TESTIMONY OF
RALPH E. SHARPE
DEPUTY COMPTROLLER OF THE CURRENCY
for
COMMUNITY AND CONSUMER POLICY
OFFICE OF THE COMPTROLLER OF THE CURRENCY

Before the
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
of the
COMMITTEE ON GOVERNMENTAL AFFAIRS
of the
UNITED STATES SENATE

November 10, 1999

Statement required by 12 U.S.C. § 250:

The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

I. Introduction

Madam Chairman, Senator Levin, and members of the Subcommittee, my name is Ralph Sharpe and I am the Deputy Comptroller for Community and Consumer Policy at the Office of the Comptroller of the Currency (OCC). We appreciate this opportunity to testify on private banking activities and the vulnerability of private banking to money laundering. Money laundering, namely the movement of criminally derived funds for the purpose of concealing the true source, ownership, or use of funds, is a serious domestic and international law enforcement problem and we commend the Subcommittee for focusing attention on the problems that it poses.

The Office of the Comptroller of the Currency (OCC) has a longstanding commitment to combat money laundering and to address this problem in the banks that we supervise. We share the Subcommittee's belief in the importance of preventing U.S. financial institutions from being used wittingly or unwittingly to aid in money laundering. As part of our efforts to combat money laundering in private banking, we are focusing on the risks associated with the increasing size, complexity and global reach of private banking, and we have taken a number of steps to prevent the misuse of national banks for money laundering. We are also committed to working with the law enforcement community to assist in the investigation and prosecution of organizations and individuals who violate the law and engage in money laundering.

My testimony today addresses the issues you raised in your invitation letter. I will begin by describing the nature of private banking, the statutory and regulatory requirements, the vulnerabilities of private banking, techniques banks may use to protect themselves against these

vulnerabilities, and the examination procedures OCC uses to address potential money laundering in all aspects of a bank's operations, including those relating to private banking. I will then discuss our review of Citibank's anti-money laundering programs, including those carried out in the bank's private banking department. Then, I will discuss our experience in obtaining customer information from banks supervised by the OCC in foreign jurisdictions, and OCC initiatives to combat money laundering. I will conclude by addressing the Administration's National Money Laundering Strategy of 1999 and how it should enhance our ability to deal more effectively with the many challenges presented in this area.

II. BackgroundBroadly defined, private banking involves providing a wide range of financial services to high net-worth customers. Based on an informal 1997 OCC examiner survey of several large banks supervised by the OCC, the typical private banking customer has assets of between $1 million to $5 million available for investment. Of course, these figures may be considerably less in some markets.

Once a service provided only by European banks to a small number of wealthy clients, private banking has become a growing source of business for a number of banks in the United States, particularly larger banks. The United States has become the largest private banking market in the world and private banking services provide an important source of fee income for banks seeking to diversify and provide additional services to their customers. Continued expansion of private banking is likely as the number of high net-worth individuals grows.

Banks offer a mix of financial services under the umbrella of private banking. A relationship manager is typically the single point of contact for the private banking customer within the bank, identifying the needs of the customer and arranging for the delivery of products and services designed to meet those needs. These services often include: asset management relationships (trust, investment advisory, and investment management accounts), offshore facilities, custodial services, funds transfer, lending services, checking accounts, overdraft privileges, letter of credit financing, bill-paying services and tax and estate planning. There is no uniform structure for the location of private banking activities within a bank. Private banking activities may be conducted within a separate unit of a bank, or may be interspersed throughout the bank according to product lines. Several national banks also operate as independent trust banks that offer private banking services exclusively.

III. Statutory and Regulatory Requirements

The Bank Secrecy Act (BSA), and its implementing regulations is one of the primary tools the government uses to fight drug trafficking, money laundering, and a host of other crimes. Congress enacted the BSA to attempt to prevent banks and other financial institutions from being used as intermediaries for or to hide the transfer or deposit of money derived from criminal activity.

The reporting and record keeping requirements of BSA regulations create a paper trail for law enforcement to follow to trace drug and other illegal proceeds to their sources. The paper trail is

used by the government to help identify, detect and investigate criminal, tax and regulatory violations. It is used to deter illegal activity and to trace the movements of money into and out of the United States. Over the years Congress has amended the BSA to enhance its usefulness as a law enforcement tool while also reducing the regulatory burden.

