REPORT OF FOREIGN BANK AND FINANCIAL ACCOUNTS, TD F 90-22.1, BY ''BANKS'' LOCATED IN THE UNITED STATES (INCLUDING AGENCIES AND BRANCHES OF FOREIGN BANKS)

The regulation that calls for the reporting of foreign financial accounts implements the Currency and Foreign Transactions Reporting Act of 1970, commonly referred to as the Bank Secrecy Act (BSA). In the late 1960's, law enforcement and tax collection officials noted an increased use of foreign bank accounts by U.S. citizens and residents to evade taxes. Such citizens established and maintained financial accounts in ''tax haven'' countries with strict bank secrecy laws in order to hinder U.S. investigations into their unlawful activities. For example, funds obtained from illicit narcotics sales in the U.S. would be deposited into foreign bank accounts and then repatriated back to the U.S. owner in the form of innocent-appearing sham loans or investments.

The Form 90-22.1 requirements serve two useful purposes in combating the use of foreign financial accounts to circumvent U.S. law. First, the information provides leads to investigators in identifying or tracing illicit funds or unreported income maintained or generated abroad. Also, and often more importantly, the Form 90-22.1 filing requirements provide an additional prosecutorial tool in combating money laundering, tax evasion, drug trafficking, and numerous white collar crimes. Often it is difficult or impossible to obtain detailed evidence of financial activity and assets from outside of the jurisdiction of the U.S. Frequently, this evidence is critical in convicting violators of U.S. law who use foreign financial accounts to ''cover the tracks'' of their illegal activities. Generally, such persons do no comply with the Form 90-22.1 filing requirement as they do not want to notify the government of their interest in foreign financial accounts. Accordingly, persons may be prosecuted for criminal violation of the reporting requirements instead of for commission of the underlying crimes.

Treasury Form 90-22.1 is used to report foreign account relationships and is required by section 103.24 of the BSA regulations, 31 C.F.R. Part 103. The BSA is not an income tax statute, and Form 90-22.1, though filed with the Internal Revenue Service, is not a tax form. Accordingly, a person may have a Form 90-22.1 reporting obligation even though that person's assets held through foreign accounts produce no taxable income.

In general, each United States person having a financial interest in, or signatory authority over, foreign financial accounts with an aggregate value exceeding $10,000, must report the account relationships to the Internal Revenue Service. See form 90-22.1, Instruction A, and Sections 103.24 and 103.27 of the Bank Secrecy Act regulations, 31 C.F.R. Part 103. A report must be filed for each calendar year in which the aggregate value of the foreign accounts exceeded U.S. $10,000. No report is required for calendar years where the aggregate value of the foreign financial accounts at no time exceeded U.S. $10,000.

The term ''United States person'' means (1) a U.S. citizen, (2) a resident of the United States e.g., any individual who was in the United States for any 60 consecutive day period during the reporting year, (3) a domestic partnership, (4) a domestic corporation, or (5) a domestic estate or trust. A branch, agency, or representative office of a foreign corporation, including a foreign bank, which is not recognizable as a separate legal personality is not a United States person for the purposes of this form.

An officer or employee of a federally-insured depository institution branch, or agency office within the United States of a foreign bank that is subject to the supervision of a federal bank regulatory agency need not report that he or she has signature or other authority over a foreign bank, securities or other financial account maintained by such entities unless he or she has a personal financial interest in the account. See form 90-22.1, Instruction A.

Form 90-22.1 shall be filed on or before June 30 of each calendar year with the Internal revenue Service, Post Office Box 32621, Detroit, Michigan 48232. The year for which the report is made must be identified on the form. Please note that if an extension of time to file is needed, request such extension by writing to the Financial Crimes Enforcement Network, Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Washington, D.C. 20220.

Accounts subject to reporting are all maintained with a bank (except a military banking facility as defined in Instruction E) or broker or dealer in securities that is located in a foreign country, even is it is part of a Unites States bank or other institution. Accounts maintained with a branch, agency, or other office of a foreign bank or other institution that is located in the United States, Guam, Puerto Rico, the Northern Mariana Islands, American Samoa, the Trust Territory of the Pacific Islands, and the Virgin Islands are not foreign accounts and are not subject to reporting. Foreign assets (such as securities issued by foreign corporations) that are held directly by a U.S. person, or through an account maintained with a U.S. office of a bank or other institution are not subject to the BSA foreign account reporting requirements. Form 90-22.1 is for the reporting of foreign accounts, and not all ''foreign'' assets owned or controlled by U.S. persons. Also, international, interbank transfer accounts (''nostro accounts'') held by domestic banks are not subject to reporting on Form 90-22.1 52FR 11436, 11438 (April 8, 1987).

Reportable bank accounts include both deposit accounts and loan/credit line accounts. The term ''bank deposit account'' means a savings, demand, checking, or any other funds deposit account maintained with a financial institution or other person engaged in the business of banking. It includes certificates of deposit. The term ''loan/credit line account'' means disbursed loan, funds drawn under credit lines, and secured, undrawn credit lines and other secured, undisbursed extensions of credit by a financial institution to a U.S. person. A federally insured depository institution, however, should not report any loans and credit extensions from foreign banks.

Advisory #1

The Federal Reserve has developed examination procedures for reviewing compliance by U.S.-based institutions, whether domestic or foreign operated, with the Bank Secrecy Act (''BSA'') and other related anti-money laundering statutes. These procedures, entitled the ''Workprogram for Financial Recordkeeping and Reporting of Currency and Foreign Transactions Examination,'' is designed for conducting BSA reviews of the U.S-based operations only and can be located at Section 100 of the *BSA Examination Manual*.

In contrast, the following examination procedures should be utilized by the examiner when conducting BSA on-site reviews of the overseas operations of U.S.-based institutions. It is imperative that the examiner understand that each foreign country may have its own anti-money laundering statutes, if any at all, and that the statutes may differ significantly from those utilized in the U.S. The availability of records may also differ significantly from the U.S.

Advisory #2

The following examination procedures have been designed to be completed in two parts. The first is to be completed at the head office in the U.S. prior to conducting the on-site examination of the overseas branch or subsidiary of the U.S.-based institution. The second relates to the on-sight foreign country review.

PART 1: HEAD OFFICE REVIEW

Operational Considerations On-Site in the U.S.

Contact the appropriate U.S. representative with overseas branch/subsidiary responsibility to advise that information regarding BSA and related anti-money laundering laws is needed to conduct the initial portion of the examination. Follow-up the conversation in writing to request the needed information.

The following information, at a minimum, should be obtained from the head office:

	Y	*N*	*Comments*
1. Policies and Procedures Does the head office maintain and periodically review policies and procedures for overseas operations? The following should be reviewed: a. Policies and procedures applicable to the foreign offices such as the corporate policy statement or program designed to monitor compliance with U.S. and local anti-money laundering statutes. b. Applicable laws and regulations affecting the foreign operations. Does the foreign country in which the institution operates maintain similar reporting requirements as that of the U.S.?.			

	Y	*N*	*Comments*
c. The mission statement and a detailed description of the foreign branch/subsidiary's primary business and a listing of the services offered (i.e. retail, wholesale, private banking, trust, money exchange, letters of credit secured with cash or time deposits).			
d. Organization Chart, including a listing of management and other key personnel at the foreign offices.			
e. Listing of financial reports available from the foreign branch/subsidiary and copies of the most recent reports forwarded by the foreign operation to the head office to determine: • addresses/recipients • method of reporting to the U.S. • content of required reports • frequency of reports • required responses to provided reports (review responses) • record retention requirements at the foreign operation • type of accounting systems in place (manual or automated)			

Advisory #3

The examiner should determine whether or not the records on-site at the foreign operation are available in a foreign language only and if so, what arrangements can be made to translate the information.

	Y	*N*	*Comments*
2. Audit Are internal or external audit reports available? Contact should be made with the auditor responsible for the on-site overseas audit to determine the: a. scope of internal/external audits b. frequency of audits c. location of audit workpapers d. audit procedures implemented e. reporting lines			

	Y	*N*	*Comments*
2. Audit (Continued) Is a copy of the latest internal and/or external audit of the overseas operation available at the head office? If so, review the audit for pertinent information that may assist the conducting of the on-site review. Has senior management reviewed the internal and/or external audits and implemented corrective actions regarding criticisms noted within the audits?			

Advisory #4

Section 1502 of the *BSA Examination Manual* contains information regarding the Financial Action Task Force (FATF) and its recommendations to member countries in adopting anti-money laundering statutes. For each foreign country in which the U.S. institution operates, management should be able to provide information regarding the foreign country's adoption of the FATF recommendations. Keep in mind that a foreign country's formal adoption of the FATF recommendations does not necessarily mean that the anti-money laundering statutes and regulations are now in place, or that the statutes and regulations are being adequately followed by the financial community or monitored by the country's federal government. The foreign country on-site examination should be able to assist you in making the determination as to the adequacy of the country's adoption of the FATF recommendations.

Advisory #5

The U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC") administers laws that impose economic sanctions against foreign countries to further U.S. foreign policy and national security objectives. OFAC is also responsible for making regulations that restrict transactions by U.S. persons or entities (including banks), located in the U.S. or abroad, with certain foreign countries, their nationals or "specially designated nationals.[1]" OFAC regularly provides to banks, or banks may subscribe to certain databases or other informational providers (including the *Federal Register*), current listings of foreign countries and designated nationals that are prohibited from conducting business with any U.S. entity or individual. Some of the OFAC examination procedures listed below can be conducted at the head office while others may have to be checked during the on-site foreign country review. Refer to Section 1505 for additional information.

1. Includes "specially designated narcotics traffickers," "specially designated terrorists," "blocked persons," and "blocked vessels."

	Y	*N*	*Comments*
3. Office of Foreign Assets Control (OFAC)			
Does the institution have policies and procedures in place for complying with OFAC laws and regulations?			
Does the U.S. bank maintain a current listing of OFAC information?			
Is the OFAC information disseminated to foreign country offices?			
Are new accounts compared to the OFAC listing prior to opening?			
Are established accounts regularly compared to current OFAC listings?			

Advisory #6

Deliver a first day letter to the U.S. office for each foreign branch or subsidiary to be examined. The head office should be able to provide the name(s) of responsible personnel to be contacted and to ensure their presence during the on-site portion of the examination. Tailor the first day letter to reflect information obtained from the U.S. head office examination. The following is a list of some of the information that should be available prior to the on-site country review:

	Y	*N*	*Comments*
4. First Day Letter			
List of the different currencies used in cash operations.			
Average amount of cash held on premises in a normal working day.			
Information concerning customers, including type of business and location, who frequently conduct large cash transactions.			
List of banks that ship/receive currency with the foreign country offices.			
Copy of procedures and sample reports used to monitor large currency deposits.			
Description of teller systems (automated or manual).			
Description of and sample reports utilized in conducting electronic funds transfers.			
Average volume of daily funds transfers.			
List of private banking/trust accounts, including name and country of origin.			
List of banks that clear dollar denominated instruments (e.g., checks, money orders, and traveller's checks).			

Advisory #7

Upon completion of the examination of the head office records, you may be able to make an adequate assessment of the entire operations efforts, both domestically and internationally, in complying with the BSA and other related statutes. Nonetheless, you should complete as many of the overseas on-site procedures located in Part 2 as possible.

Advisory #8

Prior to the commencement of the on-site foreign country review, you should check with your Reserve Bank BSA representative to determine the nature and scope of any examination conducted on the institution or foreign country anti-money laundering initiatives by either the home country supervisor or team of FATF auditors.

PART 2: ON-SITE FOREIGN COUNTRY EXAMINATION

	Y	*N*	*Comments*
5. Internal Compliance Program and Procedures Does the institution follow a written program? Does the written program provide for the following: a. a system of internal controls to ensure compliance with applicable rules, regulations and internal policies? b. independent testing for compliance? If conducted by an outside party, list the name of the party. c. a designated position(s) responsible for daily compliance with BSA and related statutes? List name(s) of individuals. d. training for personnel? e. adequate control of currency flows and cash transactions?			
6. Know Your Customer Policy Does the institution have policies and procedures that require reasonable efforts to be made to ascertain the identity of individuals and/or stated business purpose of each commercial enterprise with whom the institution conducts business? (Refer to Section 600 of the *BSA Examination Manual*—"Know Your Customer") Does the institution allow accounts to be opened under fictitious names? If so, does the institution maintain records containing the actual names and other identifying information regarding the individuals and their stated "activities?" Do the bank employees receive adequate training regarding the identifying and reporting of unusual or suspicious transactions? Does the bank have an adequate monitoring system to identify unusual or suspicious transactions (structuring of cash transactions, concentration of accounts, unusual wire transfer activity, cash collateralized loans, or other transactions inconsistent with the nature of a customer's stated business activity)?			

	Y	*N*	*Comments*
7. Private Banking and Trust Departments Does the institution provide for private banking or trust services in the host country? If so, determine what requirements are necessary for opening an account: a. identification b. recommendation from third party c. business or profession Are numbered accounts or accounts with coded names permitted? If so, review documentation of: a. actual names and country of origination b. concentration of accounts by country Determine the source and destination of funds (checks, wires).			
8. Wire Transfers What systems are in place for recording the initiation and reception of wire transfers (automated, manual)? Is documentation available to identify the remitter, destination and description of the transaction? Does the institution maintain daily transaction logs for both incoming and outgoing transfers? Does the institution accept cash from non-customers to initiate funds transfers? Do wire room personnel receive regular training in anti-money laundering procedures and the identification of unusual or suspicious activities?			

Advisory #9

Credit extensions can serve as one of the channels to conceal money laundering activities, whether extended to individuals or business entities. In view of the numerous methods and complex nature of such transactions, you should complete the following procedures. The list is not meant to be exhaustive, rather, it should provide a conceptual framework for analysis.

	Y	*N*	*Comments*
9. Credit Extensions			
Does the bank have a clear understanding of its customers business and credit needs?			
Does the bank clearly understand the ownership structure of corporate borrowers?			
Is the purpose of the credit extension well defined and commensurate with the business activity?			
Are the sources of payment well defined? What is the repayment history (are extensions paid down ahead of schedule?)?			
Are credits secured with cash? If so, what is the reasoning and is this structure in line with the client's business objectives and needs?			
Are cross-border credit extensions being booked on the basis of cash deposits at an affiliate or correspondent bank?			
Is the pricing of credit services in line with general practices, including the payment of ''up-front'' fees?			

Advisory #10

Section 1100 of the BSA Examination Manual provides information on ''Payable Through Accounts.'' You should determine whether the foreign country operation deals in such accounts and what policies and procedures are in place for the proper opening and monitoring of such relationships. A review of the correspondent bank relationships should also be conducted.

Findings, particularly criticisms, should be noted in the consolidated examination report and brought to management's attention.

Advisory #11

If there are adequate policies, procedures and internal controls regarding currency flows, stop here. If not, proceed to #10.

	Y	*N*	*Comments*
10. Bank Secrecy Act (Anti-Money Laundering Statutes) Does the foreign branch/subsidiary accept cash for deposits, loan payments or other financial transactions? If so, review the following: a. teller operations, including daily cash proof sheets, tapes, computer-generated reports and any other documents to support the cash activity. b. sources of cash (clients, non-clients) c. uses of cash (deposits, wire transfers, purchase of monetary instruments) Are deposits accepted for U.S. accounts? If so, ascertain how credit is accomplished (pouch delivery, nostro account debit/credit). Determine the make-up of the deposits. Is the U.S. foreign office in compliance with local anti-money laundering statutes regarding reporting and record retention.			

Sound Practices Paper—Private Banking
Prepared by the Federal Reserve Bank of New York, July 1997

Section 1301.0

This paper presents the observations of examiners of the Federal Reserve Bank of New York regarding sound risk management and internal control practices with respect to private banking activities. Findings are based on a year-long cycle of on-site examinations of the risk management practices of approximately forty institutions in the Second Federal Reserve District that are engaged in the provision of financial services to high net worth individuals, which is commonly referred to as private banking. These examinations represented a cross section of commercial banks, Edge Act corporations, trust companies, and U.S. branches of foreign banks. Our examiners found varying degrees of sophistication and depth in private banking activities. And, we recognize that what constitutes sound practice may vary according to the particulars of each organization's business.

The guidance presented in this paper is not a regulation and should not be interpreted as such. The sound practices reflect the type of information banks need to have to satisfy existing legal requirements as well as transactions testing performed by examiners, and the types of controls essential to minimize reputational and legal risk and deter money laundering. The goal of the paper is to ensure that banks are aware of the major issues currently under review by regulatory and legal authorities and to further the dialogue with institutions engaged in private banking.

Heightened supervisory interest in private banking activities primarily reflects market developments. Recently, domestic and foreign banking organizations have been increasing their private banking activities and their reliance on income from this business line. Several large institutions reported plans to increase sharply the net contribution of private banking to their organizations' earnings. Additionally, the target market for private banking—high net worth individuals—is growing and becoming more sophisticated and diverse with regard to product and service preferences and risk appetites. As the target market for private banking is growing, so is the level of competition among institutions that provide private banking services. Banking organizations are experiencing competition for private banking clients from non-bank financial institutions, including securities dealers, and asset management and brokerage firms. Accordingly, there are increased pressures on the relationship managers and marketing officers of banking organizations to obtain new clients, increase their assets under management, and contribute a greater percentage to the net income of their organizations.

