THE DELAWARE BANKERS ASSOCIATION

5 E. REED STREET * SUITE 300 * P.O. BOX 781 * DOVER, DE 19903-0781
(302) 678-8600 * FAX (302) 678-5511 * www.debankers.com

38

September 6, 2002

VIA ELECTRONIC MAIL ONLY

Email: comments@fdic.gov
Executive Secretary
Attn: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429

Email: regs.comment@federalreserve.gov
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, D.C. 20551
Docket No. R-1127

Email: regs.comments@occ.treas.gov
Office of the Comptroller of the Currency
250 E Street, SW
Public Information Room, Mail Stop 1-5
Washington, D.C. 20219
Attention: Docket No. 02-11

Email: regs.comments@ots.treas.gov
Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, D.C. 20552
Attention: No. 2002-27

Re: Comments to Proposed Regulations to Implement Section 326 of the USA PATRIOT Act of 2001

Dear Ladies and Gentlemen:

The Delaware Bankers Association appreciates the opportunity to submit comments in response to the joint notice of proposed rulemaking regarding *"Customer Identification Programs for Banks, Savings Associations and Credit Unions"* (67 Fed. Reg. 48290) implementing Section 326 of the USA PATRIOT Act of 2001 (31 U.S.C. §5318(1)) ("the Act") published by the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN"), the Office of the Comptroller of the Currency, The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, The Office of Thrift Supervision and the National Credit Union Administration (hereinafter "the Agencies").

STATEMENT OF INTEREST

The Delaware Bankers Association ("DBA") is a not-for-profit, private trade association that represents thirty-nine (39) dues and tax paying financial institutions chartered to do banking business in the State of Delaware. Combined, these institutions maintain assets of almost $200 billion in the State. Accordingly, we are filing this formal response on their collective behalf and we appreciate the opportunity to comment on this important matter.

OVERVIEW

Section 326 of the Act provides that the regulations must contain certain requirements. At minimum, the regulations must require financial institutions to implement reasonable procedures for:

1. verifying the identity of any person seeking to open an account, to the extent reasonable and practicable;
2. maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and,

3. determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.

GENERAL COMMENTS

The Delaware Bankers Association strongly supports the public policy goals of the USA PATRIOT Act of 2001as a means to limit the ability of terrorists and other criminals to utilize the American banking system to promote their illegal operations. We are also pleased that the proposed regulation permits each bank to adopt "risk-based" procedures for verifying a customer's identity and that the procedures should enable the bank to form a reasonable belief that it knows the true identity of the customer. However, on behalf of our membership, we wish to make the following specific comments on common areas of concern that we believe, if implemented, will enhance the effectiveness and efficiency of bank and governmental operations related to the Act without impeding its goals.

SPECIFIC COMMENTS

DEFINITIONS

A. Definition of Accounts – 103.121 (a)(1)

The proposal defines the term "account" in the bank customer identification rules as a "formal" banking or business relationship established to provide "ongoing" services, dealings or other financial transactions. The definition, as the Agencies clarify in the preamble to the bank rules, is not intended to apply to infrequent transactions such as an occasional purchase of a money order or wire transfer. The definition of "account" in the proposed rules, however, does not appear to incorporate this necessary concept of providing "ongoing" services. The DBA recommends that the Agencies incorporate the definition of "Account" as it appears in the preamble into the final rule.

B. Definition of Customer – 103.121 (a)(3)

The proposed definition of "customer" is very problematic for many of our member banks. The proposed regulation defines the term "customer" to mean: (i) Any person seeking to open a new account; and (ii) Any signatory on the account at the time the account is opened, and any new signatory added thereafter. We have several concerns regarding the proposed definition and its implications.

Section 326 of the Act dictates that the regulations must require financial institutions to implement reasonable procedures for verifying the identity of any person seeking to open an account, to the extent reasonable and practicable. This requirement fails to provide financial institutions with sufficient flexibility in designing a customer identification program because it does not take into consideration that the risks associated with money laundering and terrorism, and to a lesser extent identity theft, are quite different depending on the type of account at issue and the relationship of the signer to the account. Further, the inclusion of "any signatory" in the definition of "Customer" will be extraordinarily costly to financial institutions, inconvenient and potentially confusing to customers and potential customers, and will likely be of little practical use to the government. The problem with the definition's blanket coverage of all authorized signatories can be demonstrated by reference to the effect on credit card, corporate and other accounts.

i. Application of the definition of "Customer" to credit card and other similar accounts

As currently drafted, clause (ii) of the definition appears to cover any additional signatory or user on a credit card or other similar account. When opening a credit card account, it is customary to obtain essential identification information about the account applicant. A credit check is done of the applicant, the address is verified, the card is sent to the billing address and the customer must activate the card. It is increasingly common for cardholders to request the addition of one or more authorized users, who most often are members of the

same household. Following such a request, the card issuer will first check the name against the government list of suspected terrorists or terrorist organizations. If the name is not on any government list, the card issuer will mail an additional card with the authorized user's name to the cardholder's address. All charges on the card are the responsibility of the cardholders.