In addition to the BSA, in 1986 Congress made money laundering itself a criminal activity with the enactment of the Anti-Drug Abuse Act of 1986, which included the Money Laundering Control Act of 1986 (MLCA). The law prohibits any person from knowingly engaging in a financial transaction that involves the proceeds of a specified unlawful activity.

The primary responsibility for compliance with the BSA and the anti-money laundering statutes rests with the nation's financial institutions themselves -- they represent the front lines in the fight against money laundering. National banks have significant anti-money laundering responsibilities. As described in the BSA section of the Comptroller's Handbook for National Bank Examiners (BSA Handbook), 12 CFR 21.21 requires national banks to establish and maintain adequate internal controls and independent testing, to designate an individual or individuals to coordinate and to monitor day-to-day compliance with the BSA, and to train responsible personnel. In addition, OCC regulations at 12 CFR 21.11, require banks to report suspicious transactions and violations of law or regulation. An adequate BSA program must enable a bank to detect and report suspicious activity, including any such activity in its private banking department.

IV. Protecting Against the Vulnerabilities of Private Banking

If a bank does not adequately maintain due diligence and compliance standards with associated internal controls, audit and management information systems, it may be exposed to money laundering. Specific vulnerabilities associated with private banking operations include the following:

Account Opening Procedures.

Determining the identity and bona fides of high net-worth customers should generally be no more challenging to a bank than determining the identity of any other customer. However, the large dollar amounts involved, the potential for the existence of other beneficial parties and the complications of obtaining current and accurate information regarding these matters may present unique challenges. This is particularly the case when the customer is a foreign national and the source of the funds comes from outside of the country. Moreover, the desire of the customer to maintain a high degree of confidentiality can also serve to increase the difficulty of obtaining this information.

Compensation of Relationship Managers.

The high dollar volume of private banking and resulting earnings for the bank and account officers pose additional challenges and potential vulnerabilities. In some private banking units,

the pressure for increased income based on new business and compensation programs based solely on quantitative factors can cause bank officers to ignore or short-cut established controls and procedures designed to protect banks from money laundering. The prestige and specialized treatment that private banking clients generally receive may also tempt a bank employee to sacrifice adherence to control procedures in favor of accommodating a client. This can also lead to a reluctance to follow up on indications of suspicious activity or to file suspicious activity reports.

Access to Account Information.

U.S. banks may offer private banking services domestically or in their overseas offices.

Some accounts are opened domestically, but supporting documentation relating to ownership, and background information, may be maintained in one or more foreign jurisdictions with stringent secrecy laws. Other accounts may be opened and maintained in such jurisdictions from the outset. In either case, such accounts can present significant barriers to access to information needed to fully determine the source of funds flowing into the account or the identity of beneficial owners.

There are, however, a number of things that banks can do to protect themselves against these vulnerabilities. Many of these relate to money laundering in general; some relate more specifically to the vulnerabilities for money laundering in private banking operations. Listed below are a number of fundamental safeguards that should be employed to address and minimize the risk that a bank will be subjected to money laundering.

Effective Account Opening Procedures.

Effective account opening policies and procedures are fundamental risk controls for private banking relationships. Effective procedures include the proper identification of the owners of the account, including beneficial owners, the sources of their wealth and their normal and expected transactions. Bank management should have specific policies for employees who approve, accept and document new private banking accounts. To verify the legal and financial status of a business, the bank's account opening process should require responsible bank personnel to identify the principal owners and should include a review of relevant documentation, such as articles of incorporation, partnership agreements, financial statements, credit reports and referrals.

To the extent possible, banks should also have adequate documentation to allow for appropriate due diligence when opening accounts in jurisdictions with strong secrecy regimes. Banks should also ensure that they will have access to information during the life of an account so that it can be monitored appropriately.

Customers brought in by a third party financial intermediary (e.g., investment advisors) may require particular attention. A bank should confirm that the intermediary maintains and adheres

to adequate standards to verify the identity and legitimacy of its customers. Based on the bank's assessment of the adequacy of this verification process, the bank should gauge its degree of confidence in relying on the third party's customer review process. These standards should also be applied to recently hired private banking representatives who bring in new accounts. Banks should also be cautious in establishing financial services relationships with intermediaries that refuse to provide their policies and procedures for accepting new accounts.