The reviews underlying this paper focused primarily on assessing each banking institution's ability to recognize and manage the potential reputational and legal risks that may be associated with inadequate knowledge and understanding of the clients' personal and business background, source of wealth and use of their private banking accounts. Also considered were the essential characteristics of an appropriate control infrastructure that is suited to support the effective management of these risks.

To varying degrees, the sound practices identified here either are currently in place or are in the process of being implemented in most institutions, although it is recognized that practices observed in the United States may differ from global practices. The discussion is structured as follows: (I) management oversight, (II) policies and procedures, (III) risk management practices and monitoring systems, and (IV) segregation of duties, compliance and audit.

I. MANAGEMENT OVERSIGHT OF PRIVATE BANKING

Senior management's active oversight of private banking activities and the creation of an appropriate corporate culture are crucial elements of a sound risk management and control environment. Senior management is responsible for identifying clearly the purpose and objectives of the organization's private banking activities. A statement that describes the target client base, the range of services offered to clients, and the financial objectives and risk tolerances should be approved by senior management and establish accountability for risk management and control functions. Well-developed goals and objectives not only describe the target client base in terms of factors such as minimum net worth, investable assets and the types of prod-

ucts and services sought, but specifically indicate the types of clients the institution will and will not accept, and establish multiple and segregated levels of authorization for new client acceptance. Institutions that follow such sound practices will be better positioned to design and deliver products and services that match their clients' needs, while reducing the likelihood that unsuitable clients will be accepted.

Senior management should be actively involved in strategic planning for the private banking operation. Sound strategic planning should involve not only setting targets such as revenue, assets under management, and the number of new accounts, but also include the establishment of control and risk management goals, such as satisfactory audit and compliance reviews. The most control-conscious institutions have passed these and other specific qualitative goals through to relationship managers. In some cases, they have included these factors in employee compensation schemes, thus promoting accountability and responsibility for risk management and control processes.

The culture that exists within the private banking operation invariably reflects senior management's level of commitment to controls and risk management. A focused, integrated, ''top-down'' approach to embracing risk management and control concepts will most effectively foster an environment in which managers and staff are knowledgeable and aware of the risks in their portfolio. This approach to private banking activities will help ensure that staff members apply consistent practices, communicate effectively, and assume responsibility and accountability for controls.

Each organization should ensure that its policies and procedures for conducting private banking activities are evaluated and updated regularly, and that there is a clear delineation of roles, responsibilities and accountability for implementing such policies and procedures.

II. POLICIES AND PROCEDURES

As a private banking operation frequently functions as a ''bank within a bank,'' there are different policies and procedures needed to govern its activities and operations. This paper focuses primarily on the significance of sound Know Your Customer (''KYC'') policies and procedures in managing the reputational and legal risks inherent in private banking activities.

Know Your Customer Policies and Procedures

Nearly all of the institutions examined had written KYC policies and procedures—most of which captured the spirit of sound KYC guidelines. These institutions have taken a reasonable approach to including essential components of a sound KYC policy in their written policies, such as: obtaining identification and basic background information on the clients, describing the clients' source of wealth and line of business, requesting references, handling referrals and identifying red-flags or suspicious transactions. Policies also should require that the clients' source of wealth and funds be corroborated and include specific guidelines on how to corroborate information provided by the client. Sound policies also define acceptable KYC information for different types of account holders, such as individuals, operating companies, personal investment companies (''PICs''), trusts, clients of financial advisers or other intermediaries, and financial advisers. These policies also should recognize that contact/visitation reports written by private bankers, which document their meetings with clients in their home countries and places of business, are an important component to the KYC process.

Additionally, sound policies require that the type and volume of transactions expected to be passing through the clients' accounts be documented, with actual flows monitored to assist in detecting suspicious or unusual transactions. Accountability for following up on suspicious activities and making such reports as may be required should also be clearly assigned.

Compliance with policies should be expected by senior management as a matter of course; waivers should be the exception, not the rule, and reasons for any exception should be documented. Moreover, all waivers should be handled by authorized personnel—thus reinforcing senior management's oversight of the risk management process. Clearly, the best written policies and procedures will not work unless they are implemented effectively and modified appropriately to reflect changing industry practices.

Credit Policies and Procedures

Lending to high net worth individuals and their business concerns often takes on unique banking

characteristics. The majority of private banking lending is fully secured—often by cash, securities and other assets held by the private banking function. Thus, the extensions of credit to high net worth individuals on a secured basis should not result in compromising sound underwriting standards. If credit is extended based on collateral, even if the collateral is cash, repayment is not assured. For example, collateral derived from illicit activities may be subject to government forfeiture. Accordingly, when extending secured private banking loans, institutions should be satisfied as to the source and legitimacy of the client's collateral, the borrower's intended use of the proceeds and the source of repayment. Some institutions have appropriately recognized that, when lending to high net worth individuals, whether on a secured or unsecured basis, the creditworthiness determination is bolstered by a thorough and well-structured KYC process.

III. RISK MANAGEMENT PRACTICES AND MONITORING SYSTEMS

Effective risk management practices and systems that carry out the KYC policies are the foundation of a sound risk management process. These practices should be well-integrated within the organization and reassessed on an ongoing basis. Additionally, relevant personnel should recognize their roles in the process, as well as their accountability.

Documentation and Due Diligence

Virtually all institutions perform more due diligence on relationships established currently than on accounts that were opened in the past. They are supplementing basic account-opening information, such as identification through passports and national identity cards and other basic personal and business data, including the client's mailing address, profession, and estimated net worth, with more detailed and substantive information. Sound practice requires institutions to obtain references on their clients from reliable, independent sources, such as other financial institutions, the client's business associates, attorneys or accountants. Independent references that describe the capacity in which the referring party knew the client and the nature of their relationship are important components of the KYC process, and institutions routinely should seek to obtain these references. Furthermore, if internal references from personnel that serve the client from an affiliated office are used, such references should be accompanied by detailed, well-supported documentation.

Institutions employ a wide array of sound practices to corroborate a client's source of wealth and business activities, in addition to obtaining references. For example, some institutions have obtained private credit agency reports on their clients' businesses, including those in foreign countries. Private bankers have also sought out public information on high profile clients in the press, periodicals and through standard database searches. Sound practice also suggests that private bankers obtain financial statements, marketing brochures, and annual reports of clients' businesses as additional corroboration sources.[1] Examinations have confirmed that there are relatively easy and unobtrusive ways to corroborate a private banking client's source of wealth, whether that client is from the United States or abroad.

A concerted effort should be made to embrace these due diligence practices with prospective and existing private banking clients to assure that a client's source of funds is legitimate. While most institutions emphasized the significance of documentation and due diligence during the client acceptance process, it is equally important to ensure that client profiles are appropriately updated throughout the relationship with the client.

Most banking institutions maintain and manage accounts for PICs in their U.S. offices; in fact, frequently PICs are established for the client—the beneficial owner of the PIC—by one of the institution's affiliated trust companies in an offshore secrecy jurisdiction. The majority of these institutions employ the sound practice of applying the same general KYC standards to PICs as they do to personal private banking accounts—they identify and profile the beneficial owners. Most institutions had KYC documentation on the beneficial owners of the PICs in their U.S. files.

1. Note that dealings with certain types of entities—pension funds or public entities such as municipalities—require additional procedures. When dealing with a pension fund certain disclosure requirements of ERISA may apply, and a knowledge of relevant statutes or regulations may be required when dealing with public entities.

The beneficial owners of PICs have a legitimate right to protect their financial privacy, and some high net worth private clients may have a special and legitimate need for confidentiality—because of their public prominence, for example. The needed confidentiality in these cases may be afforded by promulgating special protections as to access to the records revealing the identity of a beneficial owner of a PIC. However, the ability to make proper identification of the beneficial owner remains an important control within the banking organization. First, without this control, the banking organization cannot satisfy its compliance obligations with respect to legal process served on the banking organization, which might reach property owned or controlled by a particular beneficial owner, including the PIC itself. If the banking organization has structured its records in a way that makes it impossible to comply with such process, this could cause the organization serious compliance problems. Second, the lack of transparency may be an impediment to the banking organization's understanding of its overall relationship with a particular beneficial owner; and the existence of accounts for one or more PICs could confuse the organization about the nature and depth of the overall relationship if the identity of the beneficial owner is masked within management information systems. Finally, there is no legal impediment to maintaining appropriate records. The law in the foreign jurisdiction where the PIC is organized ordinarily should present no obstacle to recording the beneficial owner in a record that the banking organization maintains with respect to a PIC account in the United States.

KYC standards for the beneficial owners of PICs (and similarly for those of offshore trusts and foundations) should be no different from those of other personal private banking accounts. Further, institutions maintaining such accounts in the United States should be able to make available, within a reasonable period of time, the identities and full KYC profiles of the beneficial owners when requested by supervisors performing test-checks of their KYC programs.[2]

Use of ''Omnibus'' and ''Concentration'' Accounts

Sound practice calls for each private banking client to have its own account(s) at the bank, through which all of the client's transactions are directed. Private banking operations should have the policies and controls in place to confirm that a client's funds flow into and out of the client's account(s), and not through any other account, such as the organization's suspense, omnibus or concentration accounts. Generally, it is inadvisable from a risk management and control perspective for institutions to allow their clients to direct transactions through the organization's suspense account(s). Such practices effectively prevent association of the clients' names and account numbers with specific account activity, could easily mask unusual transactions and flows, the monitoring of which is essential to sound risk management in private banking, and could easily be abused.

Management Information Systems

The management information systems (''MIS'') associated with private banking activities were reviewed with a focus on the utility, thoroughness, timeliness and accuracy of data reported to management and responsible individuals. While the size and complexity of the private banking operation at each organization will affect the resources devoted to MIS, private banking operations should make effective use of current technology to support their risk management framework. The level of MIS support given to private banking frequently was weaker than the support given to other areas of the same banking organization. In such cases, institutions should develop specific plans to change or upgrade their MIS.

MIS should be migrating towards providing management with timely information necessary to analyze and manage effectively the private banking business. The types of reports that may meet this objective are those that reflect each client's holdings, including those held through PICs and any affiliated accounts; any missing account opening documentation; transactions made through a client's accounts that are

2. Similarly, KYC standards should be no different than those applicable to private banking accounts when the institution deals with a financial adviser or other type of intermediary acting on behalf of a client. In order to perform its KYC responsibilities, the institution should identify the beneficial owner of the account (usually the intermediary's client, but, in rare cases, the intermediary itself) and perform its KYC analysis with respect to the beneficial owner. The imposition of an intermediary between the institution and the counter party should not lessen the private bank's KYC responsibilities.

unusual; and the private banking function's profitability. Institutions that manage private banking activities on a decentralized, functional basis may face challenges in uneven implementation of policies and procedures and in aggregating a client's total relationship with the institution, as the client's account balances might be recorded on disparate systems. Institutions with integrated management of private banking activities have more success in capturing and reporting a client's complete relationship. Management's ability to measure and analyze each client's complete relationship with the organization is a key element for sound risk management, and MIS should support that objective.

MIS should be capable of monitoring accounts for unusual and potentially suspicious activities. Many institutions are developing or enhancing systems which will identify transactions that warrant explanation and evaluation because of their size, volume, pattern, source or destination. Systems that identify individual transactions on an exception basis, for example those that are above established thresholds in dollar amount and volume, are more appropriate in the detection of aberrations in transactional behavior than systems that only recognize net balance changes. There is a wide array of thresholds used to initiate exception reports—some institutions use a dollar minimum for each transaction, regardless of the type of client or activity, while others segregate their client base and establish different dollar/volume thresholds for transactions pertaining to each client grouping or to each individual client account. Each institution should implement exception reporting that makes sense and provides appropriate information within the context of its particular business. It should recognize that the systems and reports are valuable only if there are individuals who are responsible for receiving, analyzing and acting on the information generated.

Reporting Suspicious Activity

Procedures established to investigate and, if necessary, report suspicious private banking activity also were reviewed. If legal, reputational, and other risks are to be controlled, there must be a heightened focus on preventing and detecting money laundering and other unlawful activity. Financial institutions clearly have a key responsibility in that process. The Federal Reserve's Suspicious Activity Reporting regulations, which became effective April 1, 1996, and are similar to regulations issued by the OCC, FDIC, OTS, NCUA and the Treasury, impose a duty to file a Suspicious Activity Report (''SAR'') for any transaction that:

> ''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 institution knows of no reasonable explanation for the transaction after examining the available facts including the background and possible purpose of the transaction.''

Some institutions with global private banking activities have recognized the advantages in applying their suspicious activity monitoring procedures globally, as they will be better equipped to detect and analyze patterns and trends of suspicious transactions within their organizations. Private banking senior management should ensure that sound practices are being followed throughout their organization. Management should ensure there is a proactive approach and well-established procedures covering the SAR process and that accountability exists within their organization for the analysis and follow-up of internally identified suspicious activity, for the decision-making process as to whether or not to file a SAR, and for maintaining or closing an account. Because there is a legal requirement to report suspicious transactions, it is essential for banking organizations to maintain internal programs that ensure compliance.

IV. SEGREGATION OF DUTIES, COMPLIANCE AND AUDIT

Ensuring effective implementation of established policies and procedures is a significant challenge to many private banking operations. Institutions that evidence ongoing progress towards conformity with stated policies and procedures are those that recognize the importance of segregation of duties and provide adequate attention, direction and support to the individuals responsible for compliance and internal audit.

Segregation of Duties

Adequate segregation of duties in the KYC

process is of critical importance. Institutions should not rely exclusively on any individual relationship manager or immediate supervisor to, for example, waive documentation required to open an account, approve the client profile, authorize a new client relationship, fully identify (or ''know'') the client, and monitor client accounts for unusual transactions. The more control-conscious institutions ensure that an independent unit—such as compliance, risk management or senior management—also has responsibility for these functions. Some institutions have segregated KYC duties in a KYC committee comprised of relationship managers, compliance, and senior management to determine, prior to the acceptance of any new client, if the potential client's profile meets the institution's KYC standards. Many institutions have also introduced the concept of ''back-up relationship managers'' or ''client teams'' to minimize the risk of a single relationship manager having exclusive knowledge and control over individual relationships.

Segregation of duties clearly facilitates the private banking operation's compliance with policies and procedures and, consequently, minimizes reputational and legal risk. Institutions that have not already established independent control over the above-mentioned activities are urged to introduce such measures as soon as possible.

Compliance

Compliance functions are most effective if they are proactive in ensuring the integrity of the control infrastructure of the private banking operation, as opposed to being reactive to specific, isolated events. They should ensure that policies and procedures are being followed by conducting frequent *ad hoc* reviews and tests that measure how different groups within the private banking function are complying with the policies and procedures. Some institutions assign to compliance the responsibility for reviewing all prospective client profiles to determine if the relationship managers have satisfied the institutions' profiling requirements, obtained necessary documentation and taken appropriate action where problems arise. Compliance functions should also be in a position to recognize promptly any client activity that may be unusual, to question relationship managers about the nature of potentially suspicious activities, and to follow through on their inquiries and suspicions. Compliance functions work effectively only when they have senior management commitment and sufficient resources to accomplish their mission.

In creating a culture that follows best practices of risk management and internal control, institutions should conduct frequent training of personnel that is reinforced at regular intervals, particularly in providing the ''how to'' of client profiling, conducting due diligence, preparing customer call reports and detecting and responding to unusual activities. In some cases, KYC training has been incorporated into the overall marketing and sales training programs. This serves to integrate the concepts of knowing the client's personal and business background, and source and legitimacy of wealth with those relating to the selling of appropriate products and services that meet the client's needs and interests. The majority of institutions provide training on money laundering and documentation requirements for their compliance staff. Institutions also should incorporate this training into programs conducted for their relationship managers.

Internal Audit

Comprehensive private banking audit programs are based on risk ratings that apply an appropriate weighting to the major risks of the business, such as reputational and legal risk, and audits that are conducted with sufficient frequency and involve adequate transaction testing to determine the effectiveness of the internal control environment. KYC testing, for example should be a critical element.

As internal audit plays a crucial role in independently evaluating the risk management and controls, management should ensure that audit functions are staffed adequately with individuals who are well-versed in private banking. In addition, auditors should be proactive in following-up on their findings and criticisms.

Conclusion

The purpose of this paper is to provide sound practice guidance to institutions that are engaged in private banking, while at the same time

contribute to the ongoing national and international discussion of the difficult challenges of implementing effective Know Your Customer policies and procedures. Banks face a major responsibility with their affirmative legal obligation to prevent money laundering. This is particularly true in light of the general expectation that private banking will grow significantly in size, complexity and diversity over the next several years, with the result that business practices, policies and procedures will need to be reviewed and revised to ensure effective risk management. We look forward to continuing our dialogue with banks engaged in private banking.

