



ABA

Industry Resource Guide

Identification and Verification of Accountholders

January 2002



Identification and Verification of Accountholders

Industry Resource Guide

January 2002



AMERICAN
BANKERS
ASSOCIATION®

*World-Class Solutions,
Leadership & Advocacy
Since 1875*

Identification and Verification of Account Holders

Table of Contents

Introduction	1
Findings	2
ABA Account Opening Best Practices Group	2
Account Identification and Verification Processes	3
Appendix I Suggested Process Flow	9
Appendix II Additional Resources	10
Appendix III ABA Account Opening Best Practices Group	12
Appendix IV Account Opening Best Practices Meeting Participants	13

Identification and Verification of Account Holders

Introduction

On October 26, 2001, President Bush signed into law the USA Patriot Act of 2001. The Act, a broad anti-terrorism measure, contains a major section on money laundering (title III). The ABA strongly supported the legislation, and has pledged to work closely with all aspects of the financial services industry, as well as government and law enforcement officials, to implement the provisions of this important act in the fight against terrorism.

Section 326 of the Patriot Act requires the Secretary of the Treasury to promulgate regulations that will set forth standards for financial institutions to follow in the identification and verification of customers at account opening. The regulations will, at a minimum, require that all financial institutions:

- Verify the identity of any person seeking to open an account to the extent reasonable and practicable;
- Maintain records of the information used to verify a person's identity, including name, address, and other identifying information; and
- Consult lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.

The legislative intent of Section 326 of the Patriot Act was not to force wholesale changes in the manner in which financial institutions identify and verify accountholders, but rather to ensure that the industry will continue to have adequate policies and procedures and follow best practices. This approach by Congress and the Administration is based on the view that financial institutions by-and-large already have sufficient policies and procedures for account opening.

In fact, the industry has a long history of developing and implementing comprehensive account opening identification and verification procedures and devising best practices to assist in these efforts. As an example, the ABA Check Fraud Prevention Manual, which has already been distributed to over 1,500 financial institutions, outlines a number of ways by which financial institutions can verify the identification of accountholders. This and other available resources are noted in Appendix II of this reference guide.

ABA Account Opening Best Practices Group

The ABA Account Opening Best Practices Group was organized, while the legislation was still being drafted, to develop guidance and recommendations for financial institutions to use in the identification and verification of accountholders at account opening. The guidance that has been developed should also provide valuable assistance to financial institutions to comply with the requirements of Section 326 of the USA Patriot Act.

The eight members of the Account Opening Best Practices Group represent a cross-section of ABA's membership. During its deliberations, the Group held discussions with representatives from the securities industry and a variety of state and federal law enforcement and regulatory agencies, as well as with private sector experts.

In addition, the Account Opening Best Practices Group joined efforts with a similar initiative that was organized by the New York Clearing House in response to the terrorist attacks of September 11. The Resource Guide developed by this Group will be incorporated into the broader work of a Clearing House initiative and distributed to financial services organizations and government agencies.

Findings

During the Group's discussions, it became clear that one of the challenges associated with the current process of identification and verification at account opening is the ease with which identification documents can be falsified. There are a number of vulnerabilities that currently exist in identifying customers, including:

- Lack of uniform procedures for official state identifications;
- Lack of governmental verification processes;
- Lack of meaningful biometric identifiers, and
- Lack of real-time commercial verification products.

These vulnerabilities contribute to a proliferation of Internet websites, where any driver's license or other form of identification may be purchased, sometimes with a "novelty tag" attached to create the subterfuge that the identification document was not intended to be used in a fraudulent fashion. To the extent that many states do not have a mechanism to verify identifications, the Group finds that the current system is simply not sufficient to catch fraudulent state and federal identification documents.

Financial institutions, by-and-large, already have sufficient policies and procedures for account opening. The current account opening procedures at the vast majority of institutions have not been subject to supervisory criticism. The purpose of this, therefore, is to insure that information garnered during the account opening process was properly

authenticated, balanced with the need to make the process reasonable for the customer as well as the financial institution.

It is also important to emphasize that the material in this Resource Guide is purely intended to provide guidance to financial institutions. Each institution should look within its own operations/business markets and make appropriate determinations based upon their risk assessments in order to properly use this when adjusting or creating any new account opening practices.

Any regulations promulgated under this section should not proscribe specific account opening procedures. Different financial institutions should have the latitude to take different approaches depending on their unique characteristics. Giving each financial institution the flexibility to derive its own procedures also lessens the potential burden on community financial institutions.