Large credit card issuers count their customers in the millions or tens of millions. Heretofore, card issuers have not obtained identification information required by proposed Section 326 from signatories ("authorized users" in credit card terminology) such as addresses (both residential and mailing addresses), social security numbers and dates of birth, because the authorized user was not financially obligated on the account and so the credit card issuer has no need to consider them when underwriting the credit transaction. On the other hand, credit card issuers have long been required to review both obligated and non-obligated signers against the OFAC and global terrorist lists.

If signatories on credit cards are included in the definition of "Customer", then systems will have to be built to house this information, new applications will need to be designed, telemarketing scripts will need to be altered, employees retrained and additional compliance and audit controls put in place. One of our member institutions estimates the total cost of this exercise will exceed $50 million for its credit card operations alone, which does not take into consideration other lost opportunity costs. We believe that current legal requirements under OFAC and Section 314 are adequate for authorized users. This is especially true in light of the broad consensus that credit card accounts are not of high risk for money laundering. For example, in the GAO's Report to the Chairman, Permanent Subcommittee on Governmental Affairs, U.S. Senate on Money Laundering dated July, 2002, the GAO cited bank regulators, credit card industry representatives and law enforcement officials as being in agreement that credit card accounts were not likely to be used in the initial stage of money laundering when illicit cash is first placed into the financial system because the industry generally restricts cash payments. The GAO further cited a FinCEN analysis of its SARs database filed by U.S. based financial institutions as revealing very little evidence of potential money laundering through credit cards.

ii. <u>Application of the definition to corporate accounts</u>

Another example of the impropriety of considering all signatories to be Customers under the Act is related to the different risks associated with consumer and business banking accounts. In the context of Private Banking Accounts, for example, we agree that a signatory should be considered a "Customer" for purposes of Section 326 due to the nature of such accounts and the signatory's ability to move large amounts of funds into and out of the account. Conversely, insofar as the proposed regulation covers signatories on business accounts, including corporations, limited liability companies, business partnerships and trusts, the proposal is not reasonable and will result in a substantial increased burden on financial institutions and corporate customers.

The banking practice generally followed for business accounts is to obtain and rely on corporate resolutions, certificates of incumbency, authorized signature books, authenticated SWIFT messages, and, in overseas jurisdictions, corporate registries or other documentation that is customary in the local market in order to verify the authority of a signatory. In nearly all cases, the signatory has no authority to move funds into a personal account, and the business, which owns the account, maintains procedures to ensure that the account is used for business purposes. In the final analysis, banks properly view it as the corporate entity's responsibility to monitor its employees and determine who should be authorized to bind the

entity.

It is our understanding that the current procedures are adequate to reasonably determine whether an account will be used for terrorist financing or money laundering and obtaining or verifying such information for all business accounts is not warranted and unduly burdensome. Moreover, it is not unusual for business entities to have multiple accounts at financial institutions for various business purposes related to financial management, each of which may have different lists of signatories.

If financial institutions are required to obtain date of birth and residency information, taxpayer number and photo identification for every signatory on all accounts, the additional financial and operational burden on financial institutions as well as their clients will be material. The burden becomes even more apparent when one sees that the definition of "account" includes not only deposit accounts, but also every "credit account or other extension of credit" for which a person may be a signatory, even if the funds are advanced to the corporate entity and the signatory has no interest in the loan proceeds. A requirement that all such information be retained for 5 years after account closing compounds the burden even more. If this requirement remains, our member banks will have to substantially change their corporate account procedures, which will entail significant cost and delays in implementing changes in account signatories for corporate customers. There appears to be no evidence that requiring such information is an appropriate risk-based approach to customer identification for business accounts and it is inaccurate to conclude that banks already obtain the information required by the proposed regulation. This requirement bears no relation to the Section 326 requirement that the regulations require "reasonable procedures" for verifying identity "to the extent reasonable and practicable."

iii. A suggested risk-based approach

It is suggested that a reasonable risk-based approach to the "signatory" issue would be to require financial institutions to set forth in their Customer Information Programs (CIP), the circumstances under which a signatory on an account should be considered to be a customer subject to the full customer identification requirements. Since the CIP will be subject to regular review by Supervisory Agencies, questions concerning the application of the CIP to signatories can be evaluated in the context of the actual accounts maintained by the financial institution.

