

September 6, 2002

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington DC 20552
Attn: No. 2002-27

DELIVERED ELECTRONICALLY

To whom it may concern:

This comment letter is filed on behalf of FDS Bank ("FDS") in response to the Office of Thrift Supervision's ("OTS") proposed rule implementing Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act") ("Proposal"). FDS commends the OTS for its efforts to implement the PATRIOT Act and appreciates the opportunity to comment on the Proposal.

Background

FDS is a member of the Federated Department Stores, Inc. family of companies. FDS issues private label credit cards for use solely at merchants that are members of the Federated Department Stores, Inc. corporate family ("Federated"), which include Macy's, Rich's, Lazarus, Goldsmith's, Burdines, the Bon Marché, and Bloomingdale's. FDS also issues VISA cards, which may be used at any merchant that accepts VISA payment cards. FDS uses several methods to accept applications for its private label and general purpose cards, including at the point of sale, through the mail, through the Internet, over the phone, and through use of "prescreening" and providing firm offers of credit. FDS receives approximately 5 million applications a year for private label and general purpose credit cards.

In General

Section 326 of the PATRIOT Act requires the Secretary of the Treasury to prescribe regulations establishing minimum standards for financial institutions regarding the identity of their customers. The regulations must require financial institutions to implement reasonable procedures for verifying a customer's identity, maintaining records of the information used to verify the customer's identity, and consulting certain government lists to ensure the customer does not appear on any of them. The Proposal, in turn, requires each bank¹ to establish a "Customer Identification Program" ("CIP") that includes the components of the Proposal.

¹ As in the Proposal, use of the term "bank" in this discussion includes all federally regulated depository institutions, including thrifts.

FDS believes that the report language contained in House Report 107-250, Part I (the "Report"), which includes the House Financial Services Committee's explanation of the precursor to Section 326,² is instructive of how the OTS should implement Section 326. For example, the Report states that it is the intention of the Committee that "the regulations prescribed under [Section 326]...impose requirements appropriate to the size, location, and type of business of an institution." We are pleased that the OTS has incorporated this guidance and intends to allow flexibility for a bank to establish a CIP "tailored to the bank's size, location and type of business." FDS commends the OTS for recognizing that no single CIP would be appropriate for each bank. Indeed, a bank that receives millions of applications a year, most through the point of sale, should have a CIP that varies from a small community bank that opens far fewer accounts primarily in face-to-face transactions. We urge the OTS to maintain this flexibility for banks in any final rule implementing Section 326 ("Final Rule").

The Report is also instructive in another critical area. In connection with the identification verification and the recordkeeping provisions of Section 326, the Report states that the "procedures prescribed by Treasury make use of information currently obtained by most financial institutions in the account opening process. It is not the Committee's intent for the regulations to require verification procedures that are prohibitively expensive or impractical." We believe that the OTS has attempted to craft the Proposal in a manner that coincides with the clear congressional intent so that it does not unnecessarily alter existing business practices. For example, the OTS states that the "basic information that banks would be required to obtain under [the Proposal] reflects the type of information that financial institutions currently obtain in the account-opening process." FDS believes that this is the most appropriate approach for the OTS to take, and urges the OTS to maintain this perspective as it develops a Final Rule. In this regard, as a general matter, current industry practices already provide financial institutions with a reasonable belief that they know the identity of those who hold an account with them. Therefore, we believe that changes to current practices are not justified unless such practices clearly do not meet the statutory objectives: identification verification, accurate recordkeeping, and consulting the appropriate government lists. We offer the following specific comments with this in mind.

Definition of "Customer"

Under the Proposal, a bank's obligations relate to determining the identity of its "customers." For example, the Proposal states that a bank's CIP must include procedures for verifying the identity of each "customer," to the extent reasonable and practicable. Furthermore, a bank's CIP must contain "procedures for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of a customer." Therefore, the definition of a "customer" is a key element establishing the scope of the Proposal with respect to whom a bank must identify.