BOARD OF GOVERNORS

of the

FEDERAL RESERVE SYSTEM
Washington, D.C. 20551

AD 93-56 (FIS)

September 22, 1993

TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK

SUBJECT: Bank Secrecy Act—Department of the Treasury Rulings and Directives

The Department of the Treasury, Office of Financial Enforcement, recently issued two Administrative Rulings, a policy statement and a directive with regard to Bank Secrecy Act (BSA) compliance. Summaries of these are set forth below. Additionally, copies of the Administrative Rulings and the policy statement are attached.[1] Reserve Banks are requested to disseminate this information to the examination staff and, in accordance with a request from the Department of the Treasury, to all domestic and foreign banking organizations supervised by the Federal Reserve.

ADMINISTRATIVE RULINGS

The following Administrative Rulings issued by the Department of the Treasury are with regard to: 1) the identification of elderly or disabled patrons that conduct large cash transactions or purchase monetary instruments with currency in amounts between $3,000 and $10,000; and 2) proper completion of the Currency Transaction Report (IRS Form 4789) for multiple transactions:

Administrative Ruling 92-1—Identification Of Elderly Or Disabled Patrons Conducting Large Currency Transactions

The BSA requires financial institutions to verify and record the identity of individuals conducting reportable currency transactions. However, certain elderly or disabled patrons do not possess identification documents that would normally be accepted within the banking community (e.g. driver's license, passport, state-issued identification card). Administrative Ruling 92-1 (AD 92-1) allows for other methods of verification of identification to be utilized. Financial institutions must establish formal written procedures consistent with AD 92-1 and, once implemented, there can be no exceptions to the procedures.

Administrative Ruling 92-2—Proper Completion Of The Currency Transaction Report (CTR), IRS Form 4789, When Reporting Multiple Transactions

The BSA requires financial institutions to report currency transactions that exceed either $10,000 or an exempted account's established limit. Multiple currency transactions are treated as a single transaction when the institution has knowledge that the transactions by or on behalf of any person, conducted during any business day, exceed either $10,000 or the exemption limit. When reporting multiple transactions, item 3d of the CTR must be checked and the information in item 48 of the CTR must be provided. Administrative Ruling 92-2 explains the procedures to be followed in completing a CTR for these cases.

1. Administrative rulings located in prior sections of BSA manual.

Exemption Policy For Retail Accounts In Which Retail and Money Order Sale Proceeds Are Commingled

The Department of the Treasury has issued a policy statement with regard to exemption procedures for retail accounts in which retail and money order sale proceeds are commingled. The policy statement amends the current policy that such accounts cannot be exempted from the filing of CTRs.

CURRENCY TRANSACTION REPORTS FILING DEADLINES DIRECTIVE

In 1988, the Department of the Treasury exempted all banks from the 15-day filing requirements of the BSA (31 C.F.R. 103.26 (a)(1)(1987)) with respect to the filing of CTR's on magnetic tape. For CTR's that are filed magnetically, banks must file the CTR's with the IRS Detroit Computing Center within 25 days following the date on which a reportable transaction occurs.

It is important to emphasize that this exemption applies only to CTR's filed magnetically pursuant to an agreement between a bank and the IRS. If for any reason a bank should withdraw from the magnetic tape program or for any other reason file paper CTR's, these CTR's must be filed within the 15-day period following the reportable transaction (31 C.F.R. 103.27(a)(1) (1989)).

If you have any questions regarding these procedures, you may call Richard Small, Special Counsel, at (202) 452-5235, or Dan Soto, Senior Special Examiner, at (202) 728-5829.

Stephen C. Schemering
Deputy Director

Attachment

DEPARTMENT OF THE TREASURY

WASHINGTON

OFFICE OF FINANCIAL ENFORCEMENT EXEMPTION POLICY FOR RETAIL ACCOUNTS IN WHICH RETAIL AND MONEY ORDER SALE PROCEEDS ARE COMMINGLED

(August 27, 1993).

Section 103.22(b)(2)(i) of the Bank Secrecy Act (BSA) regulations authorizes a bank to unilaterally exempt from the Currency Transaction Report (CTR) reporting requirement deposits to or withdrawals of currency from an existing account by an established depositor who is a United States resident and operates a retail type of business in the United States. However, the BSA regulations do ''. . . not permit a bank to exempt its transactions with nonbank financial institutions (except for check cashing services licensed by state or local government and the United States Postal Service). . . .'' 31 C.F.R. 103.22(c). Any business which sells more than $150,000 worth of money orders or traveler's checks within any given 30-day period is defined to be a ''financial institution.'' 31 CFR 103.11 (i)(4).

In view of this, and the fact that illegally obtained funds are frequently laundered through purchases of money orders and other monetary instruments, Treasury's policy has been that banks could not exempt accounts of retail businesses into which retail receipts and money order sale proceeds are commingled. However, Treasury recognizes that many operators of retail businesses, especially grocery, discount and convenience stores sell money orders as an incidental service to their customers and that the majority of these sales are for legitimate purposes.

Provided that the Bank monitors the accounts to detect unusual activity and reports suspicious transactions law enforcement's concerns are satisfied. Provided also that money order sales do not exceed $150,000 in any 30-day period defined as any calendar month (e.g. January 1–31; February 1–28/29; June 1–30). and that retail proceeds account for more than 50% of a business' gross revenues, such a business is not a financial institution as defined in the BSA regulations. To withhold exemption authority and to require routine CTR reporting in such a situation is burdensome to banks and could well produce information of little value to law enforcement.

Therefore, Treasury will consider on a case-by-base basis, requests from banks for special exemption authorization to exempt accounts of retail stores in which money order receipts are commingled with retail proceeds under the following conditions. First, the Bank must verify that the business is not a nonbank financial institution by taking the following steps. The Bank should review any records it has available to confirm that: (1) money order sale proceeds do not exceed $150,000 in any 30-day period (calendar month); (2) money order sale proceeds have never exceeded $150,000 in any 30-day period (calendar month); and retail proceeds account for more than 50% of the business' gross revenues. In the event that multiple locations deposit to a .single account, the exemption criteria should be applied to each location. In addition, the Bank must require the business to attest to both facts in its Exemption Statement.

The following examples illustrate application of the above verification provision:

Retail business with one location which commingles the location's retail and money order proceeds in one account:

The account may be considered for exemption only if a bank confirms that both the money order sale proceeds do not exceed and have never exceeded $150,000 in any 30-day period (calendar month) and the retail proceeds account for more than 50% of the business' gross revenues. If either of the thresholds is not met, the account may not be exempted.

Retail business with multiple locations which commingles the locations' retail and money order proceeds in one account:

The account may be considered for exemption only if a bank confirms that the money order sale proceeds do not exceed and have never exceeded $150,000 in any 30-day period (calendar month) and the retail proceeds account for more than 50% of the business' gross rev-

enues for each location. If either of the thresholds is exceeded by any location, the account may not be exempted.

Retail business which deposits retail and money order proceeds in separate accounts.

The separate money order account is never exemptible, irrespective of whether or not the business' money order sale proceeds are less than or exceed $150,000 in any 30 day period (calendar month). The retail proceeds account may be considered for exemption only if retail proceeds account for more than 50% of the business' gross revenues.

After an account has been exempted, the Bank must monitor the account and request that the business notify.it immediately should any of the above conditions change. If any of the thresholds are exceeded, the exemption must be suspended immediately. As set forth in the *Exemption Handbook*, Treasury recommends that the Bank review this exemption at least once a year, preferably every six months. At the time of the review, the Bank shall again ensure that money order sale proceeds have not and have never exceeded $150,000 in any 30-day period (calendar month) and retail proceeds still account for more than 50% of the gross revenues. The Bank must require that a depositor renew its attestations by signing a now Exemption Statement. Beyond the foregoing special requirements, the Bank must comply with all other exemption requirements as described in Treasury's *Exemption Handbook.*

This authority is limited to the customers and account numbers[s] identified in a bank's request and continues in effect only until otherwise directed by Treasury through any subsequent applicable regulation or Administrative Ruling which address this issue. Please be advised that should a bank become aware of any accounts of retail businesses that also sell money orders and are currently exempted, the Bank must make separate application to Treasury for exemption within 60 days. However, the exemption need not be revoked. If the account is not exempted, until such time as special exemption authority is granted, the Bank must report all currency transactions in excess of $10,000. Applications for special exemptions of such accounts must be made to the Director, Office of Financial Enforcement (Room 5000, Annex), Department of the Treasury, 1500 Pennsylvania Avenue N.W., Washington, D.C. 20220.

With respect to retail businesses which sell lottery tickets and traveler's checks and/or money orders, a bank may request additional authority to exempt the account. Authority to exempt such a business' account will be granted under the same conditions described above provided that the retail proceeds account for more than 50% of the business' gross revenues.

SR 95-10 (FIS)

TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK

SUBJECT: Payable Through Accounts

BACKGROUND

Over the past year, Board staff has become aware of the increasing use of an account service known as a ''payable through account'' that is being marketed by U.S. banks, Edge corporations and the U.S. branches and agencies of foreign banks (''U.S. banking entity(ies)'') to foreign banks that otherwise would not have the ability to offer their customers direct access to the U.S. banking system. This account service has also been referred to by other names, such as ''pass through accounts'' and ''pass by accounts.'' We have worked with representatives from the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision to monitor payable through account activities and to ensure that all banking organizations supervised by the Federal Reserve and the other agencies are advised about the matters described below.

The payable through account mechanism has long been used in the United States by credit unions (*e.g.*, for checking account services) and investment companies (*e.g.*, for checking account services associated with money market management accounts) to offer their respective customers the full range of banking services that only a commercial bank has the ability to provide. The problems described below do not relate to these traditional uses of payable through account relationships.

EXPLANATION OF ''PAYABLE THROUGH ACCOUNTS''

The recent use of payable through accounts as an account service being offered by U.S. banking entities to foreign banks involves the U.S. banking entity opening a checking account for the foreign bank. The foreign bank then solicits customers that reside outside of the United States who, for a fee, are provided with the means to conduct banking transactions in the United States through the foreign bank's account at the U.S. banking entity. Typically, the foreign bank will provide its customers, commonly referred to as ''sub-account holders,'' with checks that enable the sub-account holder to draw on the foreign bank's account at the U.S. banking entity. The group of sub-account holders, which may number several hundred for one payable through account, all become signatories on the foreign bank's account at the U.S. banking entity.[1] This results in individuals and businesses, who may not have been subject to the same requirements imposed on U.S. citizens or residents for opening an account at a U.S. banking entity, possessing the ability to write checks and make deposits at a U.S. banking entity, as if such individuals and businesses were the actual account holders at the U.S. banking entity.[2]

1. In a recent adaptation of the payable through account service, foreign banks have opened accounts at U.S. banking entities and then solicited other foreign banks, rather than individuals, to use their accounts at the U.S. banking entities. These second tier foreign banks then solicit individuals as customers. This has resulted in thousands, rather than hundreds, of individuals having signatory authority over a single account at a U.S. banking entity.

2. Payable through account activities should not be confused with traditional correspondent banking relationships. Under typical correspondent banking arrangements, a smaller bank will enter into an agreement with a larger bank to process and complete transactions on behalf of the smaller bank's customers or the smaller bank itself. In such an arrangement, the smaller bank's customers are not aware of the correspondent banking relationships their bank has with other financial institutions. The smaller bank's customers certainly do not have access to their bank's account at the larger correspondent bank. This differs significantly from the payable through account situations where the sub-account holders have direct control of the payable through account at the U.S. banking entity by virtue of their signatory authority over the foreign bank's account at the U.S. banking entity.

It appears that some U.S. banking entities are not exercising the same degree of care with respect to payable through accounts that they exercise for domestic customers that want to open checking or other types of account relationships directly with the banking organizations. Our experience has shown that some U.S. banking entities simply collect signature cards that have been completed abroad and have been submitted to them in bulk by the foreign banks, and then proceed to process thousands of checks issued by the sub-account holders, as well as other banking transactions, through the foreign banks' accounts at the U.S. banking entities. These U.S. banking entities undertake little or no effort independently to obtain or verify information about the individuals and businesses who use their accounts.

POSSIBLE ILLEGAL OR IMPROPER CONDUCT ASSOCIATED WITH PAYABLE THROUGH ACCOUNTS

The traditional use of payable through accounts by financial organizations in the United States (*i.e.,* credit unions and investment companies) has not been a cause for concern by bank regulators. These organizations are regulated by federal or state agencies, or are otherwise subject to established industry standards; and they appear to have adopted adequate policies and procedures to establish the identity of, and monitor the activity of, sub-account holders—in essence the credit union's depositors or the investment company's mutual fund account holders. The same types of safeguards do not appear to be present in some U.S. banking entities that provide payable through account services to foreign banks.

Board staff is concerned that the use of payable through accounts by foreign banks at U.S. banking entities may facilitate unsafe and unsound banking practices and other misconduct, including money laundering and related criminal activities. Unless a U.S. banking entity is able to identify adequately, and understand the transactions of, the ultimate users—all or most of whom are off-shore—of the foreign bank's account maintained at the U.S. banking entity, there is a potential for serious illegal conduct. Recent reports from law enforcement agencies, as well as our own investigatory efforts, confirm that some money laundering and related illicit schemes have involved the use of foreign banks' payable through account arrangements at U.S. banking entities. Should accounts at U.S. banking entities be used for illegal purposes, the entities could be exposed not only to reputational risks, but also to serious risks of financial losses as a result of asset seizures and forfeitures brought by law enforcement authorities.

GUIDELINES ON PAYABLE THROUGH ACCOUNT ACTIVITIES

Because of the possibility of illicit activities being conducted through payable through accounts at U.S. banking entities, we believe that it is inconsistent with the principles of safe and sound banking for U.S. 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.

These policies and procedures must be fashioned to enable each U.S. banking entity offering payable through account services to foreign banks to identify sufficiently the ultimate users of its foreign bank customers' payable through accounts, including obtaining (or having the ability to obtain) in the United States substantially the same type of information on the ultimate users as the U.S. banking entity obtains for its domestic customers. This may require a review of the foreign bank's own procedures for identifying and monitoring sub-account holders, as well as the relevant statutory and regulatory requirements placed on the foreign bank to identify and monitor the transactions of its own customers by its home country supervisory authorities. In addition, U.S. banking entities should have procedures whereby they monitor account activities conducted in their payable through accounts with foreign banks and report suspicious or unusual activity in accordance with applicable Federal Reserve criminal referral regulations.

In those situations where (1) adequate information about the ultimate users of the payable through accounts cannot be obtained; (2) the U.S. banking entity cannot adequately rely on

the home country supervisor to require the foreign bank to identify and monitor the transactions of its own customers; or (3) the U.S. banking entity is unable to ensure that its payable through accounts are not being used for money laundering or other illicit purposes, it is recommended that the U.S. banking entity terminate the payable through arrangement with the foreign bank as expeditiously as possible.

NOTICE TO U.S. BANKING ENTITIES AND NEW EXAMINATION PROCEDURES

Because of the existing and potential problems associated with payable through accounts, we are asking that U.S. banking entities immediately begin to establish and maintain policies and procedures designed to guard against the possible improper or illegal use of their payable through account facilities, and that your Reserve Bank start to review such activities during the course of future examinations. To assist the banking organizations in your District with their understanding of our concerns in this area, we have attached a suggested letter to disseminate our payable through account guidelines to the state member banks, Edge corporations, and U.S. branches and agencies of foreign banks in your District. We have also developed new examination procedures that should be used by your examination staff to review payable through account activities. The new examination procedures will be sent to you under separate cover shortly.

After your Reserve Bank disseminates the attached suggested letter and begins to use the new payable through account examination procedures, we ask that, for the next six months, your examiners concentrate on reviewing U.S. banking entities' existing policies and procedures related to monitoring payable through account activities, to the extent that the banking organizations conduct such activities, and that they make suggestions for improvements or enhancements, where appropriate, consistent with our new guidelines in this area. Because the Federal Reserve, as well as other federal bank regulators, have not previously issued any guidance regarding the operation of payable through accounts at U.S. banking entities, we request that, until September 30, 1995, you focus on improvements and enhancements at U.S. banking entities where some deficiencies in this area are discovered and not include criticisms of U.S. banking entities' payable through account activities in your reports of examination. In addition, we request that your Reserve Bank not recommend any follow-up supervisory actions related to a U.S. banking entity's policies and procedures regarding its payable through account activities until the fourth quarter of 1995, unless your examiners find apparent violations of the Bank Secrecy Act or indicia of other serious criminal misconduct associated with such activities.

COLLECTION OF DATA RELATED TO PAYABLE THROUGH ACCOUNTS

Board staff is in the process of collecting data on payable through accounts in order to determine as soon as possible the extent of such activities in the United States. In this regard, please provide the following information to Ronald J. Ranochak, Senior Financial Analyst, International Supervision Section, Mail Stop 182, as soon as such information becomes available through your upcoming examinations, contacts with U.S. banking entities following the dissemination of the attached suggested letter, or through other sources:

1. The name and location of each U.S. banking entity offering payable through accounts to foreign banks.
2. For each such banking entity, as identified above:
   a. the name, location and licensing authority of each foreign bank that maintains a payable through account, to the extent that such information is available at the U.S. banking entity;
   b. the ownership structure data on each foreign bank, to the extent that such information is available at the U.S. banking entity; and
   c. the number of sub-account holders in each payable through account, including the name and number of foreign banks that are sub- account holders.