The low-dollar volume and conventional nature of the accounts utilized by the terrorists, and the fact that many aspects of the terrorist's financial behavior are still unknown, adds to the complexity of determining appropriate account opening process, and further dictates a flexible approach to regulation.

The vulnerabilities associated with the current system of identification are magnified when the potential customer is a foreign national. The many challenges associated with the visa and foreign passport identification systems render them unacceptable for authentication purposes. The vulnerability of these documents to fraud, as well as the ease with which they can be obtained legally, demonstrates that neither document should be able to stand on its own as a form of identification.

The Group strongly recommends that financial institution efforts to authenticate accountholders focus on the information contained within the identification document, not on attempting to determine the veracity of the identification document. Moreover, in terms of the veracity of the identification, it is imperative that financial institutions receive effective, timely and comprehensive governmental support to enhance the verification process and efforts to authenticate identification documents and information provided.

Account Identification And Verification Processes

Based on previous industry guidance and recent discussions with a wide range of industry, government and related experts, the American Bankers Association and the Account Opening Best Practices Group have devised the following set of options for financial institutions to consider in developing customer identification processes. These options take into account the diverse customer identification practices used throughout the financial services industry and are not intended to provide rigid requirements that may not address the specific products, customers or compliance risks that individual financial institutions may identify in connection with their businesses.

In providing these options, the Group recognizes that due to the widespread availability of false documentation, the lack of accessible identification data bases, the inability to verify identification documents with issuing government agencies, as well as other factors, even the most comprehensive customer identification and verification processes will not assure the identity of the person opening an account. Consequently, the verification processes provided below deal primarily with the accuracy of information provided by the customer in the identification process. Without additional verification tools that deal with the legitimacy of the identification document provided by a customer, assurances of actual customer identity in many cases would be difficult to confirm.

Financial institutions have substantial incentives for strong policies to verify account applicants' identification in order to prevent fraud losses. The following are suggested policies to address the identification challenge facing financial institutions. These policies align with the suggested account opening identification and verification process flow chart included as Appendix I:

Individual Accounts

The collection of various types of identifying information and documentation and the processes for verification, as suggested below, may not be applicable to every type of customer or account. Financial institutions may conclude that based on their risk assessment of the customer and the type of services being provided that some customers (e.g. non-resident aliens) or types of accounts (e.g. private bank accounts) may require more or less extensive identifying information and verification than others.

For new accounts at a financial institution opened by a natural person (or more than one natural person) including a sole proprietor business account, the institution should, at a minimum, obtain and record the following information about each owner of the account:

1. Name
2. Tax Identification Number
3. Address
4. Telephone Number
5. Occupation
6. Date of Birth

7. Information concerning business (if sole proprietor business account), such as business address, telephone number and Tax Identification Number, if different than the information of the individual.

As technology advances, institutions may also wish to evaluate and consider certain “biometric” identification information, when practicable, (such as fingerprint or other process that provides information unique to the person opening the account).

In addition, depending upon the nature of the relationship, additional information may be useful, such as email address (for accounts opened via an Internet product delivery channel).

Upon obtaining this information, the financial institution should, to the extent practicable and as warranted by the nature of the account, verify the accuracy of the information provided by the customer. Such verification processes can include one or more of the following:

1. Visibly compare a photograph contained on an unexpired government-issued identification (drivers license, passport, military identification, or other government identification with a photograph of the customer) with the customer to confirm that the photograph is that of the customer.
2. Obtain a U.S. government-issued identification to confirm the address, date of birth, or other information provided by the customer.
3. Obtain other identification from the customer which, while not government-issued, can be used to confirm the identification provided by the customer (such as a utility bill with customer address, expired government identification with picture, senior citizen identification, Amish or other special group identification).
4. Utilize information verification processes that either specifically verifies the information provided by the customer (such as a credit report) or generally confirm the legitimacy of the information provided by the customer (such as an anti-fraud review which has general variables used to evaluate customer information).
5. Contact the customer following the opening of the account, either by mail, telephone, electronic communication or personal visit, to confirm the customer information.
6. Other processes applicable to internet banking include customer authentication for new accounts.¹

¹ ABA’s December 2001 “Summary of Internet Banking Survey” found that the majority of banks authenticate the *identity* of a *new* customer applicant after the online application session is terminated. Three authenticate some aspects online and other aspects after the fact. Nearly all banks authenticate by comparing information to both existing bank data and consumer report data. A number of the banks verify

There are also situations where a financial institution obtains reliable, specific customer information about a customer as an integral component of the services requested, such as a fiduciary or similar account. These cases require the financial institution to document more detailed information about the customer than might be provided in traditional account opening processes for other products, allowing the institution to replace these processes with this detailed information. For example, when establishing a complex estate planning trust for a customer that requires the confirmation of a customer's source of wealth, residence and family members, it may be unnecessary for the institution to obtain a government issued identification for the creators and beneficiaries of the trust.