"Seeking to Open a New Account"

² The origins of Section 326 can be found in Section 123 of H.R. 3004, as passed by the House of Representatives. Although there is no House or Senate report associated with H.R. 3162 (enacted as the PATRIOT Act), House Report 107-250, Part I clearly reflects the congressional intent of the language in Section 326 of the PATRIOT Act.

The Proposal includes in the definition of a customer “any person seeking to open a new account.” The Supplementary Information accompanying the Proposal notes that this portion of the definition includes an individual applying for an account but would not cover a person simply seeking information about an account. We agree that it would be inappropriate for a bank to verify the identification of an individual who is seeking only information about an account, but not applying for one. This distinction may be more clear if the definition of the term “customer” is amended to omit reference to an individual “seeking” to open a new account, and refers instead to an individual “applying” to open a new account. We believe this change would provide more clarity while remaining true to the statutory requirement that the bank verify the identification of an individual seeking to open a new account.

Signatories

A “signatory” to an account is also deemed to be a customer of a bank under the Proposal. Although the term “signatory” is not defined in the Proposal, the Supplementary Information adds that “an individual with signing authority over a corporate account is a” signatory for purposes of the Proposal. FDS requests that the OTS provide some clarification with respect to how the term “signatory” is to be interpreted for purposes of the Proposal.

FDS believes that *Black’s Law Dictionary* provides an appropriate definition of “signatory,” meaning “a party that signs a document, personally or via an agent, and thereby becomes a party to an agreement.” This definition would capture those individuals who should be covered by the Final Rule, that is, customers of the bank. In this regard, we believe that only those people who have a relationship with the bank itself, *i.e.* are a party to the account agreement and liable thereunder, should be deemed to be customers.

FDS urges the OTS to clarify that an individual must have some level of authority or obligation, *i.e.* that they are a party to the account agreement, in order to become a signatory under the Proposal. This clarification is critical for FDS and other banks in the context of how the Final Rule will apply to authorized users of credit card or other accounts. For example, FDS may issue a credit card to an individual for which the individual becomes liable. As part of the issuing process, FDS will require identification information, evidence of creditworthiness (*e.g.* a consumer report), and a contractual commitment from the individual that he or she will repay any debt incurred through the account. This information will also be of use in connection with FDS’s CIP obligations, as envisioned in the Proposal.

As a convenience to its customers, FDS, like many banks, allows its customers to add authorized users to their credit card accounts. Generally, an authorized user is provided with a credit card bearing his or her name and the ability to use the credit card in much the same way the account holder may. However, an authorized user is not obligated under the account agreement, does not become party to any agreement with FDS, and has no legal authority with respect to the account itself. In other words, *an authorized user is not a customer of the bank.* We respectfully urge the OTS to recognize this distinction explicitly.

If an authorized user is deemed to be a signatory, and therefore a customer of the bank, under the Final Rule, we believe that account holders will be unnecessarily inconvenienced since

many banks (including FDS) may not be able to allow authorized users on an account and still be able to comply with the Final Rule. In this regard, FDS is similar to most of the industry in that we currently collect only the name of the individual who is to become an authorized user. In order to meet its obligations as outlined in the Proposal, FDS would need to obtain additional information it does not currently collect if an authorized user were considered a signatory. Such a result would deviate from the stated congressional intent, that “the procedures make use of information currently obtained by most financial institutions in the account opening process,” and would require significant systems changes.

Identification Verification

The Proposal requires a bank’s CIP to contain procedures describing when the bank will verify a customer’s identity through use of documents and setting forth the documents that the bank will use for this purpose. The CIP must also contain procedures that describe non-documentary methods the bank will use to verify a customer’s identity and when these methods will be used in addition to, or instead of, relying on documents. The Proposal states that the CIP must address situations, among others, where the account “is not opened in a face-to-face” transaction, or the account is opened without obtaining documents.