In short, the bank should exercise the degree of due diligence necessary to determine what types of risks are included in opening a particular account and then ensure that adequate procedures are in place to identify and control those risks.

Monitoring for High Risk Activity.

Private banking services are subject to the same anti-money laundering requirements as any other bank relationship. Banks should monitor high-risk customer activity in order to detect and report suspicious activity in a timely manner.

Banks should evaluate accounts on a risk-grade basis, whether by type of business, geographical location, or bank product or service that may be more vulnerable to money laundering. While not all private banking accounts or relationships will fall into a higher risk category under this approach, those that do should be managed accordingly. For example, a high net-worth private banking client in the United States with an import/export business that trades with businesses located in a drug source country would clearly warrant more scrutiny than a lower net-worth demand deposit account with no international activity.

Compensation and Oversight.

Banks should design compensation programs that balance quantitative and qualitative factors and that provide measurement tools to assess employee performance in both areas. They should also ensure that account relationship managers are subject to the same or a higher degree of oversight and control as managers of other areas of operation that may expose the bank to risk. Internal controls, audit and compliance processes should ensure that account managers operate with appropriate oversight and are subjected to periodic audit checks, and banks should include private banking relationships in their suspicious activity identification programs.

Audit for Compliance with the BSA.

Banks must have an independent testing or audit function for BSA compliance, including suspicious activity reporting. Audit programs should focus on high-risk accounts and should include comprehensive transaction testing.

Training for BSA Compliance.

Banks are required to train all appropriate personnel with respect to their responsibilities to comply with the requirements of the BSA. Bank training programs should provide relevant

examples of money laundering in the private banking area and should discuss bank policies and procedures, liability issues and regulatory requirements. In addition, the training program should provide for regular updates to ensure employees are kept current in bank policies and regulatory changes.

V. OCC Supervision - Controls Against Money Laundering.

The OCC conducts regular examinations of national banks, and branches and agencies of foreign banks in the United States, covering all material aspects of each institution's operations, including foreign offices. These examinations include reviews for compliance with the BSA and reviews of anti-money laundering efforts in various divisions of the banks, includovering all material aspects of each institution's operations, including foreign offices. These examinations include reviews for compliance with the BSA and reviews of anti-money laundering efforts in various divisions of the banks, including lending, deposit taking, investments, fiduciary, international, wire transfer and private banking. The OCC's BSA Handbook contains procedures designed to assess BSA compliance, as well as identify money laundering, in accordance with the mandate in section 404 of the Money Laundering Suppression Act of 1994, which required the federal banking agencies to develop enhanced examination procedures to better identify money laundering. The OCC developed these procedures in cooperation with the other federal banking agencies.

The OCC's BSA examination procedures aid our examiners in determining whether national banks have established and maintained adequate compliance programs and management information systems to detect the possibility of money laundering in all aspects of their operations, including private banking. Specifically, the OCC conducts examinations to evaluate whether national banks have adequate systems in place to: (1) detect and report suspicious activity; (2) comply with BSA requirements; (3) establish account opening and monitoring standards; (4) understand the source of funds for customers opening accounts; (5) verify the legal status of customers; and, (6) identify beneficial owners of accounts.

To use our resources most effectively, the OCC conducts top-down BSA/anti-money laundering examinations in large national banks (defined as having $1 billion or more in assets). We begin with a review of policies, procedures and internal controls, which may be followed by more in-depth procedures in areas of higher risk. This review helps determine whether the bank should implement additional policies, procedures, systems or controls to comply with the BSA, and to prevent, detect and report money laundering. If the OCC identifies significant weaknesses in the bank's systems, we will use our supervisory authority to ensure that the bank takes appropriate corrective measures. Similarly, if the OCC uncovers significant risks, the OCC will take steps to ensure that the bank is properly managing those risks. At the next scheduled exam, or sooner, OCC examiners will evaluate the adequacy of the bank's corrective action.