In the event that you have any questions concerning any of the matters described herein,

please contact Richard A. Small, Special Counsel, at (202) 452-5235, or Daniel D. Soto, Senior Special Examiner, at (202) 728-5829. For questions related to the collection of data on payable through accounts, Mr. Ranochak can be reached at (202) 452-5275.

Richard Spillenkothen
Director

Attachment

SUGGESTED LETTER

TO THE CHIEF EXECUTIVE OFFICER OF EACH STATE MEMBER BANK, EDGE CORPORATION, AND U.S. BRANCH AND AGENCY OF A FOREIGN BANK

SUBJECT: PAYABLE THROUGH ACCOUNTS

DEAR _____ :

Over the past year, the Federal Reserve has become aware of the increasing use of an account service known as a ''payable through account'' that is being marketed by U.S. banks, Edge corporations and the U.S. branches and agencies of foreign banks (''U.S. banking entity(ies)'') to foreign banks that otherwise would not have the ability to offer their customers access to the U.S. banking system. This account service has also been referred to by other names, such as ''pass through accounts'' and ''pass by accounts.'' We have worked with representatives from the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision to monitor payable through account activities and to ensure that all banking organizations supervised by the Federal Reserve and the other agencies are advised about the matters described below.

The payable through account mechanism has long been used in the United States by credit unions (*e.g.*, for checking account services) and investment companies (*e.g.*, for checking account services associated with money market management accounts) to offer their respective customers the full range of banking services that only a commercial bank has the ability to provide. The problems described below do not relate to these traditional uses of payable through account relationships.

EXPLANATION OF ''PAYABLE THROUGH ACCOUNTS''

The recent use of payable through accounts as an account service being offered by U.S. banking entities to foreign banks involves the U.S. banking entity opening a checking account for the foreign bank. The foreign bank then solicits customers that reside outside of the United States who, for a fee, are provided with the means to conduct banking transactions in the United States through the foreign bank's account at the U.S. banking entity. Typically, the foreign bank will provide its customers, commonly referred to as ''sub-account holders,'' with checks that enable the sub-account holder to draw on the foreign bank's account at the U.S. banking entity. The group of sub-account holders, which may number several hundred for one payable through account, all become signatories on the foreign bank's account at the U.S. banking entity.[1] This results in individuals and businesses, who may not have been subject to the same requirements imposed on U.S. citizens or residents for opening an account at a U.S. banking entity, possessing the ability to write checks and make deposits at a U.S. banking entity, as if such individuals and businesses were the actual account holders at the U.S. banking entity.[2]

It appears that some U.S. banking entities are not exercising the same degree of care with respect to payable through accounts that they exercise for domestic customers that want to open checking or other types of account relationships directly with the banking organizations. Our experience has shown that some U.S. banking entities simply collect signature cards that have been completed abroad and have been submitted to them in bulk by the foreign banks,

1. In a recent adaptation of the payable through account service, foreign banks have opened accounts at U.S. banking entities and then solicited other foreign banks, rather than individuals, to use their accounts at the U.S. banking entities. These second tier foreign banks then solicit individuals as customers. This has resulted in thousands, rather than hundreds, of individuals having signatory authority over a single account at a U.S. banking entity.

2. Payable through account activities should not be confused with traditional correspondent banking relationships. Under typical correspondent banking arrangements, a smaller bank will enter into an agreement with a larger bank to process and complete transactions on behalf of the smaller bank's customers or the smaller bank itself. In such an arrangement, the smaller bank's customers are not aware of the correspondent banking relationships their bank has with other financial institutions. The smaller bank's customers certainly do not have access to their bank's account at the larger correspondent bank. This differs significantly from the payable through account situations where the sub-account holders have direct control of the payable through account at the U.S. banking entity by virtue of their signatory authority over the foreign bank's account at the U.S. banking entity.

and then proceed to process thousands of checks issued by the sub-account holders, as well as other banking transactions, through the foreign banks' accounts at the U.S. banking entities. These U.S. banking entities undertake little or no effort independently to obtain or verify information about the individuals and businesses who use their accounts.

POSSIBLE ILLEGAL OR IMPROPER CONDUCT ASSOCIATED WITH PAYABLE THROUGH ACCOUNTS

The traditional use of payable through accounts by financial organizations in the United States (*i.e.,* credit unions and investment companies) has not been a cause for concern by bank regulators. These organizations are regulated by federal or state agencies, or are otherwise subject to established industry standards; and they appear to have adopted adequate policies and procedures to establish the identity of, and monitor the activity of, sub-account holders—in essence the credit union's depositors or the investment company's mutual fund account holders. The same types of safeguards do not appear to be present in some U.S. banking entities that provide payable through account services to foreign banks.

Federal Reserve staff is concerned that the use of payable through accounts by foreign banks at U.S. banking entities may facilitate unsafe and unsound banking practices and other misconduct, including money laundering and related criminal activities. Unless a U.S. banking entity is able to identify adequately, and understand the transactions of, the ultimate users—all or most of whom are off-shore—of the foreign bank's account maintained at the U.S. banking entity, there is a potential for serious illegal conduct. Recent reports from law enforcement agencies, as well as the Federal Reserve's own investigatory efforts, confirm that some money laundering and related illicit schemes have involved the use of foreign banks' payable through account arrangements at U.S. banking entities. Should accounts at U.S. banking entities be used for illegal purposes, the entities could be exposed not only to reputational risks, but also to serious risks of financial losses as a result of asset seizures and forfeitures brought by law enforcement authorities.

GUIDELINES ON PAYABLE THROUGH ACCOUNT ACTIVITIES

Because of the possibility of illicit activities being conducted through payable through accounts at U.S. banking entities, we believe that it is inconsistent with the principles of safe and sound banking for U.S. 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.

These policies and procedures must be fashioned to enable each U.S. banking entity offering payable through account services to foreign banks to identify sufficiently the ultimate users of its foreign bank customers' payable through accounts, including obtaining (or having the ability to obtain) in the United States substantially the same type of information on the ultimate users as the U. S. banking entity obtains for its domestic customers. This may require a review of the foreign bank's own procedures for identifying and monitoring sub-account holders, as well as the relevant statutory and regulatory requirements placed on the foreign bank to identify and monitor the transactions of its own customers by its home country supervisory authorities. In addition, U.S. banking entities should have procedures whereby they monitor account activities conducted in their payable through accounts with foreign banks and report suspicious or unusual activity in accordance with applicable Federal Reserve criminal referral regulations.

In those situations where (1) adequate information about the ultimate users of the payable through accounts cannot be obtained; (2) the U.S. banking entity cannot adequately rely on the home country supervisor to require the foreign bank to identify and monitor the transactions of its own customers; or (3) the U.S. banking entity is unable to ensure that its payable through accounts are not being used for money laundering or other illicit purposes, it is recommended that the U.S. banking entity terminate the payable through arrangement with the foreign bank as expeditiously as possible.

Even though we are asking that you begin immediately to establish and maintain policies

and procedures designed to guard against the possible improper or illegal use of payable through account facilities, we understand that such new policies and procedures will take some time to implement fully. As a first step, you should contact each foreign bank that maintains any type of payable through account relationship with your banking organization in order to bring the records related to its accounts into conformity with the aforementioned guidelines.

Over the next several months, during our regular examinations, Reserve Bank examiners will be reviewing your existing policies and procedures related to payable through account activities, to the extent that you conduct such activities, any improvements or enhancements that you may make in light of the aforementioned guidelines, and your efforts, if needed, to contact foreign banks that maintain payable through accounts at your institution.

In order to provide your banking organization with sufficient time to implement our guidelines in this area, our examiners will not include criticisms of any U.S. banking entity's payable through account activities in reports of examinations until the fourth quarter of 1995. Also, we will not recommend any follow-up supervisory actions addressing deficiencies in this area until the fourth quarter of 1995, except in those situations where examiners find apparent violations of the Bank Secrecy Act or indicia of other serious criminal misconduct associated with such activities.

Should you have any questions with regard to this matter, please contact _____ at the Reserve Bank.

Sincerely,

SR 97-19 (SUP)

June 30, 1997

TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK

SUBJECT: Private Banking Activities

Private banking activities, which involve, among other things, personalized services such as money management, financial advice, and investment services for high net worth clients, have become an increasingly important aspect of the operations of some large, internationally active banking organizations. The Federal Reserve has traditionally reviewed private banking activities in connection with regular on-site examinations. In 1996 and 1997, the Federal Reserve Bank of New York undertook a comprehensive review of private banking activities at approximately 40 domestic and foreign banking organizations in the Second District in order to enhance the Federal Reserve's understanding about private banking operations. Examiners focused principally on assessing each institution's ability to recognize and manage the potential reputational and legal risks that may be associated with inadequate knowledge and understanding of its clients' personal and business backgrounds, sources of wealth, and uses of private banking accounts. In carrying out the reviews, examiners considered the parameters of an appropriate control infrastructure that is suited to support the effective management of these risks.

The reviews indicated that there are certain essential elements associated with sound private banking activities, and these elements are described in a paper, prepared by the Federal Reserve Bank of New York, entitled ''Guidance on Sound Risk Management Practices Governing Private Banking Activities.'' A copy of the sound practices paper is attached for the use of your examiners, and we are requesting that you provide copies to each domestic and foreign banking organization in your District that conducts private banking activities.[1] A suggested transmittal letter is also attached.

The sound practices paper provides banking organizations with guidance regarding the basic controls necessary to minimize reputational and legal risk and to deter illicit activities, such as money laundering. The essential elements associated with sound private banking activities are, in brief outline, as follows:

- *Management Oversight.* Senior management's active oversight of private banking activities and the creation of an appropriate corporate culture are crucial elements of a sound risk management and control environment. Goals and objectives must be set at high levels, and senior management must be proactive in overseeing compliance with corporate policies and procedures.

- *Policies and Procedures.* All well run private banking operations have written ''Know Your Customer'' policies and procedures, consistent with guidance provided by the Federal Reserve over the past several years, that require banking organizations to obtain identification and basic background information on their clients, describe the clients' source of wealth and lines of business, request references, handle referrals, and identify red flags and suspicious transactions. They also have adequate written credit policies and procedures that address, among other things, money laundering-related issues, such as lending secured by cash collateral.

- *Risk Management Practices and Monitoring Systems.* Sound private banking operations stress the importance of the acquisition and retention of documentation relating to their clients, as well as due diligence regarding obtaining follow-up information where needed to verify or corroborate information provided

1. See section 1301 of the BSA manual.

by a customer or his or her representative. Inherent in sound private banking operations is the retention of beneficial owner information in the United States for accounts opened by financial advisors or through the use of off-shore facilities. Adequate management information systems capable of, among other things, monitoring all aspects of an organization's private banking activities are also stressed. These include systems that provide management with timely information necessary to analyze and effectively manage the private banking business and systems that enable management to monitor accounts for suspicious transactions and to report any such instances to law enforcement authorities and banking regulators as required by the regulators' suspicious activity reporting regulations.

- *Segregation of Duties, Compliance, and Audit.* Because private banking activities are generally conducted through relationship managers, banking organizations need to have an effective system of oversight by senior officials and by board committees, as well as guidelines pertaining to the segregation of duties to prevent the unauthorized waiver of documentation requirements, poorly documented referrals, and overlooked suspicious activities. Likewise, strong compliance and internal audit programs are essential to ensure the integrity of the risk management and internal control environment established by senior management and the board of directors.

OTHER RELATED PROJECTS AND PRODUCTS

The lessons learned from the private banking reviews will be incorporated into a new examination manual for private banking activities. The manual will be in two parts: one which describes the examination procedures for a comprehensive, top to bottom review of a private banking operation; and the other, a set of ''risk focused'' guidelines aimed at assisting examiners in determining which procedures should be followed depending, for example, on the level of private banking activity, any noted deficiencies, management's responsiveness in implementing corrective action, and the sufficiency of the organization's internal audit program. We expect to start field testing these new procedures within the next three months.

In the next few weeks, the Federal Reserve will also distribute an updated Bank Secrecy Act examination manual. The updated version will include examination procedures relating to recent additions and changes to the Bank Secrecy Act, as well as updated sections related to anti-money laundering initiatives.

Staff is in the process of developing a draft regulation that would require banking organizations to establish ''Know Your Customer'' policies and procedures. The results of the private banking reviews will be incorporated into the proposed regulation. In moving forward with this initiative, the Federal Reserve will coordinate its efforts with the other federal banking agencies regarding the breadth and scope of the rules in order to ensure that all banking organizations in the United States operate under the same standards.

In the event you have any questions regarding the attached sound practices paper, please contact Ms. Nancy Bercovici, Senior Vice President, Federal Reserve Bank of New York, at (212) 720-8227, or Mr. Richard A. Small, Special Counsel, Division of Banking Supervision and Regulation, at (202) 452-5235. Other questions can be directed to Mr. Small.

Richard Spillenkothen
Director

ATTACHMENTS TRANSMITTED ELECTRONICALLY BELOW

SUGGESTED LETTER

TO THE CHIEF EXECUTIVE OFFICER OR GENERAL MANAGER
OF EACH STATE MEMBER BANK, BANK HOLDING COMPANY, AND
U.S. BRANCH AND AGENCY OF A FOREIGN BANK
THAT CONDUCTS PRIVATE BANKING ACTIVITIES

SUBJECT: ''SOUND PRACTICES'' FOR PRIVATE BANKING ACTIVITIES

DEAR _____ :

Private banking activities, which involve, among other things, personalized services such as money management, financial advice, and investment services for high net worth clients, have become an increasingly important aspect of the operations of some large, internationally active banking organizations. The Federal Reserve has traditionally reviewed private banking activities in connection with regular on-site examinations. In 1996 and 1997, the Federal Reserve Bank of New York undertook a comprehensive review of private banking activities at approximately 40 domestic and foreign banking organizations in the Second District in order to enhance the Federal Reserve's understanding about private banking operations. Examiners focused principally on assessing each institution's ability to recognize and manage the potential reputational and legal risks that may be associated with inadequate knowledge and understanding of its clients' personal and business backgrounds, sources of wealth, and uses of private banking accounts. In carrying out the reviews, examiners considered the parameters of an appropriate control infrastructure that is suited to support the effective management of these risks.

The reviews indicated that there are certain essential elements associated with sound private banking activities, and these elements are described in a paper, prepared by the Federal Reserve Bank of New York, entitled ''Guidance on Sound Risk Management Practices Governing Private Banking Activities.'' A copy of the sound practices paper is attached for your information.

The sound practices paper provides you with guidance regarding the basic controls necessary to minimize reputational and legal risk and to deter illicit activities, such as money laundering. The essential elements associated with sound private banking activities are, in brief outline, as follows:

- *Management Oversight.* Senior management's active oversight of private banking activities and the creation of an appropriate corporate culture are crucial elements of a sound risk management and control environment. Goals and objectives must be set at high levels, and senior management must be proactive in overseeing compliance with corporate policies and procedures.

- *Policies and Procedures.* All well run private banking operations have written ''Know Your Customer'' policies and procedures, consistent with guidance provided by the Federal Reserve over the past several years, that require banking organizations to obtain identification and basic background information on their clients, describe the clients' source of wealth and lines of business, request references, handle referrals, and identify red flags and suspicious transactions. They also have adequate written credit policies and procedures that address, among other things, money laundering-related issues, such as lending secured by cash collateral.

- *Risk Management Practices and Monitoring Systems.* Sound private banking operations stress the importance of the acquisition and retention of documentation relating to their clients, as well as due diligence regarding obtaining follow-up information where needed to verify or corroborate information provided by a customer or his or her representative. Inherent in sound private banking operations is the retention of beneficial owner information in the United States for accounts opened by financial advisors or through the use of off-shore facilities. Adequate management information systems capable of, among other things, monitoring all aspects of an organization's private banking activities are also stressed. These include systems that provide management with timely information necessary to analyze and effectively manage the private banking business and systems that

enable management to monitor accounts for suspicious transactions and to report any such instances to law enforcement authorities and banking regulators as required by the regulators' suspicious activity reporting regulations.

- *Segregation of Duties, Compliance, and Audit.* Because private banking activities are generally conducted through relationship managers, banking organizations need to have an effective system of oversight by senior officials and by board committees, as well as guidelines pertaining to the segregation of duties to prevent the unauthorized waiver of documentation requirements, poorly documented referrals, and overlooked suspicious activities. Likewise, strong compliance and internal audit programs are essential to ensure the integrity of the risk management and internal control environment established by senior management and the board of directors.

In the event you have any questions regarding the attached sound practices paper, please contact Ms. Nancy Bercovici, Senior Vice President, Federal Reserve Bank of New York, at (212) 720-8227, or Mr. Richard A. Small, Special Counsel, Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System, at (202) 452-5235.

