magnetic tape with FinCEN may also file SARs by magnetic tape.

Regulatory Flexibility Act

The Board certifies that this final regulation will not have a significant financial impact on a substantial number of small banks or other small entities.

Paperwork Reduction Act

In accordance with Section 3506 of the Paperwork Reduction Act of 1995 (44 U.S.C. Ch. 35; 5 CFR 1320 Appendix

A.1), the Board reviewed the rule under the authority delegated to the Board by the Office of Management and Budget.

The collection of information requirements in this regulation are found in 12 CFR 208.20, 211.8, 211.24, and 225.4. This information is mandatory and is necessary to inform appropriate law enforcement agencies of known or suspected criminal or suspicious activities that take place at or were perpetrated against financial institutions. Information collected on this form is confidential (5 U.S.C. 552(b)(7) and 552a(k)(2), and 31 U.S.C. 5318(g)). The federal financial institution regulatory agencies and the U.S. Department of Justice may use and share the information. The respondents/recordkeepers are for-profit financial institutions, including small businesses.

The Federal Reserve may not conduct or sponsor, and an organization is not required to respond to, this information collection unless it displays a currently valid OMB control number. The OMB control number is 7100-0212.

No comments specifically addressing the hour burden estimate were received.

It is estimated that there will be 12,000 responses from state member banks, bank holding companies, Edge and agreement corporations, and U.S. branches and agencies of foreign banks.

Both the new regulation and revisions made to the proposed regulation and reflected in this final rule simplify the

submission of the reporting form and shorten the records retention requirement. However, the same amount of information will be collected under the new rule. The burden per respondent varies depending on the nature of the criminal or suspicious activity being reported. The Federal Reserve estimates that the average annual burden for reporting and recordkeeping per response will remain .6 hours. Thus the Federal Reserve estimates the total annual hour burden to be 7,200 hours. Based on an hourly cost of $20, the annual cost to the public is estimated to be $144,000.

Send comments regarding the burden estimate, or any other aspect of this collection of information, including suggestions for reducing the burden, to: Secretary, Board of Governors of the Federal Reserve System, 20th and C Streets, N.W., Washington, D.C. 20551 and to the Office of Management and Budget, Paperwork Reduction Project (7100-0212), Washington, D.C. 20503.

List of Subjects

12 CFR Part 208

Accounting, Agriculture, Banks, Banking, Confidential Business information, Crime, Currency, Federal Reserve System, Flood insurance, Mortgages, Reporting and recordkeeping requirements, Securities.

12 CFR Part 211

24

Exports, Federal Reserve System, Foreign Banking, Holding companies, Investments, Reporting and recordkeeping requirements.

25

12 CFR Part 225

Administrative practice and procedures, Banks, Banking, Federal Reserve System, Holding companies, Reporting and recordkeeping requirements, Securities.

For the reasons set forth in the preamble, Parts 208, 211 and 225 of chapter II of title 12 of the Code of Federal Regulations are amended as set forth below:

PART 208 -- MEMBERSHIP OF STATE BANKING INSTITUTIONS IN THE FEDERAL RESERVE SYSTEM (REGULATION H)

1. The Authority citation for 12 CFR Part 208 continues to read as follows:

Authority: 12 U.S.C. 36, 248(a), 248(c), 321-338a, 371d, 461, 481-486, 601, 611, 1814, 1823(j), 1828(o), 1831o, 1831p-1, 3105, 3310, 3331-3351, and 3906-3909; 15 U.S.C. 78b, 781(b), 781(g), 781(i), 78o-4(c)(5), 78q, 78q-1 and 78w; 31 U.S.C. 5318; 42 U.S.C. 4102a, 4104a, 4104b, 4106, and 4128.

2. Section 208.20 and its heading are revised to read as follows:

§ 208.20 Suspicious Activity Reports.

(a) Purpose. This section ensures that a state member bank files a Suspicious Activity Report when it detects a known or suspected violation of Federal law, or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act. This section applies to all state member banks.

(b) Definitions. For the purposes of this section:

26

(1) FinCEN means the Financial Crimes Enforcement Network of the Department of the Treasury.