The OCC recently developed, and will soon test, expanded-scope BSA/anti-money laundering examination procedures for private banking. These procedures specifically address employee compensation programs, account opening standards, risk management reports, and suspicious

activity monitoring of private banking activities. The procedures also focus attention on high-risk accounts, such as import/export businesses, private investment companies, accounts of foreign government officials from high risk countries, and high fee income accounts, concentration accounts, and nominee name accounts.

VI. OCC BSA Supervision of Citibank, N.A.

The OCC=s BSA examinations of Citibank in the 1990's began with a routine examination in 1992. During this examination, the OCC advised the bank to establish and formalize a process to identify high risk accounts, such as money service and cash-intensive businesses.

The OCC's 1994 BSA examination identified the need to improve the bank's compliance program in the private bank. Specifically, examiners found weaknesses in the bank=s training program and the processes it employed to supervise its private banking account officers and ensure that the bank's "Know Your Client" standards were being followed. The OCC recommended that the bank establish procedures to monitor the activities of relationship managers to ensure the bank=s standards were not compromised through the unique client/ banker relationship.

In a series of examinations conducted in 1996, OCC examiners noted progress by the bank in correcting deficiencies that had been identified previously. The bank's training program had been upgraded and the bank was in the process of implementing global policies regarding customer identification and source of wealth information. In developing its global policy, a number of revisions were made causing implementation to be re-started several times.

In 1996, in recognition of a need to improve the bank's "Know Your Client" program and in response to an OCC recommendation, the bank developed an account monitoring program and a management information system (MIS) report. In February 1997, using this new report, the Federal Reserve identified an account with unusual activity and referred it for further investigation to the OCC. This is the specific account identified in the Subcommittee's invitation letter. The OCC conducted a detailed review of the bank=s handling of the account, including a review of the activity in the account and the bank=s documentation. Also, the OCC requested additional information from the bank on the customer=s source of wealth. After considering this additional information supplied by the bank, the OCC concluded that a suspicious activity report was not warranted.

In early 1998, OCC provided to the bank an overall assessment of its 1997 performance. This assessment included specific comments relating to the need to improve the bank's control environment in the private bank. While progress in many areas was noted, we informed the bank that there was still a need for increased attention to the control environment. The OCC also pointed out that the OCC had identified a number of audit and control failures in the private bank that required attention.

During several domestic and overseas examinations in 1998, the OCC noted that the long process of documenting the bank's existing private banking customers was nearing completion. The bank had created a new quality control unit to ensure compliance with the bank's policies, and management was effectively responding to issues identified by the unit and the OCC. During these examinations, we found improved internal controls and adequate documentation regarding client source of wealth. However, the OCC also recommended that management implement its "Global Know Your Client" policy within established timeframes, improve information regarding clients' expected transaction volumes, and formalize and implement a monitoring program for all private banking clients, in addition to the high-risk client monitoring program.

In early 1999, the OCC communicated to the bank that the control environment in the private bank, which had led to adverse publicity, had improved. The OCC acknowledged the attention this had received from senior management and the board. In addition, during several overseas examinations of Citibank offices in 1999, examiners continued to note progress in the bank's global compliance and anti-money laundering program.

VII. OCC Experience in Obtaining Information From Foreign Jurisdictions

In most instances, the OCC has not encountered problems in obtaining from the banks that we supervise routine supervisory information domiciled in foreign jurisdictions. This type of information typically includes information which allows OCC examiners to gain an overall perspective on the safety and soundness of a bank's operations in the foreign jurisdiction, particularly the risk environment and controls that are in place. The OCC often obtains information directly from national banks through requests, onsite inspections of their offices in a host foreign jurisdiction, or through a request to a foreign supervisory authority.

For example, in April 1998, the OCC sent three examination teams to South America to conduct eight examinations. We conducted these examinations to review and analyze measures taken by national banks operating in foreign countries to minimize money-laundering risks. During these examis taken by national banks operating in foreign countries to minimize money-laundering risks. During these examinations, the OCC reviewed each bank's corporate and local anti-money laundering policies and procedures and audit functions and met with host country bankers associations and central bank officials. While these examinations were limited in scope, the examiners were able to identify strengths and weaknesses in the local anti-money laundering policies and practices of the subject banks. We are using the results of these examinations to design supervisory approaches for future examinations of overseas offices.