The financial institution should maintain a record of the processes used to verify the identification information provided by the customer. Should the information verification process reflect any discrepancies between what the customer provided and what the process disclosed, the financial institution should document what steps were taken to resolve the discrepancy.

Business Accounts

The collection of various types of identifying information and documentation and the processes for verification, as suggested below, may not be applicable to every type of customer or account. Financial institutions may conclude that based on their risk assessment of the customer and the type of services being provided that some customers (e.g., those who in the institution's view are engaged in businesses associated with money laundering) may require more extensive verification than others.

For new accounts at a financial institution opened by a business (partnership, corporation, business trust or other entity other than a sole proprietor), the institution should, at a minimum, obtain and record the following information:

1. The name of the business
2. Tax Identification Number of the business
3. Principal place of business operations
4. Mailing address of business (if different than (3))
5. Phone number of business

phone numbers, require a copy of a drivers' license or other identification, or use a third party vendor to verify information. The identities of *existing* customers' opening an account on the internet are most often authenticated by comparing application information to existing bank data. Some banks, in addition, compare the information to consumer report data. Only two use a debit card personal identification number.

6. Type of business organization (corporation, partnership, trust, other)
7. Ownership information of the business (is the business publicly held, number and/or identity of owner of privately-owned business, type of tax-exempt entity, or other information regarding the business's ownership)
8. If applicable, the website or email address of the business

Depending upon the type of account or other factors, it may be desirable for the financial institution to obtain additional information about the business, including the following:

1. Whether the business is a holding company for assets owned by affiliated organizations.
2. The primary type of activity engaged in by the business and whether its operations are primarily domestic or international.
3. For certain privately owned businesses, the information which is obtained for individual account holders.

Upon obtaining this information about the business, the financial institution should, to the extent practicable and as warranted by the nature of the account, verify the information provided by the business. Such verification can utilize one or more of the following:

1. Obtain a copy of the document confirming the existence of the business (e.g. certificate or articles of incorporation).
2. Obtain a financial statement (which may be certified) regarding the business.
3. Conduct a site visit of the place of business.
4. Utilize an independent information verification process (e.g. Dun and Bradstreet, or a credit reporting agency) to confirm the existence of the business.
5. Visit the business website or send a confirming electronic message to the business email address.
6. For privately owned businesses, perform one or more of the information verification processes regarding the information provided on behalf of the business owners.

Not every process may be applicable to every customer or account, and financial institutions may conclude that certain types of customers (for example, those who in

the institution's view are engaged in businesses associated with money laundering) may require more extensive verification than others.

The financial institution should maintain a record of the processes used to verify the identification information provided by the customer. Should the information verification process disclose any discrepancies between what the customer provided and what the verification process disclosed, the financial institution should document what steps were taken to resolve the discrepancy.