(2) Institution-affiliated party means any institution-affiliated party as that term is defined in 12 U.S.C. 1786(r), or 1813(u) and 1818(b)(3),(4) or (5).

(3) SAR means a Suspicious Activity Report on the form prescribed by the Board.

(c) SARs required. A state member bank shall file a SAR with the appropriate Federal law enforcement agencies and the Department of the Treasury in accordance with the form's instructions by sending a completed SAR to FinCEN in the following circumstances:

(1) Insider abuse involving any amount. Whenever the state member bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.

(2) Violations aggregating $5,000 or more where a suspect can be identified. Whenever the state member bank

27

detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $5,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an "alias," then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers' license or social security numbers, addresses and telephone numbers, must be reported.

(3) Violations aggregating $25,000 or more regardless of a potential suspect. Whenever the state member bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $25,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.

28

(4) Transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act. Any transaction (which for purposes of this paragraph (c)(4) means a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected) conducted or attempted by, at or through the state member bank and involving or aggregating $5,000 or more in funds or other assets, if the bank knows, suspects, or has reason to suspect that:

(i) The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under federal law;

(ii) The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or

(iii) The transaction has no business or apparent lawful purpose or is not the sort in which the

particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

(d) Time for reporting. A state member bank is required to file a SAR no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of detection of the incident requiring the filing, a state member bank may delay filing a SAR for an additional 30 calendar days to identify a suspect. In no case shall reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. In situations involving violations requiring immediate attention, such as when a reportable violation is on-going, the financial institution shall immediately notify, by telephone, an appropriate law enforcement authority and the Board in addition to filing a timely SAR.

(e) Reports to state and local authorities. State member banks are encouraged to file a copy of the SAR with state and local law enforcement agencies where appropriate.

(f) Exceptions. (1) A state member bank need not file a SAR for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities.

30

(2) A state member bank need not file a SAR for lost, missing, counterfeit, or stolen securities if it files a report pursuant to the reporting requirements of 17 CFR 240.17f-1.

(g) Retention of records. A state member bank shall maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of the filing of the SAR. Supporting documentation shall be identified and maintained by the bank as such, and shall be deemed to have been filed with the SAR. A state member bank must make all supporting documentation available to appropriate law enforcement agencies upon request.

(h) Notification to board of directors. The management of a state member bank shall promptly notify its board of directors, or a committee thereof, of any report filed pursuant to this section.

(i) Compliance. Failure to file a SAR in accordance with this section and the instructions may subject the state member bank, its directors, officers, employees, agents, or other institution-affiliated parties to supervisory action.

(j) Confidentiality of SARs. SARs are confidential. Any state member bank subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed citing this section, applicable law (*e.g.*, 31 U.S.C. 5318(g)), or both, and notify the Board.

31

(k) Safe Harbor. The safe harbor provisions of 31 U.S.C. 5318(g), which exempts any state member bank that makes a disclosure of any possible violation of law or regulation from liability under any law or regulation of the United States, or any constitution, law or regulation of any state or political subdivision, covers all reports of suspected or known criminal violations and suspicious activities to law enforcement and financial institution supervisory authorities, including supporting documentation, regardless of whether such reports are filed pursuant to this section or are filed on a voluntary basis.

PART 211 -- INTERNATIONAL BANKING OPERATIONS (REGULATION K)

1. The Authority citation for 12 CFR Part 211 continues to read as follows:

Authority: 12 U.S.C. 221 et seq., 1818, 1841 et seq., 3101 et seq., 3901 et seq..

§§ 211.8 and 211.24 [Amended]

2. In §§ 211.8 and 211.24(f), remove the words "criminal referral form" and add, in their place, the words "suspicious activity report".

PART 225 -- BANK HOLDING COMPANIES AND CHANGE IN BANK CONTROL (REGULATION Y)

1. The Authority citation for 12 CFR Part 225 continues to read as follows:

Authority: 12 U.S.C. 1817(j)(13), 1818, 1831i, 1831p-1, 1843(c)(8), 1844(b), 1972(l), 3106, 3108, 3310, 3331-3351, 3907, and 3909.