Obtaining account-specific information from some foreign jurisdictions has been significantly more difficult. While legitimate reasons for protecting accounts from review by outside authorities exist, the lack of access to this information is a critical problem in cases where accounts are possibly being used to commit financial crimes, including money laundering. Most foreign jurisdictions with more stringent bank secrecy laws do not consider account-specific records to be routine supervisory information. As a result, those jurisdictions typically prohibit foreign supervisory authorities from accessing customer records. The ability of the OCC to

conduct on-site examinations of foreign branches varies depending on the laws of the jurisdiction. In some locations, financial secrecy and privacy laws prevent on-site OCC examinations. These jurisdictions may also impose criminal sanctions for breaches of financial privacy. In other countries, the scope of the examination is limited because examiners cannot review customer specific records or reports. As a result, the OCC cannot always conduct comprehensive bank examinations or obtain account-specific information that is so important to money laundering investigations.

The OCC addresses problems raised by secrecy laws in foreign jurisdictions in a number of ways. For example, the OCC expects national banks to implement internal controls, monitoring systems and processes to reduce money-laundering risks on a company-wide basis, including in its foreign offices. When on-site reviews are not possible because of bank secrecy and financial privacy laws, the OCC reviews the corporate policy and audit functions of the bank. When we have concerns, we require the bank to address those concerns. This may also include requiring external audits or enhanced reporting requirements.

These difficulties are also being addressed through the many initiatives on the international front that are focused on the concerns surrounding the misuse of offshore accounts for financial crime purposes. International groups such as the Financial Action Task Force (FATF) and the Caribbean Financial Action Task Force (CFATF) have developed guidance and recommendations to help prevent and detect money laundering. Additionally, groups such as the Basel Committee on Banking Supervision and the Financial Stability Forum are taking a broader approach to dealing with secrecy jurisdictions, including the problems these jurisdictions pose with respect to obtaining the information needed for effective cross-border supervision. The G-7, also recognizing the scope and the seriousness of the problem, has developed principles for information sharing between multi-jurisdictional supervisory and law enforcement authorities. The OCC has been directly involved in all of these initiatives.

Most recently, at the request of the Basel Committee, the OCC developed a paper to help supervisors identify potentially problematic jurisdictions. The focus of the paper was on the supervisory and regulatory environment in the various countries and the ability of the jurisdictions to share information with cross-border supervisory counterparts. The paper also highlights a number of steps that home country authorities can take to remedy problems with a host authority, or with U.S. operations in that host jurisdiction.

VIII. Other OCC Initiatives Against Money Laundering

The OCC has undertaken a number of anti-money laundering initiatives. In 1997, the OCC formed an internal task force on money laundering called the National Anti-Money Laundering Group (NAMLG). Since that time, NAMLG has embarked on several important projects. One such project involves targeting banks for expanded scope money laundering examinations, including private banking departments. The targeted examinations are staffed by experienced examiners and other OCC experts who specialize in BSA compliance, money laundering and fraud examinations. The banks are selected for examination by using a filtering process that

includes, among other considerations: (1) locations in high intensity drug trafficking areas; (2) excessive currency flows; (3) significant private bank activities; (4) unusual suspicious activity reporting patterns; (5) unusual large currency transaction reporting patterns; and (6) fund transfers or account relationships with drug source countries or countries with stringent bank secrecy laws.

In addition, the OCC is working with the Financial Crimes Enforcement Network (FinCEN) to further enhance our ability to identify banks at risk for money laundering. For example, the OCC's fraud and BSA/anti-money laundering specialists now have on-line access to the primary databases at FinCEN. These databases house currency transaction reports, suspicious activity reports and other BSA information, as well as Federal Reserve cash flow data (currency flows between the Federal Reserve and depository institutions). This on-line access allows the OCC to analyze data to identify banks with unusual currency or suspicious report activity. The OCC is also working with FinCEN to utilize the agency's "artificial intelligence" capabilities to facilitate our targeting program.