Sincerely,

Enclosure

Basle Committee Statement of Principles
Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering

Section 1501.0

PREAMBLE

1. Banks and other financial institutions may be unwittingly used as intermediaries for the transfer or deposit of funds derived from criminal activity. Criminals and their associates use the financial system to make payments and transfers of funds from one account to another; to hide the source and beneficial ownership of money; and to provide storage for bank-notes through a safe-deposit facility. These activities are commonly referred to as money-laundering.
2. Efforts undertaken hitherto with the objective of preventing the banking system from being used in this way have largely been undertaken by judicial and regulatory agencies at a national level. However, the increasing international dimension of organized criminal activity, notably in relation to the narcotics trade, has prompted collaborative initiatives at the international level. One of the earliest such initiatives was undertaken by the Committee of Ministers of the Council of Europe in June 1980. In its report[1] the Committee of Ministers concluded that ''. . . the banking system can play a highly effective preventative role while the cooperation of the banks also assists in the repression of such criminal acts by the judicial authorities and the police''. In recent years the issue of how to prevent criminals laundering the proceeds of crime through the financial system has attracted increasing attention from legislative authorities, law enforcement agencies and banking supervisors in a number of countries.
3. The various national banking supervisory authorities represented on the Basle Committee on Banking Regulations and Supervisory Practices[2] do not have the same roles and responsibilities in relation to the suppression of money-laundering. In some countries supervisors have a specific responsibility in this field; in others they may have no direct responsibility. This reflects the role of banking supervision, the primary function of which is to maintain the overall financial stability and soundness of banks rather than to ensure that individual transactions conducted by bank customers are legitimate. Nevertheless, despite the limits in some countries on their specific responsibility, all members of the Committee firmly believe that supervisors cannot be indifferent to the use made of banks by criminals.
4. Public confidence in banks, and hence their stability, can be undermined by adverse publicity as a result of inadvertent association by banks with criminals. In addition, banks may lay themselves open to direct losses from fraud, either through negligence in screening undesirable customers or where the integrity of their own officers has been undermined through association with criminals. For these reasons the members of the Basle Committee consider that banking supervisors have a general role to encourage ethical standards of professional conduct among banks and other financial institutions.
5. The Committee believes that one way to promote this objective, consistent with differences in national supervisory practice, is to obtain international agreement to a Statement of Principles to which financial institutions should be expected to adhere.
6. The attached Statement is a general statement of ethical principles which encourage banks' management to put in place effective procedures to ensure that all persons conducting business with their institutions are properly identified; that transactions that do not appear legitimate are discouraged; and that cooperation with law enforcement agencies is achieved. The Statement is not a legal document and its implementation will depend on national practice and law. In particular, it should be noted that in some countries banks may be subject to additional more stringent legal regulations in this field and the Statement is not intended to replace or diminish those requirements. Whatever the legal position in different countries, the Committee

1. Measures against the transfer and safeguarding of funds of criminal origin. Recommendation No. R(80)10 adopted by the Committee of Ministers of the Council of Europe on 27th June 1980.

2. The Committee comprises representatives of the central banks and supervisory authorities of the following countries: Belgium, Canada, France, Germany, Italy, Japan, Netherlands, Sweden, Switzerland, United Kingdom, United States, and Luxembourg.

considers that the first and most important safeguard against money-laundering is the integrity of banks' own managements and their vigilant determination to prevent their institutions becoming associated with criminals or being used as a channel for money-laundering. The Statement is intended to reinforce those standards of conduct.

7. The supervisory authorities represented on the Committee support the principles set out in the Statement. To the extent that these matters fall within the competence of supervisory authorities in different member countries, the authorities will recommend and encourage all banks to adopt policies and practices consistent with the Statement. With a view to its acceptance worldwide, the Committee would also recommend the Statement to Supervisory authorities in other countries.

Basle, December 1988

STATEMENT OF PRINCIPLES

I. Purpose

Banks and other financial institutions may unwittingly be used as intermediaries for the transfer or deposit of money derived from criminal activity. The intention behind such transactions is often to hide the beneficial ownership of funds. The use of the financial system in this way is of direct concern to police and other law enforcement agencies; it is also a matter of concern to banking supervisors and banks' managements, since public confidence in banks may be undermined through their association with criminals.

This Statement of Principles is intended to outline some basic policies and procedures that banks' managements should ensure are in place within their institutions with a view to assisting in the suppression of money-laundering through the banking system, national and international. The Statement thus sets out to reinforce existing best practices among banks and, specifically, to encourage vigilance against criminal use of the payments system, implementation by banks of effective preventive safeguard, and cooperation with law enforcement agencies.

II. Customer Identification

With a view to ensuring that the financial system is not used as a channel for criminal funds, banks should make reasonable efforts to determine the true identity for all customers requesting the institution's services. Particular care should be taken to identify the ownership of all accounts and those using safe-custody facilities. All banks should institute effective procedures for obtaining identification from new customers. It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity.

III. Compliance with Laws

Banks' management should ensure that business is conducted in conformity with high ethical standards and that laws and regulations pertaining to financial transactions are adhered to. As regards transactions executed on behalf of customers, it is accepted that banks may also have no means of knowing whether the transaction stems from or forms part of criminal activity. Similarly, in an international context it may be difficult to ensure that cross-border transactions on behalf of customers are in compliance with the regulations of another country. Nevertheless, banks should not set out to offer services or provide active assistance in transactions which they have good reason to suppose are associated with money-laundering activities.

IV. Cooperation with Law Enforcement Authorities

Banks should cooperate fully with national law enforcement authorities to the extent permitted by specific local regulations relating to customer confidentiality. Care should be taken to avoid providing support or assistance to customers seeking to deceive law enforcement agencies through the provision of altered, incomplete or misleading information. Where banks become aware of facts which lead to the reasonable presumption that money held on deposit derives from criminal activity or that transactions entered into are themselves criminal in purpose, appropriate measures, consistent with the law, should be taken, for example, to deny assistance,

sever relations with the customer and close or freeze accounts.

V. Adherence to the Statement

All banks should formally adopt policies consistent with the principles set out in this Statement and should ensure that all members of their staff concerned, wherever located, are informed of the bank's policy in this regard. Attention should be given to staff training in matters covered by the Statement. To promote adherence to these principles, banks should implement specific procedures for customer identification and for retaining internal records of transactions. Arrangements for internal audit may need to be extended in order to establish an effective means of testing for general compliance with the Statement.

INTRODUCTION

1. The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering—the processing of criminal proceeds in order to disguise their illegal origin. These policies aim to prevent such proceeds from being utilized in future criminal activities and from affecting legitimate economic activities.
2. The FATF currently consists of 26 countries[1] and two international organizations.[2] Its membership includes the major financial center countries of Europe, North America and Asia. It is a multi-disciplinary body—as is essential in dealing with money laundering—bringing together the policy-making power of legal, financial and law enforcement experts.
3. This need to cover all relevant aspects of the fight against money laundering is reflected in the scope of the forty FATF Recommendations—the measures which the Task Force have agreed to implement and which all countries are encouraged to adopt. The Recommendations were originally drawn up in 1990. In 1996 the forty Recommendations were revised to take into account the experience gained over the last six years and to reflect the changes which have occurred in the money laundering problem.[3]
4. These forty Recommendations set out the basic framework for anti-money laundering efforts and they are designed to be of universal application. They cover the criminal justice system and law enforcement; the financial system and its regulation, and international cooperation.
5. It was recognized from the outset of the FATF that countries have diverse legal and financial systems and so all cannot take identical measures. The Recommendations are therefore the principles for action in this field, for countries to implement according to their particular circumstances and constitutional frameworks allowing countries a measure of flexibility rather than prescribing every detail. The measures are not particularly complex or difficult, provided there is the political will to act. Nor do they compromise the freedom to engage in legitimate transactions or threaten economic development.
6. FATF countries are clearly committed to accept the discipline of being subjected to multilateral surveillance and peer review. All member countries have their implementation of the forty Recommendations monitored through a two-pronged approach: an annual self-assessment exercise and the more detailed mutual evaluation process under which each member country is subject to an on-site examination. In addition, the FATF carries out cross-country reviews of measures taken to implement particular Recommendations.
7. These measures are essential for the creation of an effective anti-money laundering framework.

THE FORTY RECOMMENDATIONS OF THE FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING

A. General Framework of the Recommendations

1. Each country should take immediate steps to ratify and to implement fully, the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention).
2. Financial institution secrecy laws should be conceived so as not to inhibit implementation of these recommendations.

1. Reference in this document to ''countries'' should be taken to apply equally to ''territories'' or ''jurisdictions.'' The twenty six FATF member countries and governments are: Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, the Kingdom of the Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States.

2. The two international organizations are: the European Commission and the Gulf Cooperation Council.

3. During the period 1990 to 1995, the FATF also elaborated various Interpretive Notes which are designed to clarify the application of specific Recommendations. Some of these Interpretive Notes have been updated in the Stocktaking Review to reflect changes in the Recommendations (not included in this manual).

3. An effective money laundering enforcement program should include increased multilateral co-operation and mutual legal assistance in money laundering investigations and prosecutions and extradition in money laundering cases, where possible.

B. Role of National Legal Systems in Combating Money Laundering

Scope of the Criminal Offense of Money Laundering

4. Each country should take such measures as may be necessary, including legislative ones, to enable it to criminalize money laundering as set forth in the Vienna Convention. Each country should extend the offense of drug money laundering to one based on serious offenses. Each country would determine which serious crimes would be designated as money laundering predicate offenses.
5. As provided in the Vienna Convention, the offense of money laundering should apply at least to knowing money laundering activity, including the concept that knowledge may be inferred from objective factual circumstances.
6. Where possible, corporations themselves—not only their employees—should be subject to criminal liability.

Provisional Measures and Confiscation

7. Countries should adopt measures similar to those set forth in the Vienna Convention, as may be necessary, including legislative ones, to enable their competent authorities to confiscate property laundered, proceeds from, instrumentalities used in or intended for use in the commission of any money laundering offense, or property of corresponding value, without prejudicing the rights of bona fide third parties.

   Such measures should include the authority to: 1) identify, trace and evaluate property which is subject to confiscation; 2) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; and 3) take any appropriate investigative measures.

   In addition to confiscation and criminal sanctions, countries also should consider monetary and civil penalties, and/or proceedings including civil proceedings, to void contracts entered into by parties, where parties knew or should have known that as a result of the contract, the State would be prejudiced in its ability to recover financial claims, e.g. through confiscation or collection of fines and penalties.

C. Role of the Financial System in Combating Money Laundering

8. Recommendations 10 to 29 should apply not only to banks, but also to non-bank financial institutions. Even for those non-bank financial institutions which are not subject to a formal prudential supervisory regime in all countries, for example bureaux de change, governments should ensure that these institutions are subject to the same anti-money laundering laws or regulations as all other financial institutions and that these laws or regulations are implemented effectively.
9. The appropriate national authorities should consider applying Recommendations 10 to 21 and 23 to the conduct of financial activities as a commercial undertaking by businesses or professions which are not financial institutions, where such conduct is allowed or not prohibited. Financial activities include, but are not limited to, those listed in the annex at the end of this document. It is left to each country to decide whether special situations should be defined where the application of anti-money laundering measures is not necessary, for example, when a financial activity is carried out on an occasional or limited basis.

Customer Identification and Recordkeeping Rules

10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to iden-

tify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

In order to fulfill identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

(i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

(ii) to verify that any person purporting to act on behalf of the customer is so authorized and identify that person.

11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).
12. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

    Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

    These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.
13. Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Increased Diligence of Financial Institutions

14. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established inwriting, and be available to help supervisors, auditors and law enforcement agencies.
15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.
16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.
17. Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.
18. Financial institutions reporting their suspicions should comply with instructions from the competent authorities.
19. Financial institutions should develop programs against money laundering. These programs should include, as a minimum:

    (i) the development of internal policies, procedures and controls, including the

designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;

(ii) an ongoing employee training program;

(iii) an audit function to test the system.

Measures to Cope with the Problem of Countries with No or Insufficient Anti-Money Laundering Measures

20. Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply these Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the mother institution should be informed by the financial institutions that they cannot apply these Recommendations.
21. Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

Other Measures to Avoid Money Laundering

22. Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.
23. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerized data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.
24. Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities, as a means to encourage the replacement of cash transfers.
25. Countries should take notice of the potential for abuse of shell corporations by money launderers and should consider whether additional measures are required to prevent unlawful use of such entities.

Implementation, and Role of Regulatory and other Administrative Authorities

26. The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should cooperate and lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.
27. Competent authorities should be designated to ensure an effective implementation of all these Recommendations, through administrative supervision and regulation, in other professions dealing with cash as defined by each country.
28. The competent authorities should establish guidelines which will assist financial institutions in detecting suspicious patterns of behavior by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.
29. The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates.

D. Strengthening of International Cooperation

Administrative Cooperation

Exchange of general information

30. National administrations should consider recording, at least in the aggregate, international flows of cash in whatever currency, so that estimates can be made of cash flows and reflows from various sources abroad, when this is combined with central bank information. Such information should be made available to the International Monetary Fund and the Bank for International Settlements to facilitate international studies.
31. International competent authorities, perhaps Interpol and the World Customs Organization, should be given responsibility for gathering and disseminating information to competent authorities about the latest developments in money laundering and money laundering techniques. Central banks and bank regulators could do the same on their network. National authorities in various spheres, in consultation with trade associations, could then disseminate this to financial institutions in individual countries.

Exchange of information relating to suspicious transactions

32. Each country should make efforts to improve a spontaneous or "upon request" international information exchange relating to suspicious transactions, persons and corporations involved in those transactions between competent authorities. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection.

Other Forms of Cooperation

Basis and means for co-operation in confiscation, mutual assistance and extradition

33. Countries should try to ensure, on a bilateral or multilateral basis, that different knowledge standards in national definitions—i.e. different standards concerning the intentional element of the infraction—do not affect the ability or willingness of countries to provide each other with mutual legal assistance.
34. International cooperation should be supported by a network of bilateral and multilateral agreements and arrangements based on generally shared legal concepts with the aim of providing practical measures to affect the widest possible range of mutual assistance.
35. Countries should be encouraged to ratify and implement relevant international conventions on money laundering such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

Focus of improved mutual assistance on money laundering issues

36. Cooperative investigations among countries' appropriate competent authorities should be encouraged. One valid and effective investigative technique in this respect is controlled delivery related to assets known or suspected to be the proceeds of crime. Countries are encouraged to support this technique, where possible.
37. There should be procedures for mutual assistance in criminal matters regarding the use of compulsory measures including the production of records by financial institutions and other persons, the search of persons and premises, seizure and obtaining of evidence for use in money laundering investigations and prosecutions and in related actions in foreign jurisdictions.
38. There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate proceeds or other property of corresponding value to such proceeds, based on money laundering or the crimes underlying the laundering activity. There should also be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.
39. To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in

the interests of justice in cases that are subject to prosecution in more than one country. Similarly, there should be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

40. Countries should have procedures in place to extradite, where possible, individuals charged with a money laundering offense or related offenses. With respect to its national legal system, each country should recognize money laundering as an extraditable offense. Subject to their legal frame-works, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, extraditing their nationals, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Annex to Recommendation 9: List of Financial Activities Undertaken by Business or Professions Which Are Not Financial Institutions

1. Acceptance of deposits and other repayable funds from the public.
2. Lending.[4]
3. Financial leasing.
4. Money transmission services.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques and bankers' drafts . . .).
6. Financial guarantees and commitments.
7. Trading for account of customers (spot, forward, swaps, futures, options . . .) in:
   (a) money market instruments (cheques, bills, CDs, etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of clients.
11. Life insurance and other investment related insurance.
12. Money changing.

---

4. Including inter alia
   - consumer credit
   - mortgage credit
   - factoring, with or without recourse
   - finance of commercial transactions (including forfeiting)

INTRODUCTION

The Treasury Department's Financial Crimes Enforcement Network (FinCEN) offers the following guidance to filers of the new Currency Transaction Report (CTR) Form 4789 (Rev. October 1995). This guidance is intended to answer general, basic questions about completing and filing the new CTR. It is not meant to be comprehensive and does not replace the CTR Form instructions and/or the regulations. Its development is based on questions received from the financial community by FinCEN and advice received from the Treasury Department's Bank Secrecy Act Advisory Group (BSAAG). The BSAAG, comprised of approximately 30 private (bank and non-bank) and government representatives, was established by the Treasury Department in March 1994 pursuant to the Annunzio–Wylie Anti–Money Laundering Act of 1992.

Copies of this FinCEN ''Guidance on the New CTR'' (published in September 1995) may be ordered: (1) by calling FinCEN's recording at 1-800-949-2732, or (2) via computer with a modem from the Treasury Bank Secrecy Act (BSA) Bulletin Board at 313-234-1453.

WHY CTR REVISED

The purpose of revising the CTR was to further the goal of reducing regulatory burdens on financial institutions. This CTR revision reduces the amount of information required by approximately 30 percent, which makes it the first time (in the 25-year history of the Bank Secrecy Act's requirement that CTRs be filed by financial institutions) that the form has been revised to reduce the amount of regulatory information required. The revised CTR is designed to be beneficial to both the law enforcement and financial communities because it focuses on the quality of information rather than the quantity.