Face-to-Face/In Person Transactions

FDS receives a majority of its applications for credit at the point of sale. For example, a customer will be purchasing products in one of our affiliated retail outlets and may apply for a credit card issued by FDS as part of the checkout process. The customer may complete an application at the register, and the information is transmitted to FDS for purposes of determining whether to extend credit. In most instances, FDS’s decision is communicated back to the customer almost immediately, while he or she is still at the cash register. Although the customer may be physically present in our affiliate’s store, the customer is not transacting directly with any employee of the bank.

We raise this issue in light of some of the comments included in the Supplementary Information and the Proposal itself. Specifically, there are portions of the verification process that the OTS suggests may be done differently depending on whether the customer is “face-to-face” with the bank, or “physically present” in the bank. This is undoubtedly true. However, we urge the OTS to recognize and clarify that simply because a customer may be face-to-face with a store clerk, that customer is not necessarily transacting directly with the bank. Therefore, a bank’s CIP or compliance with the Final Rule should not be evaluated as though such transactions were face-to-face.

Information Required

A bank’s CIP must contain procedures that specify the identifying information that the bank must obtain from each customer. Included in the identifying information required under the Proposal is a residential address, if it is different from the mailing address. FDS believes that a customer’s address can be an important tool in verifying the customer’s identity. However, we do not believe that it is appropriate to require a bank to obtain two addresses for a customer if the

bank is able to form a reasonable belief that it knows the true identity of its customer using only one. We raise this issue because, like many banks, FDS generally obtains only a single address from a customer in connection with an account application. In order to obtain and record a second address, FDS would need to redesign its account opening procedures and information management systems. We respectfully submit that the relatively large costs incurred as a result of this requirement are not justified if the bank can otherwise form a reasonable belief that it knows the true identity of its customer without collecting a second address. Furthermore, we do not believe the significant changes that would be required by this provision were envisioned by Congress when it expressed its intent that the Final Rule should make use of the existing information obtained in the account opening process and should not require procedures that are prohibitively expensive or impractical.

Verification: Methods

We commend the OTS for allowing a bank's CIP to use a variety of methods to verify a customer's identity. One verification method that may be appropriate for a face-to-face transaction may not be appropriate for an application taken over the Internet. Indeed, even similar types of transactions may require different verification methods depending on the customer. For example, the OTS notes that even in face-to-face transactions, obtaining a photo identification may not be possible with respect to all customers. It is important for the OTS to maintain this flexible approach in the Final Rule in order to ensure that banks are able to develop appropriate verification methods depending on the characteristics of the accounts, the methods of opening such accounts, and the customers themselves.

FDS believes that it is of particular importance for the OTS to maintain in the Final Rule the provision indicating that an account may be opened without reviewing documents.³ As noted above, regardless of how an account may be opened, a customer may not be able to provide photo identification for one of many legitimate reasons. We believe that the Proposal correctly focuses on the fact that a bank must obtain a reasonable belief that it knows the identity of its customer, not on the specific methods the bank uses to obtain that belief. This focus should be retained in the Final Rule.

The Proposal includes a requirement that a bank's non-documentary verification procedures address situations where "the account is not opened face-to-face." Again, we simply note that a point-of-sale transaction is likely to be treated in a manner different than those transactions where the customer is face to face with a bank employee. It is our hope the OTS recognizes this distinction.

Recordkeeping

Section 326 of the PATRIOT Act requires the Secretary of the Treasury to establish "reasonable procedures for...maintaining records of the information used to verify a person's identity, including name, address, and other identifying information." We support efforts to

³ The OTS appears to use the term "documents" to refer to means of personal identification. For example, unexpired government-issued identification is the sole example provided of a "document" to be used in the verification process as it relates to individuals.

establish procedures for maintaining appropriate records in connection with a bank's verification procedures.