The OCC also conducts targeted examinations based on law enforcement leads. For example, if a U.S. Attorney's Office advises the OCC that a national bank may be involved in a money-laundering scheme, the OCC will send a team of examiners to assess the situation. If, through the examination process, OCC identifies weaknesses in the bank's BSA compliance program or other problems within the OCC's supervisory or enforcement authority, the agency will direct the bank to take appropriate corrective action. In addition, if the examiners discover information that may be relevant to a possible criminal violation, the OCC will direct the filing of a Suspicious Activity Report and provide relevant documents, information and expertise to the receiving law enforcement agency.

This targeting effort resulted in fifteen targeted exams from late 1997 to 1999. Six of these examinations involved private banking. Plans are underway to conduct at least nine more in 2000. In addition to targeting examinations throughout the United States, a special training and targeting examination project was conducted in our Southeastern District during 1999. This project provided examiners with intensive BSA/anti-money laundering training immediately followed by nine expanded scope examinations. The examinations resulted in a number of corrective actions to prevent money laundering. The OCC's Northeastern District plans to conduct a similar initiative in the first quarter of 2000.

OCC District Offices have also formed task forces to interact with the NAMLG and to attack the problem of money laundering. The overall purpose of the district-based initiatives is to implement a more proactive approach on the local level and to foster new ideas and programs for supervising compliance with the BSA and the money laundering statutes by:

identifying and examining high-risk banks;

working with local law enforcement and regulatory agencies;

providing examiner training;

developing and sharing "best practices" examination procedures; and

developing and implementing new anti-money laundering initiatives.

In addition, the OCC has assigned a BSA/money laundering specialist to the Treasury Department's Colombian Black Market Peso Exchange (CBMPE) Working Group. The group meets on a bi-weekly basis to develop and implement operational strategies against money laundering based in the CBMPE. CBMPE is a high priority item of the National Money Laundering Strategy for 1999. So far, the OCC has:

trained examiners on money laundering schemes common to CBMPE;

distributed a FinCEN advisory on CBMPE to national banks; and

developed and field tested examination procedures to detect CBMPE schemes in national banks.

With the support of NAMLG, the OCC also has enhanced its training to detect money laundering, including in private banking accounts. The training instructs examiners to focus on unusual funds transfer activity to or from known offshore money laundering havens. This training was provided in all of the OCC Districts during 1999.

NAMLG is also chairing a working group with other regulatory and law enforcement agencies to develop an interagency training curriculum to heighten awareness of money laundering schemes and to provide case studies of actual examinations that led to the filing of suspicious activity reports and criminal investigations. The interagency group plans to pilot the training program in July 2000.

Other activities of NAMLG include:

analyzing money laundering trends and emerging issues;

sharing money laundering intelligence with OCC District offices;

promoting cooperation and information sharing with national and local anti-money laundering groups, law enforcement agencies, other bank regulators and the banking industry; and

working with law enforcement to develop better means of promoting feedback to financial institutions on the effectiveness of SAR reporting and law enforcement's follow-up.

Overall, through its examination programs, cooperative efforts with others, both domestically and internationally, and NAMLG initiatives, the OCC continues to demonstrate its commitment to combating money laundering.

IX. Additional Initiatives

As you know, the Administration recently released its Congressionally-mandated National Money Laundering Strategy for 1999. The Strategy includes a number of specific objectives aimed at enhancing the ability of law enforcement and the regulatory agencies to combat money laundering. These include: (1) convening a high-level working group of federal regulators and law enforcement officials to examine what guidance would be appropriate to enhance bank scrutiny of certain transactions or patterns of transactions in potentially high-risk accounts; (2) the federal bank supervisory agencies conducting a review, in cooperation with the Treasury Department, of existing bank examination procedures relating to prevention and detection of money laundering at financial institutions; and, (3) proposing legislation to bolster domestic and international enforcement powers to combat money laundering.

The OCC is committed to working closely with all participants in these and other legislative and regulatory efforts over the coming months and years to help meet the goals and objectives of the Strategy.

X. Conclusion

The OCC is committed to preventing national banks from being used to launder the proceeds of the drug trade and other illegal activities. We recognize the potential vulnerability of private banking to money laundering, and our supervisory efforts are aimed at ensuring that banks employ control procedures to reduce that vulnerability. We stand ready to work with Congress, the other financial institution regulatory agencies, the law enforcement agencies, and the banking industry to continue to develop and implement a coordinated and comprehensive response to the threat posed to the nation’s financial system by money laundering.