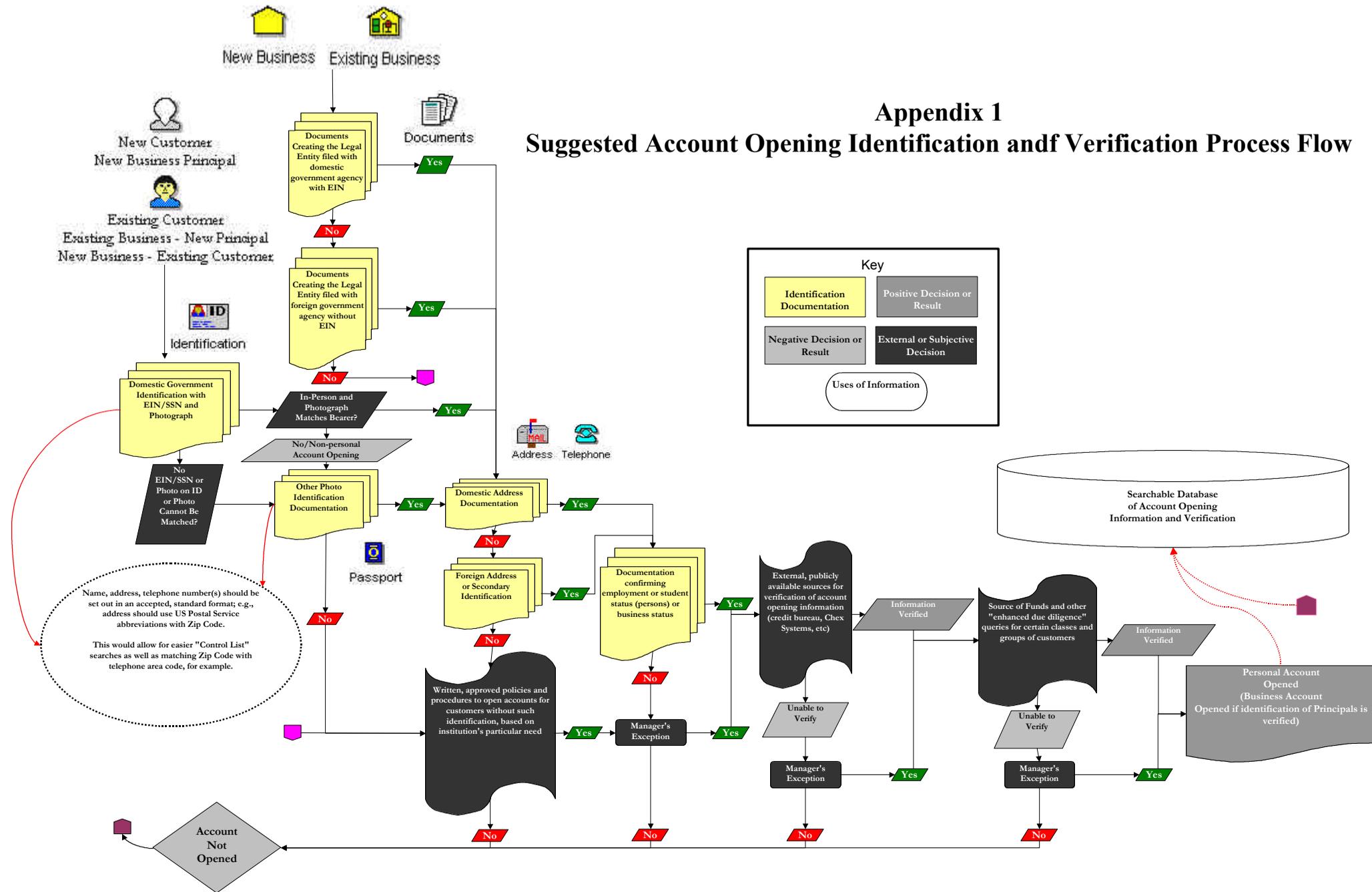
Known or Suspected Terrorists

In addition to the processes described above, it is imperative that financial institutions determine at account opening whether the potential customer is identified on any list of known or suspected terrorist suspects or organizations that may have been provided to the institution by law enforcement or other government agencies. Financial institutions must follow appropriate reporting processes as required by governing regulatory agencies if a match is identified. Financial institutions may employ automated or manual procedures for this purpose, depending upon the size of the institution and other relevant factors.

All Accounts

Financial institutions may also consider evaluating whether potential customers are on any internal list of persons who may have had previous relationships closed by the institution or an affiliate.

Appendix 1 Suggested Account Opening Identification and Verification Process Flow



The identification and verification process is designed for all new customers and existing customers seeking new products or relationships (the latter will provide a process to update old information and keep customer information current). All principals of business entities must meet the same identification and verification requirements as individual customers.

Appendix II Additional Resources*

USA Patriot Act of 2001, Section 326, Verification of Information, October 26, 2001.

Code of Federal Regulations, Part 103.28 – Financial Recordkeeping and Reporting of Currency and Foreign Transactions, Identification Required, July 1, 2001.

Comptroller's Handbook, Bank Secrecy Act/Anti-Money Laundering, December 2000, pp.19-21.

ABA Check Fraud Prevention Handbook, 1999.

ABA Internet Fraud Survey, December 2001.

ABA Summary of Internet Banking Survey by the ABA Deposit Account Fraud Committee, December 2001.

ABA New Account Opening Process Survey, October 2001.

Financial Action Task Force Special Recommendations on Terrorist Financing, October 31, 2001.