The Proposal requires a bank to maintain a record of: (i) the minimum identification required by the Proposal; (ii) a copy of any document that was relied on pursuant to the bank's documentary verification procedures that clearly evidences the type of document and any identification number it may contain; (iii) the methods and result of any measures undertaken to verify the customer's identity pursuant to the bank's non-documentary verification efforts; and (iv) the resolution of any discrepancy in the identifying information obtained. The bank must retain all records for five years after the date the account is closed.

Information to Be Retained

FDS supports the need to maintain appropriate records which evidence a bank's compliance with Section 326. We believe the most appropriate approach for keeping verification records would be to require banks to retain the information used to verify a customer's identity in addition to descriptions of the procedures used to verify a customer's identity. This would allow banks to maintain adequate records without requiring millions of redundant *individual files* describing how that customer's identity was verified, or how each discrepancy was resolved. Furthermore, such an approach is consistent with the framework established in the Proposal, requiring banks to collect specific information and to develop policies as to how a customer's identity would be verified. If this approach were taken, the bank and the OTS will have access to specific information used to verify a particular customer's identity and a description of the procedures used by the bank to verify the identity.

Although the statute requires a bank to maintain a record of only that information which was used to verify a person's identity, the Proposal would require banks to retain additional information. For example, the Proposal appears to assume that the bank will rely on *all* of the information it collects as required by the Proposal. This is not necessarily true. It may be that a bank need not rely on the individual's date of birth to verify his or her identity in some situations. Therefore, based on the plain language of the statute, the bank should not be required to maintain a record of such information.

OTS proposes to require a bank to retain a copy of any document the bank used as part of its verification procedures. We believe that this requirement may discourage many banks from relying on government-issued identification bearing a photograph if, in so doing, the bank would obligate itself to maintain a copy of the identification. In this regard, as OTS has acknowledged, it is possible for a bank to form a reasonable belief that it knows the true identity of its customer without relying on documentary evidence. If the OTS imposes the additional costs of making a copy of the identification, and storing it, banks may have little choice but to rely on other methods of verification. We also note that banks such as FDS would be forced to stop asking for photo identification as part of account-opening transactions at the point of sale (and rely strictly on non-documentary verification techniques), or cease to provide customers the opportunity to obtain credit at the point of sale altogether, if the store clerk must find a working photocopier each time a customer applies for an account. We note that Federated has approximately 32,000 cash registers and few, if any, of those registers are located in proximity to photocopiers. We

believe that a combination of non-documentary verification methods *and* a store clerk's confirmation that the person's identification information matches that on his or her government-issued identification document is an acceptable method to verify customers' identities. We urge this practice not be made unworkable by requiring a photocopy of each identification document.

The Proposal also requires the bank to maintain the "methods and result of any measures undertaken to verify the identity of the customer" pursuant to non-documentary methods. FDS respectfully suggests that this requirement does not correspond with any provision in Section 326 of the PATRIOT Act. The methods and results of identification verification are distinctly different from the information used to verify the identity, and therefore a bank should not be required to maintain such a record. Furthermore, the substance of this requirement is already addressed in the Proposal since banks are required to have a written description of the specific methods used to verify a customer's identity depending on how the application was received and the type of account sought. The results of such procedures will also become obvious depending on whether the account was maintained or whether the bank took other appropriate action under its CIP to address those situations when the bank cannot form a reasonable belief that it knows the true identity of its customer.

The OTS also intends banks to maintain a record of the resolution of any discrepancy in the identifying information obtained. Again, we respectfully submit that this information is not the type of information Congress intended banks to retain. Furthermore, the resolution of any discrepancy is likely to be simply whether an account was opened for the customer or not. We are especially concerned that this provision creates an expectation that the bank note any identification "discrepancy" and attempt to resolve it. For example, a customer may state his name as "John Doe" on the application. The consumer report used in the verification process may list the individual's name as "Jonathan F. Doe" at the same address and having the same social security number. Or perhaps the consumer report indicates that Mr. Doe lives at "123 Main Street" but Mr. Doe's application states only "123 Main." We do not believe that these "discrepancies" are noteworthy enough to warrant an investigation and resolution, much less a record of it.