§ 225.4 [Amended]

2. In § 225.4, the heading of paragraph (f) is revised to read "Suspicious Activity Report.".

3. In § 225.4(f), remove the words "criminal referral form" and add, in their place, the words "suspicious activity report".

By order of the Board of Governors of the Federal Reserve System, January 30, 1996.

(signed) William W. Wiles

William W. Wiles,
Secretary of the Board.

WHAT IS A PAYABLE THROUGH ACCOUNT?

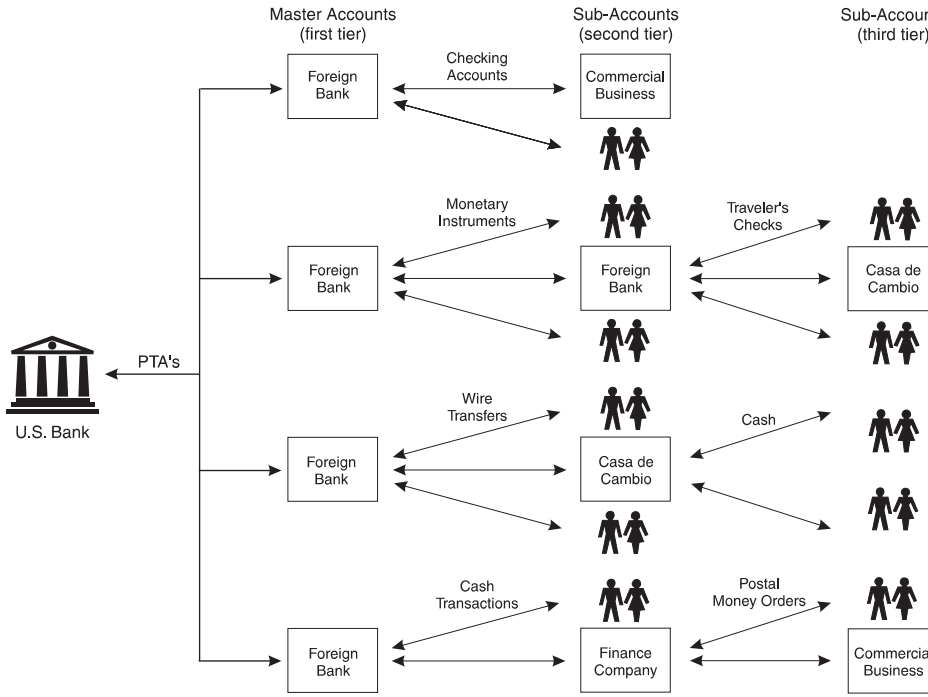
A Payable Through Account (PTA) is a demand deposit account through which banking entities located in the United States extend check-writing privileges to the customers of a foreign bank. Under this PTA arrangement, a U.S. bank, Edge corporation or the U.S. branch or agency of a foreign bank (''U.S. banking entities''), opens a master checking account in the name of a foreign bank operating outside the United States.

The master account subsequently is divided by the foreign bank into ''sub-accounts,'' each in the name of one of the foreign bank's customers. The foreign bank extends signature authority on its master account to its own customers. The number of sub-accounts permitted under this arrangement is virtually unlimited. See Diagram 1.

Deposits into the master account may flow through the foreign bank, which pools them for daily transfer to the U.S. banking entity, or the funds may flow directly to the U.S. banking entity for credit to the master account, with further credit to the sub-account. Checks encoded with the foreign bank's account number, along with a numeric code to identify the sub-account, provide sub-account holders with access to the U.S. payments system. Thus, the PTA mechanism permits the foreign bank operating outside the U.S. to offer its customers, the sub-accountholders, U.S. dollar denominated checks and ancillary services, which may include the ability to receive wire transfers and deposits into the sub-accounts, and to cash checks.

U.S. banking entities may require foreign banks to execute a contract stipulating that all matters pertaining to sub-accounts are the sole responsibility of the foreign bank. Sub-account records are typically maintained by the foreign

Diagram 1



bank in the foreign jurisdiction in which it is chartered and, for the most part, statements and account activity notices are also issued by the foreign bank outside of the United States.