Behind the Corporate Veil, Using Corporate Entities for Illicit Purposes, Organization for Economic Cooperation and Development, 2001

Websites for Performing Online Due Diligence Reviews on Persons/Entities

<http://www.pac-info.com/> - state-by-state and global databases for corporations, business licenses, etc

<http://www.freeality.com/> - Meta search engine

<http://www.anybirthday.com/> - Birthdays

<http://www.ffiec.gov/NIC/> - National Information Center's Bank Searches

<http://www.searchbug.com/> - Search for people, addresses, telephone numbers, SSNs, Zip Codes, etc.

<http://www.carol.co.uk/index.html> - Annual reports

<http://www.corporateinformation.com/> - Corporate Information

<http://209.241.184.42/> - Nelson (Journalists' Search Engine)

<http://www.searchenginecolossus.com/> - Country-specific search engines

<http://www.invisibleweb.com/> - Searchable databases on virtually everything

<http://www.treas.gov/ofac/> - OFAC's web page with access to SDN lists

<http://www.findlaw.com/directories/reverse.html> - Reverse telephone directory

<http://www.findlaw.com/directories/phone.html> - Telephone directories

<http://uscode.house.gov/usc.htm> - U.S. Code sections

<http://www.ipl.org/ref/websearching.html> - Internet Public Library listing of web search engines

<http://www.guidestar.org/search/> - Guidestar's American charitable organizations

http://www.access.gpo.gov/su_docs/ - U.S. Government Printing Office website

<http://www.ssa.gov/search/index.htm> - Use the search term "highest group issued" to get latest SSN numbers

<http://www.bxa.doc.gov/DPL/Default.shtm> - Bureau of Export Administration's Denied Persons List

<http://www.sec.gov/edgar/searchedgar/webusers.htm> - SEC's Edgar database for company filings

* The sites listed in this have been provided as examples of verification tools that are available and are not recommended or endorsed by the American Bankers Association. Given the dynamic nature of Internet links, some of the links may have been amended since this guide was published and therefore may no longer be active.

Appendix III Account Opening Best Practices Group

<p>Dennis L. Algieri Senior Vice President Compliance The Washington Trust Company 23 Broad Street Westerly, RI 02891-0512 Tel: (401) 348-1207 Fax: (401) 348-1392 dlalgieri@washtrust.com</p>	<p>Rod Brown CEO Montecito Bank & Trust Montecito, CA 1010 State Street Santa Barbara, CA 93101 Tel: (805) 963-7511 rbrown@montecito.com</p>
<p>Susan Flynn Senior Vice President Sarasota Bank 2 North Tamiami Trail Sarasota, FL 34236-0157 Tel: (941) 955-2626 Fax: (941) 957-6474 Susan@SarasotaBank.com</p>	<p>Michael D. Kelsey Corporate Bank Secrecy Act Compliance PNC Bank, N.A. 300 Delaware Avenue, 6th Floor Wilmington, DE 19899-0791 Tel: (302) 429-1775 Fax: (302) 429-1536 Michael.Kelsey@PNCBank.com</p>
<p>James R. Richards BSA Compliance Officer FleetBoston Financial 100 Rustcraft Road Mail Code MADE22501K Dedham, MA 02026 Tel: (781) 467-2435 Fax: (781) 467-2517 James_r_Richards@fleet.com</p>	<p>Bradley Rock Chairman, President & CEO Bank of Smithtown 1 East Main Street Smithtown, NY 11787 Tel: (631) 360-9304 brock@bankofsmithtown.net</p>
<p>Richard Small Director of Global Anti-Money Laundering Citigroup, Inc. 399 Park Avenue, 5th Floor Zone 2A New York, NY 10043 Tel: (212) 793-0655 Fax: (212) 793-0735 smallr@citi.com</p>	<p>Andrew M. Zavoina, CRCM Senior Vice President Compliance Officer First National Bank Texas PO Box 937 Killeen, TX 76540-0937 Tel: (254) 554-4318 Fax: (254) 554-4289 zavoina@1stnb.com</p>
<p>ABA Contact John J. Byrne Senior Counsel and Compliance Manager Regulatory and Trust Affairs 1120 Connecticut Avenue Washington, DC 20036 Tel: (202) 663-5029 jbyrne@aba.com</p>	