iv. Application to persons "seeking" to open an account

We suggest a modest change in clause (i) of the definition to make it clear that a "customer" only includes persons for whom an account is actually opened. Although the proposed language tracks the legislation, the Section-By-Section analysis expresses the correct risk-based concept that the regulation is not meant to cover a person who seeks information about an account, but does not actually open an account or a person who seeks to open an account but is denied. We suggest that the Agencies follow existing regulatory procedure requirements such as the Equal Credit Opportunity Act ("ECOA") with respect to individuals who submit an application for credit. Therefore, we recommend that, with respect to credit accounts, a person "*seeking to open a new account*" be defined as a person who has submitted an application.

v. Government Accounts

The DBA is also concerned that the proposed rule does not incorporate the same exemption

for governmental authorities that is included in other Bank Secrecy Act rules. Banks provide numerous services to state and local governments, such as handling payrolls and cash management, as well as serving in a fiduciary and agency capacities (corporate trustee, employment benefit plan trustee, paying agent, registrar, custodian, investment advisor, etc.). Governmental accounts are already subject to heavy scrutiny, and pose little risk of being used for money laundering purposes. Accordingly, the DBA urges Treasury to amend the proposal to incorporate the existing Bank Secrecy Act exemption.

IDENTITY VERIFICATION PROCEDURES

A. Identification Number and Reliance On Third Parties

Section 326 of the Act dictates that the regulations must require financial institutions to implement reasonable procedures for verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; and for maintaining records of the information used to verify the person's identity. In the preamble to the proposed regulation, the Agencies note that the legislative history of Section 326 of the Act indicates that Congress intended the verification procedures prescribed by this regulation to make use of information currently obtained by most financial institutions.

For U.S. persons, a bank must obtain a U.S. taxpayer identification number (e.g., social security number, individual taxpayer identification number, or employer identification number). We ask the Agencies to allow banks to obtain this information from a trusted third party source such as a credit-reporting agency. The heightened awareness to identify theft and fraud has generated numerous guidance and advisories to consumers. These guidance and advisories warn of the dangers associated with disclosing a social security number to anyone.

Banks are finding it increasingly difficult to convince consumers to provide their social security numbers in order to obtain a credit bureau. Until recently, the Social Security Administration website warned consumers against providing their social security number when applying for credit and stated banks could obtain a credit report without this information. Banks that use non face-to-face methods of acquisition (telemarketing, internet, mail, etc.) increasingly rely on trusted third party sources, such as a credit bureau, to provide taxpayer identification numbers. Accordingly, we ask the Agencies to recognize this dichotomy in the final rules to implement Section 326. In addition, we would like to bring to the Agencies' attention that it is not feasible to request a tax identification number on every signatory of a consumer loan or corporate account. The account belongs to the persons who are primarily liable for the debts incurred. Signatories are not obligated under the terms of the account and are added as a convenience to the account-holder. Requiring tax identification numbers for each signatory will only discourage the use of this account benefit. We ask the agencies to limit the need for tax identification number to the person or business primarily liable for the debts incurred.

DBA also urges that the Agencies permit reliance on third parties or affiliates to perform the customer identification program in the case of brokered deposits where other money managers open accounts at financial institutions. As drafted, the proposal requires a duplicative verification process. The regulation should permit financial institutions to rely on third parties or affiliates to perform customer identification under various circumstances as noted in the examples below.

i. **Intermediated Accounts.** Frequently, money management firms, brokers and other third parties open accounts at financial institutions for customer funds. Under the Act, including Section 326, these financial institutions have an obligation to obtain and verify customer

information. To avoid duplication and waste, one financial institution should be able to reasonably rely on another financial institution's verification of the customer identification information so long as that other financial institution undertakes to obtain and maintain such information.

ii. **Purchase of Accounts.** Frequently financial institutions engage in the purchase of accounts, loans or other assets from third parties. In connection with a purchase of accounts or other assets, the purchasing institution should be able to reasonably rely on representations made by the selling institution without having to undertake its own customer identification and verification investigation. The regulation should make clear that the purchase of accounts or other assets does not constitute the establishment of a new account that requires the purchasing institution to conduct a new customer identification process.

iii. **Reliance on Affiliates.** It is common for a customer to maintain several different accounts with a financial institution and its affiliates. The same customer, for example, may have a credit card account with one affiliate, a home mortgage with another affiliate and a brokerage account with a broker dealer affiliate. The regulation should make clear that the customer identification process only has to be conducted once and that affiliates may share the customer identification and verification information to the extent reasonably necessary for each entity to comply with Section 326.