Certain aspects of the PTA arrangement may provide opportunities for illicit activities. First, weak licensing laws, promulgated by a proliferating offshore financial services sector and compounded by weak or absent bank supervision in some offshore financial centers, have created an environment in which access to banking licenses is unencumbered and unregulated.

Second, in the PTA arrangement, the U.S. banking entity may regard the foreign bank as its sole customer. This means that even if the U.S. banking entity has adequate ''know your customer'' guidelines in place with respect to its own customers, such guidelines may not be extended to the customers of the foreign bank.

In addition, some U.S. banking entities routinely permit sub-account holders to have cash deposit and cash withdrawal privileges from the foreign bank's master account. These activities, especially if they are frequent and involve large amounts, indicate a potential for abuse, in light of uncertainty as to the true identity of the sub-account holders. Finally, PTAs used in conjunction with a U.S. office of the foreign bank, such as a representative office or a subsidiary, may enable the foreign bank to, in effect, offer the same services as a branch without being subject to Federal Reserve supervision.

PTAs have been used for many years by credit unions, insurance companies and investment companies. More recently, PTAs have been marketed to foreign banks that do not have a U.S. presence as a way to clear U.S. dollar denominated checks through the U.S. payments system. This product has also been offered under different names by a variety of banking entities. Although the most common alternative names used by banking entities are ''pass-through account'' or ''pass-by account,'' the banking entity may have another name for this product which does not identify it as a PTA. In this event, a further check into the foreign bank correspondent relationships existing at the examined institution may be necessary.

BENEFITS AND RISKS ASSOCIATED WITH PAYABLE THROUGH ACCOUNTS

The objectives of U.S. banking entities marketing PTAs, and foreign banks which subscribe to the PTA service, may vary from situation to situation. However, there are essentially three benefits that currently drive provider and user interest: a) permits U.S. banking entities to attract dollar deposits from the home market of foreign banks without jeopardizing the foreign bank's relationship with its clients; b) provides fee income potential for both the U.S. PTA provider and the foreign bank; and, c) the foreign bank can offer its customers efficient and low cost access to the U.S. payment system.

The safety and soundness risks most likely to be encountered by U.S. banking entities providing PTA services to foreign banks, in addition to the possible use of the banking entities in money laundering schemes, are ''reputational,'' with the potential related loss of business, and the payment of legal expenses. Violations of the Bank Secrecy Act and related statutes, the International Emergency Economic Powers Act, and the Trading with the Enemy Act can also result from the PTA arrangement.

CONTRACTUAL AGREEMENTS

There may be a comprehensive written contract agreement between the U.S. banking entity offering the PTA and the foreign bank that governs their relationship and, among other things, the requirements of the account and services offered, eligible sub-account holders, the accounting and recordkeeping to be done by both parties, fees, and required minimum balance, the provision of overdraft lines of credit, indemnification for bad checks and losses, and the legal jurisdiction under which disputes will be resolved. It is important to note that the contract is between the U.S. banking entity and the foreign bank. The written agreement should be reviewed as it may provide evidence and documentation for the policies and procedures that the U.S. banking entity has developed.

	Y	*N*	*Comments*
1. Review the U.S.-based bank's deposit ledger and determine if the bank offers payable through accounts to foreign banks. If so, identify which banks and country(s) of origin. If no, do not complete this section.			

Advisory #1

The Federal Reserve has established guidelines for the maintenance of payable through accounts. (See SR 95-10 (SUP), March 3, 1995, Section 1402.0 of the BSA Examination Manual). The guidelines state that it is inconsistent with the principles of safe and sound banking for U.S.-based banking entities to offer payable through account services without developing and maintaining policies and procedures designed to guard against the possible improper or illegal use of their payable through account facilities by foreign banks and their customers.

For each payable through account maintained for a foreign financial institution, the U.S. banking entity should either: (1) obtain adequate information about the ultimate users of the payable through accounts; (2) be able to rely on the home country supervisor to require the foreign bank to identify and monitor the transactions of its own customers; or (3) ensure that its payable through account is not being used for money laundering or other illicit purposes.