Appendix IV Account Opening Best Practices Meeting

American Bankers Association

November 19, 2001

<p>Dennis L. Algieri Senior Vice President Compliance The Washington Trust Company dialgieri@washtrust.com</p>	<p>Charles Bock, Jr. Senior Vice President and Director of Fraud Prevention JP Morgan Chase Charles.bockjr@chase.com</p>
<p>Rod Brown CEO Montecito Bank & Trust rbrown@montecito.com</p>	<p>Rob Douglas CEO American Privacy Consultants, Inc. Douglas@privacytoday.com</p>
<p>Ana Foster Compliance Officer Cambridge Trust Company afoster@cambridgetrust.com</p>	<p>Pam Johnson Senior Anti-Money Laundering Coordinator Federal Reserve System</p>
<p>Michael Kelsey Corporate Bank Secrecy Act Compliance Officer PNC Bank, N.A. Michael.Kelsey@pnc.com</p>	<p>Charles Klingman Senior Financial Analyst Office of Consumer Affairs & Community Policy U.S. Department of the Treasury</p>
<p>Kathleen Kordek Vice President & Assistant General Counsel First Virginia Banks, Inc. Kkordek-fvbiawdept@att.net</p>	<p>Stuart Lehr Senior Vice President/Chief Compliance Officer Union Bank of California Stuart.Lehr@uboc.com</p>
<p>Monique Maranto Senior Vice President Bank of America Monique.maranto@bankofamerica.com</p>	<p>Carter McDowell Counsel House Financial Services Committee</p>
<p>Tom McKay Chief AML Examiner Federal Reserve Bank of New York</p>	<p>Carol Mesheske Special Activities Security Manager Federal Deposit Insurance Corporation cmesheske@fdic.gov</p>
<p>James R. Richards BSA Compliance Officer FleetBoston Financial James_r_Richards@fleet.com</p>	<p>Bradley Rock Chairman, President & CEO Bank of Smithtown brock@bankofsmithtown.net</p>
<p>David Schnorbus Chief Visa Fraud Branch Diplomatic Security Service</p>	<p>Margaret Silvers Vice President Union Bank of California Margaret.Silvers@uboc.com</p>
<p>Richard A. Small Director of Anti-Money Laundering Citigroup, Inc. smallr@citi.com</p>	<p>Dan Stipano Deputy Chief Counsel Comptroller of the Currency</p>

<p>Susan Tuccillo Citibank, N.A. Susan.tuccillo@citicorp.com</p>	<p>Brock Williams Vice President, Corporate Compliance BB&T BWWilliams@BbandT.com</p>
<p>Sherry Walsh Regulatory Risk Controls Manager First Union/Wachovia</p>	<p>Golnar Buchanan American Bankers Association gbuchana@aba.com</p>
<p>John J. Byrne American Bankers Association jbyrne@aba.com</p>	<p>Nessa Feddis American Bankers Association nfeddis@aba.com</p>
<p>Doug Johnson American Bankers Association djohnson@aba.com</p>	<p>Jim McLaughlin American Bankers Association jmclaugh@aba.com</p>
<p>Alison Watson American Bankers Association awatson@aba.com</p>	<p>Jim Chessen American Bankers Association jchessen@aba.com</p>
<p>Ed Yingling American Bankers Association eyingling@aba.com</p>	<p>Lester J. Owens Managing Director Deutsche Bank</p>
<p>Edward J. Jones Managing Director Deutsche Bank</p>	<p>Dan Soto Senior Vice President Bank of America</p>
<p>Thomas Obermaier Managing Director Deutsche Bank</p>	<p>JoAnn F. Patross ** Corporate AML/BSA Officer Mellon Financial Corporation Patross.jf@mellon.com</p>
<p>Janet Shafer Chief Passport Fraud Branch Diplomatic Security Service</p>	<p>Joe Alexander New York Clearinghouse</p>
<p>John McGrath JP Morgan Chase John.McGrath@chase.com</p>	<p>Leonard Zawistowski Senior Special Investigator Federal Reserve System Leonard.Zawistowski@frb.gov</p>
<p>Deborah Thoren-Peden ** Pillsbury Winthrop thoren@PillsburyWinthrop.com</p>	<p>Barbara McGuire ** Vice President Commerce Bank and Trust BmcGuire@cbtks.com</p>
<p>Janet Otwell** Vice President Chase Bank of Texas, N.A. Janet.otwell@chase.com</p>	<p>Deidre Weatherbee ** Corporate Compliance Officer Financial Institutions, Inc. dcweatherbee@fiwarsaw.com</p>
<p>Pam Lampe ** UMB Financial Corporation Pamela.lampe@umb.com</p>	<p>** - bankers joining by conference call</p>