B. Verification (103.121 (b) (2)

The proposed regulation provides that the Customer Identification Program must contain risk-based procedures for verifying the information that the bank obtains in accordance with 103.121 (b)(2)(i), within a reasonable period of time after the account is opened. 103.121 (b)(2)(ii)(B) Non-Documentary Verification, provides for procedures describing non-documentary methods banks may use instead of relying on documents. We ask for the agencies to provide examples of how a bank can verify passport number, alien identification card number and country of any other government-issued document through non-documentary methods. We ask the agencies to postpone this requirement until such time as the government establishes a database of information related to aliens residing in the U.S. as required in the Act. Banks that rely on "non-documentary verification" to establish a customer's identification under the requirements of the proposed rule will be at a competitive disadvantage to banks that rely on traditional face-to-face verification with documents. Banks that use "non-documentary verification" will have no source to verify the information such as passport number or alien identification number as prescribed in the proposed rule.

We also ask the Agencies to address conflicting regulatory requirements under 103.121 (b)(2)(i) when applied to signatories (authorized users) on consumer loans and business loans covered under the Fair Credit Reporting Act ("FCRA"). Banks that utilize non-documentary verification to validate a customer's identification will not be able to rely on a credit bureau for signatories. As a matter of practice, signatories are not liable for the debt incurred on the account and therefore do not provide authorization to obtain a credit report. Banks utilizing a non-documentary verification method would incur significant cost and burden to obtain authorization to obtain a credit bureau from all signatories on an account. Banks with non face-to-face operations will be placed at a competitive disadvantage with those having face-to-face operations.

We ask the Agencies to consider the impact of using non-documentary verification when implementing the requirements under 103.121 (b)(2)(iii) - Lack of Verification. If a bank uses the service of trusted third party source other than a credit bureau and denies an application based on that third party source, does that source become a credit-reporting agency? We ask the Agencies to provide clarification on this issue.

RECORDKEEPING – 103.121 (b)(3)

A. Photo Identification

One of the most problematic items in this proposal is the requirement that banks keep a copy of the photo identification ("ID") used to verify the customer's identity. For years, banks have been training employees to NOT obtain the copy of the photo ID for risk of violating, or being accused of violating ECOA. A violation of this sort has serious regulatory and reputational risks attached to it and is to be avoided at all costs. In addition, with the increasing consumer awareness of identity theft, customers may be very reluctant to provide such identification. Also, many customers do not have photo identification because they do not drive and live in states that do not provide photo IDs for non-drivers. An about-face by the industry now would cause supreme confusion among customer service personnel, possibly resulting in violations of ECOA, the Act, or both. Costs to provide adequate and on-going training to prevent violations of these requirements is expensive and not always successful.

Furthermore, due to the difficulty of obtaining photocopies in all locations, many banks are moving away from paper-based records. The generally accepted practice in the industry for reviewing/documenting photo ID is to record the issuing authority, either state or country, etc., and the number of the documentation.

B. Record Retention

Another significant issue related to the proposed regulation is the maintenance of documents, including the photo IDs, for up to five years after the account relationship has ended. The five-year record retention requirement will be excessive and costly, not to mention cumbersome to maintain and store items in an easily accessible centralized location. It appears that retention of such documents for up to two years after the account has been closed is more efficient and would parallel the regulations covering electronic funds transfers, consumer leasing, Truth-in-Lending and Truth-in-Savings, and would be one month less than the requirements contained in ECOA.

Also, under the records to be covered under this section, the DBA strongly encourages Treasury to clarify that individuals who seek to open an account, but are declined, for whatever reason, not be considered customers. Therefore, no records with respect to these individuals would be required to be retained under the rule.

EFFECTIVE DATE/IMPLEMENTATION

Although Section 326 states that the Rule must be effective by October 25, 2002, this timeframe is unrealistic -- particularly in light of already scheduled year-end demand on management information technology such as the preparation of year-end statements. The proposed record-keeping requirements with respect to copying and storing the identifying information provided by the customer will impact significantly financial institutions' operations and data storage facilities. More time is needed to implement the necessary changes.

Additionally, financial institutions will need time to amend their formal Bank Secrecy Act policies and anti-money laundering compliance programs -- especially in light of seeking approval by their boards of directors. Finally, more time will be needed to develop compliance education programs and training for front-line customer service personnel.

Based on the issues addressed above, the DBA urges the Agencies to consider a one-year phased-in implementation period for all portions of this section.

CONCLUSION

The Delaware Bankers Association strongly supports the goals of Section 326 of the Act to combat terrorism. Our Delaware banks, as well as financial institutions throughout the country, have been diligently working hard to assure that they are in compliance with existing laws to address terrorist financing and will continue to do so. However, we believe that our recommendations will provide more effective and efficient methods to assist them in working with the government in further inhibiting terrorist activities in our country.

Thank you for the opportunity to present our comments. If we can assist you in any way, please do not hesitate to contact me at 302-678-8600 or via email at David.Bakerian@debankers.com.

Sincerely,

David G. Bakerian
David G. Bakerian
Executive Vice President