Generally, the new CTR was revised to require only basic information, such as who conducted the transaction, on whose behalf it was conducted, the amount, a description of the transaction, and where it occurred. The revised CTR also lists broad categories of transactions, which were intended to make it easier to complete and analyze. It eliminates duplication of information and information that was difficult to obtain or of limited value to law enforcement.

HOW CTR USED

Information from CTRs is routinely used in a wide variety of criminal, tax, and regulatory investigations and proceedings, and prosecutions, as investigative leads, intelligence for the tracking of currency flows, corroborating information, and probative evidence. The analysis of CTR data, which is a major function of the Treasury Department's FinCEN, is a vital tool in combating money laundering. CTRs filed by financial institutions facilitate the detection of money laundering because they provide a ''paper trail'' for large cash transactions that may point to the financial side of criminal activity.

FinCEN uses its computer access to CTRs independently and in conjunction with other law enforcement agency data bases to respond to requests by law enforcement agencies for tactical reports on subjects under investigation. Also, FinCEN uses CTR data to examine and forecast the currency flow in a particular area, and it produces strategic intelligence reports containing this information for use by law enforcement in detecting money laundering and other financial crimes.

Additionally, FinCEN has developed an Artificial Intelligence system. The system reviews BSA filings in order to identify potentially suspicious activity. Each filing is matched to other filings by the same subjects and accessing the same accounts, and all transactions, accounts, and subjects of BSA filings are evaluated against standard sets of criteria developed by FinCEN's computer scientists in close consultation with FinCEN agents and analysts. The FinCEN Artificial Intelligence system links and evaluates reports of large cash transactions to identify potential money laundering. Its objective is to discover previously unknown, potential high value leads for possible investigation.

Another FinCEN program, called ''Gateway,'' provides state and local law enforcement

agencies with *direct* electronic access to all of the forms pursuant to the BSA that are on file in the IRS Detroit Computing Center. Gateway makes greater use of the information captured by the BSA and at the same time provides a coordination mechanism to agencies using the data for investigative purposes. It also saves investigative time and money because agencies do not have to rely on the resources of another agency to obtain BSA information.

WHO, WHAT, WHEN, AND WHERE

1. *Question:* Who should file the revised CTR Form 4789?

   Answer: Each financial institution identified in the regulations in 31 CFR Part 103 (other than a casino, which instead must file Form 8362 and the U.S. Postal Service for which there are separate rules), must file a revised CTR Form 4789 for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution which involves a transaction in currency totaling more than $10,000 in one business day. Multiple transactions must be treated as a single transaction if the financial institution has knowledge that: (1) they are by or on behalf of the same person, and (2) they result in either currency received (Cash In) or currency disbursed (Cash Out) by the financial institution totaling more than $10,000 in any one business day.

2. *Question:* Should the revised CTR Form 4789 be used to report suspicious activity?

   Answer: The revised CTR should NOT be filed for SUSPICIOUS TRANSACTIONS involving $10,000 or less in currency OR to note that a transaction of more than $10,000 in currency is suspicious. Any suspicious or unusual activity should be reported by a financial institution in the manner prescribed by its appropriate federal regulator or FinCEN. If a transaction is suspicious and in excess of $10,000 in currency, then both a revised CTR and the appropriate referral form must be filed.

   For banks, a new Suspicious Activity Report (SAR) Form is being prepared for distribution before the end of 1995[1] for use in reporting suspicious transactions involving $10,000 or less in currency OR to note that a transaction of more than $10,000 in currency is suspicious. Until a similar form is developed for non-bank financial institutions, they should write "SUSPICIOUS" across the top of the revised CTR.

3. *Question:* When should financial institutions begin using the revised CTR Form 4789?

   Answer: The revised CTR becomes effective on the *business day* of October 1, 1995. Filers must continue to use the current CTR Form 4789 (Rev. July 1994) for reportable transactions that occur before October 1, 1995 (business day).

4. *Question:* Where can I get usable copies of the revised CTR Form 4789?

   Answer: In September of 1995, usable copies of the revised CTR will be available from the IRS Forms Distribution Centers by calling 1-800-TAX-FORMS (1-800-829-3676). Prior to September 1995, an ADVANCE COPY of the revised CTR Form 4789 (that has been available since May 1995) could be ordered from the Internal Revenue Service (IRS) Forms Distribution Centers. This ADVANCE COPY of the revised CTR was for use by financial institutions to train employees and make other necessary changes required in order to complete and file the revised CTR, effective on the business day of October 1, 1995.

5. *Question:* May the old CTR be filed after October 1, 1995?

   Answer: FinCEN is allowing a necessary transition time until the end of December 1995 for financial institutions to start filing the new CTR. Between October 1 and December 31, 1995, paper filers will *not* be penalized for continuing to file the old CTR or the ADVANCE COPY of the new CTR, which has been available for training purposes since May 1995, while making every "good faith" effort to obtain and file the new CTR as soon as possible after October 1, 1995 (business day). This same

1. Effective April 1, 1996

policy will also apply to magnetic CTR filers. (See *Answer* to *Question #7* below.)

6. *Question:* Where can I get specifications for MAGNETIC FILING of the revised CTR?

   Answer: Requests for specifications on magnetic filing of the revised CTR should be directed to the IRS Detroit Computing Center, ATTN: CTR Magnetic Media Coordinator, P.O. Box 33604, Detroit, MI 48232-5604.

7. *Question:* The IRS Detroit Computing Center issued specifications on magnetic filing of the revised CTR during the week of June 12, 1995. It will take at least six (6) months from the time of receipt of these specifications until they are fullly installed and usable on financial institutions' systems. Is it acceptable for financial institutions to continue to file magnetically the old CTR Form 4789 (Rev. July 1994) until December 1995?

   Answer: Yes, because of the transition time necessary to file the revised CTR magnetically, financial institutions will *not* be penalized for continuing to use the old CTR while making every ''good faith'' effort to work with the IRS Detroit Computing Center to implement specifications for magnetic filing of the revised CTR. It is expected that this process should be completed at the latest by the end of December 1995. This same policy will also apply to paper CTR filers. (See *Answer* to *Question #5* above.)

8. *Question:* Where should I file the revised CTR?

   Answer: File the CTR by the 15th calendar day after the day of the transaction with the IRS Detroit Computing Center, ATTN: CTR, P.O. Box 33604, Detroit, MI 48232-5604 or with your local IRS office. Keep a copy (either paper or electronic) of each CTR for at least five years from the date filed.

Identification Requirements

9. *Question:* Is a U.S. passport acceptable identification since it does not contain an address and is not specifically listed in the regulations (31 CFR Part 103.28)?

   Answer: Yes, for purposes of completing the new CTR, a U.S. passport is considered an acceptable form of identification. Although verification of an address by official document or other means (*e.g.*, through credit bureaus) is desirable, acceptable identification may be made by an official document containing name and a photograph (preferably with address) that is normally acceptable by financial institutions as a means of identification when cashing checks for nondepositors.

10. *Question:* What is a cedular card?

    Answer: A cedular card is the term used for a personal identification card issued by foreign governments, particularly in Latin America and Spain, to citizens above a certain age (not issued to minors) and within certain categories (excluding certain classifications of citizens, *e.g.*, military).

Specific Instructions

11. *Question:* What should be included on additional sheets attached to the original CTR?

    Answer: In order for attached sheets to be clearly associated with the original CTR, it would be desirable to have as much identifying information as possible on the attached sheets, including: (1) the name of the bank filing the form and (2) the date of the transaction. At a minimum, on all attached sheets of paper to the original CTR, the financial institution should note the following: (1) the name(s) of the person(s) or organization(s) on whose behalf the transaction(s) is conducted and (2) the social security or employer identification number(s).

12. *Question:* Must a financial institution amend an incomplete old CTR after October 1, 1995, if the missing information is no longer required on the revised CTR (*e.g.*, a CTR is filed on September 28, 1995, then the financial institution discovers additional information on October 3 that should have been provided as an amendment to the old CTR; however, that information is no longer required on the new CTR)? (*Item 1a: Amends prior report.*)

Answer: Because the revised CTR requires less information, after October 1, 1995, there is no requirement to amend old CTRs when the amendment concerns information on fields that have been eliminated on the revised CTR.

13. *Question:* When should the box for ''multiple persons'' be checked? (*Item 1b: Multiple persons.*)

    Answer: Multiple person transactions are those conducted by or on behalf of two or more individuals; on behalf of two or more organizations, or on behalf of at least one individual and at least one organization. In these cases, box ''1b'' (multiple persons) should be checked.

14. *Question:* Do all holders of the account, even if they do not come to the bank, need to be put on the revised CTR as ''Person(s) on Whose Behalf Transaction(s) Is Conducted''?

    Answer: For deposits, all those who are known to benefit from the transaction must be identified on the CTR. However, if a person makes a withdrawal from a joint account, only his name needs to be listed as the beneficiary of the transaction if: (1) he states that the withdrawal is on his own behalf or the financial institution knows that the person making the withdrawal is the only beneficiary, and (2) the financial institution has no reason to believe otherwise.

15. *Question:* When should the box for ''multiple transactions'' be checked? (*Item 1c: Multiple transactions*)

    Answer: Multiple transactions are any two or more transactions which the financial institution has knowledge are conducted by or on behalf of any person during the same business day and which result in a total cash-in or cash-out of over $10,000. In these cases, box ''1c'' (multiple transactions) should be checked.

    Example: A customer places one deposit bag into the night depository at a bank on Friday night, two deposit bags on Saturday and two on Sunday; then on Monday morning, a teller processes all five deposit bags and deposit slips at the same time, but posts each individual deposit separately.

    This should be reported as a multiple transaction. However, if the customer places one bag containing the five deposits in the night depository over a weekend, and the teller processes the deposit on Monday morning, totaling the five deposits and showing a single cash-in transaction, the financial institution may report it as a single transaction so that the CTR reflects the financial institution's records.

PART I

Section A: Person(s) on Whose Behalf Transaction(s) Is Conducted

One of the major changes on the new CTR is the reversal of Sections A and B from the old CTR: ''Person(s) on Whose Behalf Transaction(s) is Conducted'' which was Section B on the old CTR is now Section A, and ''Individuals(s) Conducting Transaction(s)'' which was formerly Section A is now Section B. This was done to place a greater emphasis on all those who benefit from (the beneficiaries of) the transaction by noting that information first in Section A.

16. *Question:* Must the financial institution note whether the number provided in Item 6 is a social security number (SSN) or an employer identification number (EIN) since there is no separate configuration of spaces?

    Answer: It is not necessary to note whether the number in Item 6 is an SSN or EIN, and the revised CTR has been simplified to eliminate the separate configuration of these numbers because they may be differentiated solely on the basis of their initial numbers. IRS Service Centers assign EINs, which start with numbers not assigned to SSNs; whereas, the Social Security Administration assigns SSNs, which start with numbers not assigned to EINs.

17. *Question:* While an SSN or EIN is required on a CTR, if a CTR is filed without an SSN or EIN, should the financial institution amend the CTR if it subsequently obtains an SSN or EIN? (Items 6 and 19)

    Answer: Yes, the CTR should be amended if an SSN or EIN is subsequently obtained.

18. *Question:* Are the terms ''homemaker,'' ''retired,'' or ''unemployed'' acceptable as descriptions for occupations? (*Item 13*)

    Answer: ''Homemaker,'' ''retired,'' or ''unemployed'' are acceptable as occupation descriptions, but financial institutions should attempt to get more specific information. As a basic part of ''know your customer'' programs, financial institutions should pay particular attention to customers with such non-specific occupations who continually make large cash deposits. ''Self-employed'' is not acceptable without additional information as it is too non-specific.

Section B: Individual(s) Conducting Transaction(s) (if other than above)

19. *Question:* Instructions state that financial institutions should enter as much information as is available in Section B. Does this mean that if it is not available, then they do not have to provide it? Should the financial institution refuse to conduct the transaction if the customer refuses to provide the required information?

    Answer: The law requires financial institutions to file complete and accurate CTRs. The CTR Form 4789 indicates the only circumstances in which incomplete data is acceptable (*e.g.*, Armored Car Service, Mail Deposit or Shipment, etc.). If a financial institution elects to conduct a transaction for which it files an incomplete CTR other than for these specified circumstances, then it should attach an explanation of why the CTR is incomplete.

20. *Question:* If box ''a'' in Section B is checked for Armored Car Service, should the provider's name be inserted?

    Answer: No, the Armored Car Service provider's name does not have to be recorded on the CTR.

21. *Question:* Is box ''d'' for Multiple Transactions on the revised CTR's Part I—Section B the same as the old CTR's Part I, box 3d? If so, what is considered a ''reasonable effort'' for obtaining information when the aggregation of multiple transactions has exceeded the reporting threshold? (*Part I—Section B box d: Multiple Transactions*)

    Answer: Yes, box ''d'' in Part I—Section B of the revised CTR is the same as box 3d for Multiple Transactions in Part I of the old CTR, and should be checked to indicate that some or all of the information required in Items 15–25 is missing because the transaction being reported is a multiple transaction. A reasonable effort to obtain information for reporting multiple transactions that when aggregated exceeded the reporting threshold might include a check of bank records, telephone calls to customers, and obtaining information from tellers who handled the multiple transactions. However, if complete information is still not obtained, then box ''d'' in Part I—Section B must be checked to explain why.

PART II

Amount and Type of Transaction(s)

22. *Question:* Should ''multiple transactions'' be aggregated?

    Answer: Yes, to report multiple transactions, all the individual transactions of which the financial institution has knowledge must be aggregated, which means that debits must be added to debits, and credits must be added to credits. If the cash debits or the cash credits totals exceed $10,000 in a business day, a CTR is required. If debits and credits each exceed $10,000, they can both be reported on a single CTR. Do not mix debits and credits by off-setting one against the other; that is, do not mix cash-in transactions with cash-out transactions. Following are several examples of how to report aggregated transactions:

    Example A: The financial institution has knowledge that an individual deposits $5,000 in cash into his account and returns later in the day to deposit another $5,500 in cash into his account. Both cash-ins should be added (totaling $10,500) and reported on a CTR. Complete Section A on the individual, and enter his ID in Item 14; in Section B check box d (Multiple Transac-

tions) and box e (Conducted On Own Behalf) to explain why Section B is left blank.

Example B: An individual deposits $5,000 in cash into his personal account and returns later in the day to deposit $6,000 in cash into his employer's business account. Because the financial institution has knowledge that this individual has deposited $11,000 in one business day, it must file a CTR. Complete two Section As (one Section A on the individual, entering his ID in Item 14, and the other Section A on his employer's business account, entering N/A in Item 14); in Section B check box d (Multiple Transactions) and box e (Conducted On Own Behalf) to indicate why Section B is left blank.

Example C: An individual acting on behalf of several others, deposits and withdraws various amounts during the day. Regardless of how many visits he makes, if the financial institution has knowledge that either the debit or the credit total exceeds $10,000, a CTR must be filed. When the individual conducting the transactions does *not* benefit, complete Section B with information on him, entering his ID in Item 25, and complete separate Section As on all beneficiaries of the transactions, entering their identifications in Item 14. (If beneficiaries' identifications are not available because individuals are not present or are not applicable because beneficiaries are organizations, enter N/A in Item 14.) When the individual also benefits from the transactions, enter information on him and all other beneficiaries in separate Section As, indicating his ID and the identifications of others in Item 14, if available and applicable; in Section B check box d (Multiple Transactions) and box e (Conducted On Own Behalf) to indicate why Section B is left blank.

Example D: Two or more individuals conduct separate transactions on behalf of the same account holder (a store) in the same business day. If the financial institution has knowledge that the aggregate of the transactions exceeds $10,000, a CTR is required. Complete Section A with information on the same account holder (a store), indicating N/A for ID in Item 14, and complete separate Section Bs on the individuals who conducted the transactions but were not beneficiaries, entering their identifications in Item 25.

23. *Question:* How should trusts and other third party accounts be reported?

    Answer: If Jane Doe, the trustee of the John Smith Trust, makes a reportable deposit to the Trust Account, information on Jane Doe, the trustee, including the method used to verify her identification, must be entered in Part I, Section A. Identifying information on the John Smith Trust, who is the beneficiary of the transaction, must also be reported in a separate Section A (on the back of the CTR Form). Then check box e (Conducted On Own Behalf) to indicate why Section B is left blank. However, if the transaction is conducted for Jane Doe, the trustee, by her secretary, then in addition to identifying Jane Doe, the trustee, and the John Smith Trust, the beneficiary, in separate Section "As," report identifying information on the secretary, who actually conducted the transaction, in Part I, Section B.

24. *Question:* When an individual presents an on-us check drawn on an account of someone other than the presenter's account, which box should a reporting bank check? When an individual presents an on-us check drawn on the account of the presenter to withdraw funds from his/her own account, which box should be checked?