	Y	*N*	*Comments*
2. Review the contract with the foreign bank. Does the contract: a. address procedures for opening sub-accounts? b. require the master account holder to provide the U.S.-based bank with the true identity of sub-account holders? c. allow cash transactions by sub-account holders within the U.S. borders? d. require the foreign bank to investigate suspicious transactions and report findings to the U.S.-based bank? e. clearly state the liability of both the U.S.-based bank and the foreign bank to which the payable through service is being offered?			

	Y	*N*	*Comments*
f. have approval of personnel with appropriate authority?			
g. have approval of the legal department?			
3. Does the U.S.-based bank have an effective system of internal controls for opening and monitoring payable through accounts that include written policies and procedures providing for:			
a. procedures for opening accounts?			
b. operational procedures?			
c. staff responsibilities?			
d. training?			
e. audit?			
f. identifying and reporting of unusual or suspicious transactions (e.g., money laundering)?			
4. Does the U.S.-based bank apply its ''know your customer'' policy to:			
a. payable through accounts			
b. sub-account holders?			
c. Review documentation to determine effectiveness.			
5. Does the U.S.-based bank prohibit foreign banks from opening *sub-accounts* (second tier) for other foreign banks, casas de cambios, finance companies or other financial intermediaries? If not, what procedures are in place for the U.S. bank to understand the identity of these second-tier sub-accounts holders and the nature of the business transactions (see Diagram #1 in Section 1101.0)?			
6. Does the U.S.-based bank review the listing of account and sub-account holders to ensure that no accounts have been opened to individuals or businesses located in countries that are prohibited with doing business with the U.S. and Specially Designated Nationals or Specially Designated Narcotics Traffickers as determined by the Treasury's Office of Foreign Assets Control?			

	Y	*N*	*Comments*
7. Does the U.S.-based bank have written internal controls policies to monitor account activity for suspicious transactions? Determine how monitoring occurs.			
8. Do the foreign banks that maintain the payable through relationship properly review and explain suspicious transactions to the U.S.-based bank? Review and determine if written procedures provide for the explanation of suspicious accounts.			
9. Does the U.S.-based bank allow cash transactions by sub-account holders? If so, does the U.S. bank properly report CTRs for large cash transactions?			
10. Does the U.S.-based bank conduct audits of payable through accounts to ensure compliance with the contract and appropriate laws and regulations? If so, note the scope and frequency of the audit.			
11. Does the U.S.-based bank conduct audits of the foreign bank, or review in some other way: a. the procedures of the foreign bank for opening accounts, to determine if they are consistent with U.S. requirements? b. the foreign bank's monitoring of sub-account holder activities to detect and report suspicious or unusual transactions?			
12. Does the U.S.-based bank maintain adequate documentary information (i.e. financial statements, licensing confirmation, etc.) regarding the foreign bank?			
13. Has the examiner determined, if possible, whether the home country supervisor of the foreign bank requires banks in that jurisdiction to identify and monitor the transactions of its own customers consistent with U.S. requirements?			
14. Has the U.S.-based bank determined whether the home country supervisor of the foreign bank requires banks in that jurisdiction to identify and monitor the transactions of its own customers consistent with U.S. requirements?			

	Y	*N*	*Comments*
15. After reviewing the responses to procedures 1 through 14, above, answer the questions listed below: a. Does the U.S.-based bank obtain adequate information about the ultimate users of the payable through accounts? b. Is the U.S.-based bank able to rely on the home country supervisor to require the foreign bank to identify and monitor the transactions of its own customers? c. Can the U.S.-based bank ensure that its payable through account is not being used for money laundering or other illicit purposes?			

Advisory #2

If procedure 15, a, b and c is answered in the affirmative, you may stop. In the event that the answer to procedure 15 a, b, or c is in the negative, Federal Reserve guidelines recommend that the U.S.-based banking entity terminate the payable through arrangement with the foreign bank as expeditiously as possible.

	Y	*N*	*Comments*
16. Has the U.S.-based bank taken steps to terminate the account relationship as expeditiously as possible?			

Advisory #3

In those cases where the U.S.-based institution fails to take appropriate steps to terminate the account relationship, the examiner should so note this in the ''Examiners Comments and Conclusions'' page of the examination report, and bring the inappropriate practice to the attention of bank management.