    Answer: When an individual presents an on-us check drawn on an account of someone other than the presenter's account, the bank should check box 32 (Negotiable Instrument(s) Cashed). When an individual presents an on-us check drawn on the account of the presenter to withdraw funds from his/her own account, box 32 could be checked or box 34 (Deposit(s)/ Withdrawal(s)) may be checked to indicate that the transaction is a withdrawal. In any case, list account numbers in Item 35 (Account Number(s) Affected).

25. *Question:* When a corporation/retail store's transaction exceeds its exempt limit, should a CTR be filed?

    Answer: Yes, if a customer's transaction(s) exceeds its exempt limit, a CTR must be

filed on the entire amount of the cash transaction, not just the difference between the amount exempted and the amount of the transaction.

26. *Question:* How should the purchase and redemption of a Certificate of Deposit (CD) be reported?

    Answer: It is preferred that box 34 (Deposit(s)/Withdrawal(s) be checked since the purchase of a CD is a deposit and the redemption is a withdrawal. However, it is also acceptable if a bank checks Item 36 (Other) and writes in CD redeemed/ purchased. In either case, enter the CD number(s) in Item 35 (Account Number(s) Affected).

27. *Question:* How should such transactions as loan and credit card payments be reported?

    Answer: Transactions such as loan and credit card payments should be indicated and described in Item 36 (Other) with account numbers affected recorded in Item 35.

28. *Question:* If a customer uses a check (*i.e.*, a negotiable instrument) to purchase $20,000 U.S. equivalent worth of foreign currency, how should the revised CTR be completed?

    Answer: If a check is used to purchase $20,000 in foreign currency, check box 36 (Other), indicate ''check cashed to purchase foreign currency,'' and complete Items 27 (Cash Out-Amount) and 29 (Foreign Currency). It would also be considered acceptable to check Item 32 (Negotiable Instrument Cashed) because the check is a negotiable instrument and complete Items 27 and 29.

PART III

Financial Institution Where Transaction(s) Takes Place

29. *Question:* Should dashes be used in recording the depository institution's Magnetic Ink Character Recognition MCR) number? (Item 43)

    Answer: No, dashes should not be inserted in recording of the MICR number in Item 43.

30. *Question:* May the preparer and the approver of the new CTR be the same person?

    Answer: Yes, the preparer and the approving official of the new CTR may be the same person. This is a change in policy based on standardizing paper filing with magnetic filing of the CTR. However, it is still strongly recommended that financial institutions, as a matter of internal review of CTRs, have two people involved.

31. *Question:* Must the signature of the approving official be an original, or may it be pre-printed? (Item 45)

    Answer: The signature of the approving official in Item 45 must be an original signature; it may not be pre-printed.

32. *Question:* May a department's name be pre-printed instead of the name of a person to contact? (Item 48)

    Answer: The name of a person to contact for questions about the CTR (not a department's name) is preferred in Item 48; however, the name of the compliance office or other designated department would be acceptable.

The following staff interpretive guidance addresses frequently asked questions about the new recordkeeping rules for funds transfers and transmittals of funds, which were issued under the Bank Secrecy Act by the Federal Reserve Board and the Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury.

The new requirements become effective on May 28.

This guidance is not meant to be comprehensive and does not replace or supersede the terms of the rule itself.

SECTION 103.11—MEANING OF TERMS

1. *Question:* ***Beneficiary, Beneficiary's Bank.*** Which parties are the beneficiary's bank and the beneficiary with respect to a funds transfer in which payment is made to a customer of a foreign bank?

   Answer: The foreign bank receiving a payment order for payment to its customer is the beneficiary's bank. The foreign bank's customer is the beneficiary.

2. *Question:* ***Beneficiary, Beneficiary's Bank, Recipient, Recipient's Financial Institution, Intermediary Financial Institution.*** Which parties are the beneficiary, the beneficiary's bank, the recipient's financial institution, and the recipient when funds are received by a bank for credit to an account of a licensed transmitter of funds or other person engaged in the business of transmitting funds (''money transmitter'') for further credit to the money transmitter's customer?

   Answer: The bank holding the money transmitter's account is the beneficiary's bank (and an intermediary financial institution); the money transmitter is both the recipient's financial institution and the beneficiary; the money transmitter's customer is the recipient.

3. *Question:* ***Financial Institution.*** What types of ''financial institutions'' are covered by the rule?

   Answer: The rule applies to all financial institutions subject to the Bank Secrecy Act regulations. Financial institutions, as defined in §103.11(n), include banks as well as nonbank financial institutions (NBFIs) such as securities brokers or dealers required to be registered with the SEC, currency exchange houses, casinos, and persons engaged in the business of transmitting funds. The definition of financial institution is limited to those institutions located within the United States.

   While the terms ''beneficiary's bank'' and ''originator's bank,'' as defined in §103.11(e) and §103.11(w), respectively, include institutions located outside the United States, the requirements of the Bank Secrecy Act generally do not apply to foreign beneficiary's banks or foreign originator's banks. The definitions of ''beneficiary's bank'' and ''originator's bank'' were expanded to include foreign institutions in order to clarify the role of domestic institutions involved in international transactions. Thus, domestic banks involved in international transactions are not required under the rule to contact the foreign bank for missing information on the foreign bank's customer. The Board and the Treasury Department encourage foreign banks, however, to comply with efforts to obtain and include complete information on the parties to a transfer where not otherwise forbidden by law.

4. *Question:* ***Funds Transfer.*** Does the rule apply only to ''wire transfers''?

   Answer: No. The rule applies to funds transfers and transmittals of funds, which cover a broad range of methods for moving funds. The rule includes certain internal transfers, e.g., when a bank transfers funds from an originator's account to a beneficiary's account at the same bank (if the originator and beneficiary are different parties), as well as orders made in person or by telephone, facsimile, or electronic messages sent or delivered by a customer or by an NBFI on behalf of a customer to the NBFI's bank. The definition includes all funds trans-

fers that are made within the United States, regardless of whether the transfer originates or terminates abroad.

5. *Question:* ***Originator.*** If a corporation has one or several individuals who are authorized by the corporation to order funds transfers through the corporation's account, who is the originator in such a transfer?

   Answer: The corporation, and not the individual(s) authorized to issue the order on behalf of the corporation, is the originator. Accordingly, the information must be retrievable by name of the corporation, not by the name of the individual ordering the funds transfer.

6. *Question:* ***Originator, Originator's Bank***. Which parties are the originator and the originator's bank with respect to a funds transfer initiated by a customer of a foreign bank?

   Answer: The customer of the foreign bank, i.e., the sender of the first payment order, is the originator. The foreign bank accepting the payment order from that customer is the originator's bank.

7. *Question:* ***Originator, Originator's Bank, Transmittor, Transmittor's Financial Institution, Intermediary Financial Institution.*** Which parties are the originator and transmittor of a funds transfer/transmittal of funds when funds are wired by a money transmitter (on behalf of its customer) through an account at a bank?

   Answer: The transmittor is the money transmitter's customer; the money transmitter is both the transmittor's financial institution and the originator; the bank is the originator's bank and an intermediary financial institution.

8. *Question:* ***Originator, Originator's Bank.*** Who is the originator in a transaction where a trustee initiates a funds transfer from an account at a bank held by the trust?

   Answer: The trustee is merely the person authorized to act on behalf of the trust, which is a separate legal entity. The trust, itself, is the originator of the funds transfer and the bank holding the account is the originator's bank.

9. *Question:* ***Originator's Bank.*** If a customer initiates a funds transfer through Bank 1, which uses Bank 2 as its correspondent, which bank is considered the originator's bank?

   Answer: The customer is the originator; Bank 1 is the originator's bank; Bank 2 is an intermediary bank.

10. *Question:* ***Payment Order.*** Is an instruction to a bank to effect payment under a letter of credit a payment order and subject to the recordkeeping requirements?

    Answer: This issue is discussed at length in Official Comment 3 to UCC 4A-104. As a general matter, the instruction to a bank to effect payment under a letter of credit is subject to a requirement that the beneficiary perform some act such as delivery of documents. Because the term ''payment order'' is limited to instructions that do not state a condition to payment to the beneficiary other than time of payment, the transaction is not a payment order and not a funds transfer subject to the recordkeeping requirements. Certain other transactions connected with a letter of credit, however, may meet the definition of ''payment order.''

SECTION 103.33—RECORDS TO BE MADE AND RETAINED BY FINANCIAL INSTITUTIONS

(The following questions and answers, which use the terminology associated with funds transfers through banks, also are applicable to transmittals of funds through nonbank financial institutions (NBFIs).)

§103.33(e)(1)—Recordkeeping Requirements.

11. *Question:* When does the recordkeeping rule take effect?

    Answer: May 28, 1996.

12. *Question:* Are all funds transfers subject to the recordkeeping rule, regardless of the size of the transaction?

Answer: No. Only funds transfers equal to or greater than $3,000 are subject to the rule.

13. *Question:* How long must the information collected under the rule be kept?

    Answer: Pursuant to §103.38(d), all information required to be collected under the rule must be retained for at least five (5) years.

14. *Question:* Does the rule require any reporting to the government of any information?

    Answer: No. Information related to a funds transfer may be subject to the Bank Secrecy Act's suspicious activity reporting requirements, however, which became effective on April 1, 1996.

15. *Question:* What is the relationship between the funds transfer recordkeeping rule and the rules for reporting suspicious transactions by financial institutions?

    Answer: The funds transfer recordkeeping requirements do not affect an institution's responsibility to report a transaction as suspicious under the terms of the rules requiring such reporting. The two rules are separate and distinct requirements under the Bank Secrecy Act. Circumstances under which a bank should report a funds transfer as suspicious are discussed more fully at 61 FR 4326 *et seq.*, February 5, 1996.

16. *Question:* If oral payment order instructions initially are recorded on audio tape, must the record of those instructions required by this rule be kept in that form?

    Answer: No. The bank may retain either the original or a microfiche, other copy, or electronic record of the instructions. The copy of an audio recording of the payment order need not be a verbatim transcription, so long as it contains the required information.

17. *Question:* May a bank use a code name or pseudonym for its customer?

    Answer: Banks might, for a number of reasons, use various classification schemes in connection with their funds transfer records. A bank must be able to retrieve the records, however, based on its customer's true name, rather than the code name or pseudonym.

18. *Question:* Is retaining the city and state (or country) considered a sufficient address?

    Answer: Banks should obtain a complete address including street information when possible.

19. *Question:* If a customer arranges to have its mail held for pick up at a bank location, may it use the bank's address as the address of its customer?

    Answer: No. The bank should retain a record of the customer s address, rather than the address of the bank location at which the customer's mail is held for pickup.

20. *Question:* In some circumstances, transmittal orders may be ''aggregated.'' For example, a casa de cambio in Texas may collect several transmittal orders for small amounts from different individuals who are sending money to relatives in Mexico and ''bundle'' them into a single transmittal order to a Texas bank as part of a transmittal of funds to a Mexican casa de cambio. The ''aggregate'' transmittal order does not identify the individual transmittors or recipients of the underlying transmittal orders. The Texas bank sends the ''aggregate'' transmittal order to a Mexican bank (for which it holds a clearing account), and the Mexican bank pays the Mexican casa de cambio. The casa de cambio pays the Mexican recipients based on the separate transmittal orders that it received directly from the Texas casa de cambio. What are the recordkeeping requirements for the Texas casa de cambio and the Texas bank?

    Answer: In this example, the payments are completed by a combination of (1) transmittals of funds between the casas' de cambio customers and (2) a separate funds transfer between the casas de cambio themselves. With respect to the first set of transmittals of funds, the individuals in Texas are the transmittors and the Texas casa de cambio is the transmittor's financial institution, which must collect and retain the information regarding the individual transmittal orders as required by §103.33(f)(1)(i) (except

for any transmittal order that is less than $3,000). The Texas casa de cambio sends messages (by telephone or telegraph), which are transmittal orders, to the Mexican casa de cambio providing instructions for payment to the recipients. The Mexican casa de cambio is the recipient's financial institution. The Mexican individuals are the recipients.

These transmittals of funds are settled through the separate ''aggregated'' funds transfer, in which the Texas casa de cambio is the originator and the Texas bank is the originator's bank. This is a separate funds transfer because the Texas bank has aggregated several discrete transmittals of funds, thereby changing the payment order amount as well as the parties to the transfer. The Texas bank is required to collect and retain the information regarding the Texas casa de cambio required by §103.33(e)(1)(i). With respect to the aggregated funds transfer, the Mexican bank is the beneficiary's bank and the Mexican casa de cambio is the beneficiary.

21. *Question:* Are there any differences in recordkeeping requirements for nonbank financial institutions compared to financial institutions?

Answer: There is one incremental recordkeeping requirement on NBFIs. NBFIs, but not banks, must keep the original or a copy of any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order. (See §103.33(f)(1)(i)(G).) The transmittor's financial institution may either keep the original or a microfilm, other copy, or electronic record of the information contained on the form.

§103.33(e)(2)—Originators other than established customers.

22. *Question:* Is a bank obligated to accept a payment order from someone that is not an established customer?

Answer: No. This rule merely sets forth the requirements for payment orders accepted by a financial institution.

§103.33(e)(3)—Beneficiaries other than established customers.

23. *Question:* If a beneficiary's bank attempts to obtain identification from a beneficiary who is not an established customer, and the person is unable or unwilling to provide the identification, should the bank refuse the transaction?

Answer: The responsibility of a beneficiary's bank that accepts a payment order involves laws other than the funds transfer recordkeeping rule. The recordkeeping rule does not affect that responsibility. If the beneficiary's bank is instructed to make payment to the beneficiary in person and the person claiming to be the beneficiary fails to provide identification required by the rule, the beneficiary's bank's responsibility to make that payment may be affected. If the beneficiary s bank does not believe, however, that the lack of cooperation of the person claiming to be the beneficiary provides an adequate basis for withholding payment, it should note in the record the lack of identification required by the rule. In addition, bank personnel should report any suspicious transactions to law enforcement authorities as required by the suspicious activity reporting rules.

The rule does not require identification when proceeds are not delivered in person to the beneficiary. The beneficiary's bank should retain a copy of the check or other instrument used to effect payment, or the information contained thereon, as well as the name and address of the person to which it was sent.

§103.33(e)(4)—Retrievability Requirements.

24. *Question:* How quickly must records be retrieved?

Answer: The retrievability standard is set forth in §103.38(d). Under this standard, the expected timeliness of retrievability will vary based on the circumstances. Generally, records should be accessible within a reasonable period of time, considering the quantity of records requested, the nature and age of the record, the amount and type

of information provided by the law enforcement agency making the request, as well as the particular bank's volume and capacity to retrieve the records. As a practical matter, the expected timeliness for retrievability will depend on the terms of the request.

25. *Question:* How must records be retrievable?

Answer: Information retained by an originator's bank must be retrievable by the originator's name and, if the originator maintains an account that has been used for funds transfers, by the originator's account number. A beneficiary's bank must retain and retrieve information by the beneficiary's name and, if the beneficiary is an established customer with an account, by account number.

The information need not be retained in any particular manner, as long as the bank retains the required records in such way that it is able to meet the retrieval requirements of the rule. A bank may take intermediary steps as necessary to retrieve a requested record. For example, if a bank were directed to retrieve a transfer based on the name of its customer, the bank may first look up the account number for that customer, and then review the customer account statements for the specific funds transfer(s). Using the transaction number identifying the specific transfer that is included on the customer statement, the bank may then retrieve that transfer from its funds transfer records. In addition, if the bank accepts transfers from noncustomers, the bank also must retrieve records of any noncustomer transfers based on the name provided.

26. *Question:* When there are two or more names on an account, must banks be able to retrieve records by all names on the account or just the primary account holder(s)?

Answer: Whenever a bank is obligated to provide records under this rule and the request contains the specific name of an individual, the bank must be able to retrieve records by that name, regardless of whether the person is a primary account holder.

27. *Question:* Must records retained under the rule be maintained on-site?

Answer: No. There is no requirement for records to be maintained on-site.

28. *Question:* Must a bank automate its funds transfer records and retrieval systems in order to comply with the regulation?

Answer: No. Although an automated recordkeeping and retrieval system is not required by the rule, a bank may wish to consider implementing an automated system, depending on the demand for funds transfer records and its current means of keeping the records. Based on the volume of law enforcement requests, a bank should weigh the costs of implementing an automated system versus the costs of searching manual records. The rule does not require that information be maintained in any particular order. For example, a bank may retain information about its customers in its customer file and information about funds transfers in a separate file and may cross reference and retrieve the information.

§103.33(e)(6) Exceptions.

29. *Question:* What types of transfers are excepted from the rule?

Answer: The following transfers are excepted from the rule:

i) transfers of less than $3,000;
ii) debit transfers;
iii) transfers governed by the Electronic Fund Transfer Act, as well as any other funds transfers made through ATM, ACH, and POS systems;
iv) transfers where both the originator and the beneficiary are any of the following:
   (A) A domestic bank;
   (B) A wholly-owned domestic subsidiary of a domestic bank;
   (C) A domestic broker or dealer in securities;
   (D) A wholly-owned domestic subsidiary of a domestic broker or dealer in securities;
   (E) The United States;
   (F) A state or local government; or
   (G) A federal, state or local government agency or instrumentality;
(v) transfers where both 1) the originator and the beneficiary are the same person,

and 2) the originator's bank and the beneficiary's bank are the same domestic bank.

30. *Question:* Does the rule apply to transfers from a person's individual bank account to the person's joint bank account at the same domestic bank?

    Answer: No. The originator and beneficiary are the same person, and the originator's and beneficiary's bank are the same domestic bank. These transfers are excepted from the rule.

31. *Question:* Does the rule apply to intrabank transfers where the originator and the beneficiary are different persons?

    Answer: Yes. Intrabank transfers are excepted from the rule only if the originator and beneficiary are the same person (unless the originator and the beneficiary are both excepted entities, as described in A33).

32. *Question:* Does the rule apply to transfers where the originator and beneficiary are the same person and the originator's bank and beneficiary's bank are separate banks owned by the same bank holding company?

    Answer: Yes. The rule applies to these transfers, because although the banks are affiliated, they are separate legal entities. Transfers between U.S. branches of the same domestic bank, even across state lines, are excepted, however, if the originator and the beneficiary are the same person.

33. *Question:* Please clarify the application of the exceptions for funds transfers contained in §103.33(e)(6).

    Answer: If both counterparties (originator and beneficiary) to a funds transfer are any of the listed excepted entities, the transaction is excepted. Examples of excepted transfers would include a transfer from the U.S. Treasury to a public school district (a local government instrumentality); a transfer from a domestic bank to a domestic broker/dealer; and a transfer from a domestic broker/dealer to a state treasurer.

34. *Question:* A bank's trust department uses a nominee, which is a partnership (not a wholly-owned subsidiary of the bank), and this nominee sends recurring wire transfers from the nominee account to an account in the nominee name at another bank. Are these transactions excepted from the recordkeeping requirements?

    Answer: It is not uncommon for a bank to establish a nominee for purposes of registering stock certificates, commercial paper, participations, and registered bonds. The nominee generally is a partnership of designated officers or staff members and possesses a legal name (different from the bank) that is registered in accordance with state laws. Because the nominee is a separate legal entity, and not a wholly-owned subsidiary of the bank, its funds transfers are not excepted from the recordkeeping requirements.

35. *Question:* Comment 5 to UCC 4A-104 states that there are limited instances in which the paper on which a check is printed can be used as a means of transmitting a payment order that is covered by Article 4A. For example, if an originator's bank (Bank A) does not have a correspondent relationship with the beneficiary's bank (Bank B), Bank A may send a teller's check to Bank B if the amount of the transfer is small and Bank A and Bank B do not have an account relationship. Bank A may execute the originator's payment order by issuing a teller's check payable to Bank B along with instructions to credit the beneficiary account in that amount. The instruction to Bank B to credit the beneficiary's account is a payment order, and the check is the means by which Bank A pays its obligation as sender of the payment order. The instructions may be given in a separate letter accompanying the check, or printed on the check. According to the Official Commentary to UCC 4A-104, the instruction to pay the beneficiary is the payment order, but the check itself is an instrument under Article 3 and not a payment order. Is this type of transaction subject to the rule's recordkeeping requirements?

    Answer: Yes. If a transaction is defined as a funds transfer under UCC 4A and not subject to any of the specific exceptions in the rule, it is subject to the rule's requirements.

The Treasury and the Board have attempted to conform the definitions of the rule as closely as possible to UCC 4A definitions to avoid confusion in the banking industry. The Treasury and the Board do not plan to expand the exceptions to the rule at this time, but may consider whether modifications to the exceptions would be appropriate as part of Treasury's study of the industry and law enforcement's experience under the rule.

INTRODUCTION

The Office of Foreign Assets Control of the U.S. Department of Treasury (''OFAC'') administers and enforces economic and trade sanctions against targeted foreign countries, terrorism sponsoring organizations and international narcotics traffickers based on U.S. foreign policy and national security goals. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments. While OFAC is responsible for promulgating, developing and administering the sanctions for the Secretary under eight basic statutes (not listed here), all of the bank regulatory agencies cooperate in ensuring financial institution compliance with the regulations.

EXAMINATION PROCEDURES

Contained within the BSA Workprogram is a series of questions regarding the examination of an institution's OFAC compliance program. Specific questions regarding possible applicable transactions or other general OFAC questions can be directed to OFAC offices in a variety of ways, including by phone at 1-800-540-OFAC (6322).

FEDERAL RESERVE COMMUNICATION OF OFAC UPDATES

The Federal Reserve System disseminates OFAC updates to points of contact at each Federal Reserve Bank. Specific questions regarding the dissemination of information or compliance questions can be directed to the Federal Reserve Board's Special Investigations and Examinations Section at 202-452-3168.

OFAC HOME PAGE SITE

General information regarding prohibited transactions, compliance, penalties and other matters can be located on OFAC's home page site: http//www.ustreas.gov/treasury/services/fac/fac.html.

Interim Exemption Procedure for Currency Transaction Reporting

U.S. Department of the Treasury
Financial Crimes Enforcement Network

Section 1506.0

INTRODUCTION

This document is intended to answer general, basic questions about how to implement the new CTR exemption procedures. It is not meant to be comprehensive and does not replace or supplement the regulations.

The existing administrative exemption process is being amended to revise, expand and simplify the exemption procedures. A copy of this interim rule is located in section 502 of this manual. We welcome comments on how to simplify or otherwise improve the procedures still further.

Copies of this FinCEN document ''new exemption procedures for currency transaction reporting'' (published in May 1996) may be obtained: via computer by a modem from the Treasury Bank Secrecy Act (BSA) Bulletin Board at 313-234-1453.

A. New Procedures

1. What new exemption procedures are in effect?

The Financial Crimes Enforcement Network has issued an interim rule that eliminates the requirement that banks file currency transaction reports (CTR, Internal Revenue Service form 4789) for transactions by exempt persons.

2. What is an interim rule?

An interim rule becomes effective immediately, without a notice and comment period. One reason for its use is to grant immediate relief from an existing regulatory requirement.

3. Are banks required to adopt the new exemption procedure?

No. This interim rule *permits* but does not require banks to use the new simplified exemption procedure for certain types of customers. This rule implements Bank Secrecy Act mandatory exemption requirements, and grants significant relief to banks. The Financial Crimes Enforcement Network believes that the benefits of this rule will motivate banks to adopt this new procedure voluntarily.

4. Is there a transition period between the old exemption procedures, and the new exemption procedure, for currency transaction reporting by banks?

No. There is no formal transition period, because banks are not required to implement these new exemption procedures. A bank may continue to operate under the previous, more labor-intensive and cumbersome procedures if it wishes. But, if a bank does so, the bank remains subject to all the requirements, and to the penalty rules governing that system. The Financial Crimes Enforcement Network anticipates that banks will use the new exemption procedures because they require significantly less effort and afford banks a limitation on liability.

5. Will this interim rule become permanent?

The Financial Crimes Enforcement Network is seeking public comment on this rule. The comments will be analyzed and any appropriate amendments will be made. The rule will then be published as a final (or permanent) rule in the *Federal Register*. Again, comments are welcome regarding this rule and any suggestions to improve or clarify it.

B. Suspicious Transaction Reporting and Other Bank Secrecy Act Reporting

6. If a customer is exempt from currency transaction reporting, is it then also exempt from other BSA requirements?

No. This is especially important for banks to remember, because of the new suspicious trans-

action reporting requirements. A customer that is exempt from currency transaction reporting is, nonetheless, fully subject to the suspicious transaction reporting requirements.

If a bank knows, suspects, or has reason to suspect that a currency transaction constitutes a suspicious transaction, as defined in the suspicious transaction reporting rules that became effective April 1, 1996, a Suspicious Activity Report is required. Thus, for example, if a bank suspects that a government agency is engaged in suspicious activity, the bank must file a suspicious activity report. Similarly, if a customer is engaged in frequent, large currency transactions that lack any apparent business purpose and the bank knows of no reasonable explanation for the transactions, the bank may be required to file a Suspicious Activity Report.

C. Exempt Person

7. What is an ''exempt person''?

An ''exempt'' person is:

a) a bank (wherever chartered) to the extent of its United States activities;
b) federal, state, or local government department or agency
c) any entity exercising governmental authority (such as the power to tax, to exercise eminent domain, or to exercise police powers); and
d) any corporation whose common stock is listed on the New York Stock Exchange *or* the American Stock Exchange (but not the Emerging Company Market) *or* the NASDAQ National Market (but not the NASDAQ Small-Cap Issues Market).
e) any subsidiary of any listed exempt corporation *if* it filed a consolidated federal income tax return with the publicly traded corporation.

8. What documentation do I need to show that an entity is exempt?

In general, a bank must take steps to assure itself that a customer is exempt comparable to those that a reasonable and prudent bank would take to protect itself from fraud based on misidentification of a person's status. The rule includes operating rules to make this easier.

In the case of a bank or federal, state or local government, the same documentation a bank receives now authorizing the establishment of a business account with a bank or a governmental unit is generally sufficient. Such documentation might include a corporate resolution by the other bank authorizing the establishment of an account and granting signature authority over its account to named individuals. In addition, any documentation that demonstrates that a customer is a bank is sufficient. A bank is expected to exercise the same prudent standards of due diligence that it employs in the conduct of its banking activities.

The Financial Crimes Enforcement Network is aware that certain small governmental units, such as a volunteer fire department, or a rural water authority may not issue detailed documentation that specifically attests to their governmental status. A bank may rely on reasonable documentation, based on the type and nature of the governmental agency involved. In addition, a bank may rely on community knowledge or knowledge based on the customer s name to make such a determination.

In the case of an entity exercising governmental authority, a bank must determine and document characteristics that make such an authority governmental in nature. Such characteristics include the authority to exercise eminent domain, the authority to tax the public, and the authority to routinely exercise police powers. A clear example of governmental authority is the Port of New Orleans.

It is important to note that government contractors are *not* governmental authorities solely by virtue of the services that they provide to the government.

9. How does a bank determine that a corporation's common stock is listed on one of the exchanges that make the corporation eligible for exemption?

The business section of many newspapers, and business weeklies, such as *Barron's, the Wall Street Journal,* or *Investor's Daily* contain listings for businesses that are listed on the stock exchanges.

10. How does a bank determine that a business is a subsidiary of one of the exemption-eligible corporations and *that it files a consolidated tax return with the publicly traded corporation?*

Any reasonable documentation will be sufficient. Examples of such documentation might

include a letter signed by a company officer, or by a company official listed as a signatory on a company account, or a copy of the affiliation schedule for the tax return filed.

11. How are franchises treated under these rules?

Franchises are *not* exempt simply because the company that awards the franchise license is exempt. For example, McDonald's owns approximately 20% of all restaurants nationwide. Thus, for the 80% of McDonald's restaurants that are franchises, a bank must determine whether the franchise is itself a publicly traded corporation or its consolidated subsidiary. In many cases the result will be that the franchise is not exempt.

D. Designation of Exemption

12. Is the designation of exemption automatic, once a bank determines that a customer is exempt?

No. There is one additional requirement. To take advantage of this new procedure, a bank must generally make a designation of exemption within 30 days of a reportable transaction, and stop filing CTRs. A designation of exemption is made by filing a single CTR in which Part I, Section A and Part III are fully completed and box 36 is marked ''Designation of Exempt Person.'' The bank must file one such designation of exemption for each customer that it treats as an exempt person.

13. When a bank files a designation of exemption, must it describe why a particular customer is exempt?

No. However, internal records maintained at the bank should indicate why a particular customer is exempt (*e.g.,* a public school is a government agency, General Electric Corp. is listed on the New York Stock Exchange, etc.). In addition, on the designation of exemption, the bank must state the occupation of the exempt person, and may state County government or State police or similar occupations that will indicate why the customer is exempt.

14. Should a bank file a separate exemption for each account, or one for all accounts that an eligible customer has?

A single designation of exemption should be filed for each 'exempt person' that is a customer at a bank, regardless of the number of accounts held by an exempt person.

15. What if an exempt customer does not have an account at the bank?

An exempt customer, which does not have an account at a bank, is nonetheless exempt, and a designation of exemption may be made. Common examples are governmental agencies. It is not uncommon for the United States government, especially the armed forces, to cash large checks at banks at which it does not have an account. Such transactions are by exempt persons.

A bank should bear in mind that large currency transactions by many types of listed corporations, in contrast, may be suspicious, if the corporation does not have an account at the bank. Such suspicious transactions may be required to be reported.

E. Benefits and General Information

16. What is the benefit of this new exemption procedure to the bank?

There are several benefits. First, this is far simpler than the existing system and should reduce the filing burden for banks.

Second—a bank that exempts a customer in this manner *cannot be penalized* for a failure to file a CTR unless the bank knowingly filed a false or incomplete report, or if the bank *knew or had reason to believe* that the customer or the transaction was not exempt or was not transacted by the exempt customer.

17. What is the benefit of this rule to the public?

This rule will significantly reduce the Bank Secrecy Act compliance burden and liability for banks, while maintaining the usefulness of CTRs

for law enforcement, and regulatory purposes. As such, this rule advances the principles of Executive Order 12866 to create ''regulations that are effective, consistent, sensible, and understandable.'' By making the CTR process more consistent, sensible and understandable, these rules will be more effective for both the government and for the banking industries.

18. Will the Treasury Department exempt other types of businesses?

The Treasury Department is committed to reducing the number of CTRs while retaining filings that are *highly useful* for tax, regulatory, and criminal proceedings. FinCEN has solicited public comments on whether businesses not incorporated that have equity interests publicly traded on major exchanges should be deemed 'exempt persons.'

The Financial Crimes Enforcement Network is interested in comments on whether privately held firms should be able to be exempted, under an exemption process that takes into account the lower level of public scrutiny afforded such firms. FinCEN is aware that the new procedure will provide the greatest benefit to large banks in urban areas, and may provide less benefit to smaller, community-based banks. FinCEN remains committed to providing a similar degree of regulatory relief to community-based banks, and intends to propose a regulation that will exempt other types of businesses as well.

19. To whom may a bank go should it have further questions?

Any bank may contact its primary Bank Secrecy Act examination authority, or the Treasury Department's Financial Crimes Enforcement Network can be contacted regarding questions on the Bank Secrecy Act rule at (800) 949-2732 or (703) 905-3920.

Workpapers are the written documentation of the procedures followed and the conclusions reached during a Bank Secrecy Act examination. In addition, the workpapers are used to document management's responses and commitments to issues raised during the course of the examination. Accordingly, they include, but are not necessarily limited to, examination procedures and verifications, memoranda, schedules, questionnaires, checklists, abstracts of bank documents and analyses prepared or obtained by examiners.

The workpapers are important to the supervisory process because they are expected to support the information and conclusions contained in the related report of examination. The primary purposes of workpapers are to:

- Organize the material assembled during an examination to facilitate review and future reference.
- Aid the examiner in efficiently conducting the examination.
- Document the policies, practices, procedures and internal controls of the institution.
- Provide written support of the examination and audit procedures performed during the examination.
- Document the results of testing and formalize the examiner's conclusions.
- Substantiate the assertions of fact or opinion contained in the report of examination.
- Aid the examiner-in-charge in planning, directing, and coordinating the work of the assistants.
- Guide future examinations in terms of estimated personnel and time requirements.

Workpapers are to be prepared in a manner designed to facilitate an objective review, organized to support an examiner's current findings, and should document the scope of the current examination. The following is a listing of possible workpapers to support the Bank Secrecy Act examination. The list is not meant to be all inclusive and the final contents should be dictated by the scope of the examination:

- Copy of previous findings/management responses.
- Listing of Currency Transaction Reports obtained from the IRS database.
- Cash flow and/or Intelligence data obtained during examination, if applicable.
- Bank Secrecy Act policies and procedures.
- Audit workprogram/independent review program.
- Most recent internal audit/independent review results.
- Bank Secrecy Act training program.
- Exemption list and related documentation.
- IRS and Treasury correspondence regarding special exemptions.
- Know Your Customer policies.
- Copy of completed examiner BSA workprogram.
- Anti-money laundering/suspicious activity reporting program.

Judgment is required as to what workpapers should be retained for each examination. Lengthy documents should be summarized or highlighted (underlined) so that the examiner who is performing the work in the related area can readily locate the important provisions without having to read the entire document. If the documents are voluminous, as may be the case with the Bank Secrecy Act policies and procedures, a summary of the document or table of contents should be included rather than the entire document.

WORKPAPER RETENTION

Examiners should retain on a readily available basis those workpapers from:

- the most recent Federal Reserve System Bank Secrecy Act examination.
- past Federal Reserve System Bank Secrecy Act examinations where adverse findings are cited, up to a five-year period.
- examinations performed by other regulatory agencies where adverse findings are cited (up to five years).
- examinations disclosing conditions which lead, or may eventually lead, to a suspicious activity report or criminal investigation.

These guidelines are the minimum required retention period for workpapers; longer retention periods may be set by individual Reserve Banks.