The result of the Proposal's requirement to keep a record of a variety of information not used to verify the identity of the customer, and copies of documents not currently made today, would result in excessive recordkeeping burdens. Retaining the records contemplated in the Proposal would create significant systems changes for most banks, including FDS. We do not believe that such a result was intended by Congress, and we therefore urge the OTS to amend the recordkeeping requirements to include only that information used by the bank to verify the customer's identity.

Length of Time a Record Must Be Kept

A bank's CIP must include provisions for retaining the required records for five years after the date the account is closed. Although FDS understands the need to retain identification information for a reasonable period of time, we believe that the record retention period specified in the Proposal would be unnecessarily long. For example, it is not uncommon for a customer to have a relationship with us for 20 years or more. The Proposal would require a bank to maintain

the verification records for such a customer for 25 years. Furthermore, in light of technology advances, systems changes, etc., records may not be readily accessible after such a period of time unless FDS were required either to maintain *paper* copies of them or to reformat such electronic records to keep up with technological changes continually over the duration of the account relationship plus five years.⁴

In order for the Final Rule to impose an effective, more manageable requirement on banks, FDS urges the OTS to amend the record retention requirement. We believe that a requirement to maintain the information used to verify the customer's identity for two years after the account is opened would create a more manageable obligation on banks without sacrificing the benefits the records provide. In this regard, a two-year retention period would allow examiners the opportunity to evaluate a bank's compliance with the Final Rule and its own CIP. This time period will also allow a bank's own required anti-money laundering compliance audit procedures to determine whether it is complying with the Final Rule and its own CIP. Furthermore, if the bank continues to hold the account after the two-year period, it will continue to have the information needed by the OTS or law enforcement (*e.g.* name, address, account number, etc.) in connection with examinations or investigations. We believe that this information is likely to be of more use than information that may have been used several years prior and that may not be current.

Notice

The statute requires Treasury to issue regulations that "at a minimum, require...customers (after being given adequate notice) to comply with" reasonable customer identification procedures. In other words, the statute states that the Proposal should require customers to comply with identification procedures after they receive notice that such procedures are being used and that they must comply with them. However, the OTS has omitted the requirement for customers to comply with the identification requirements while retaining the notion that banks should notify customers that identification verification procedures will be used. Specifically, the Proposal requires a bank's CIP to include procedures for providing bank customers with adequate notice that the bank is requesting information to verify their identity. According to the Supplementary Information, such notice may take the form of a sign in a bank lobby or any other form of written or oral notice.

We believe that a plain reading of the statute requires the Secretary of the Treasury to require customers to comply with the reasonable procedures outlined in the Proposal. Such a requirement would be consistent with other situations where the Secretary of the Treasury has required compliance by individuals in connection with anti-money laundering efforts (*e.g.* reporting an interest in a foreign account). Furthermore, we believe that the phrase "after being given adequate notice" must be read in the context of the requirement that the customer comply with the identification verification procedures. In other words, the notice requirement exists only in the context of customers having statutory obligations—*it appears that Congress did not intend*

⁴ The Proposal's compliance burdens increase exponentially if FDS were required to maintain paper copies of the identification information, or reformat the electronically stored information continually throughout the life of an account. We do not believe this is OTS's intent.

to impose legal obligations on bank customers (i.e. to comply with identification verification procedures) without making them aware of the obligation.

Since the Proposal has omitted the statutory requirement that customers comply with the identification verification procedures, FDS does not believe that it is necessary to provide notice to customers that FDS will verify their identities. In the absence of a legal obligation to comply with verification obligations, requiring a bank to notify a customer that it will verify the customer's identity assumes either that the customer is not already aware that such verification is taking place when an account is opened or that the customer would object to such verification. This simply cannot be the case. A customer naturally expects that a bank will make an effort to verify his or her identity in connection with opening an account—in fact, as the OTS notes in the Supplementary Information, banks already request and verify identification information in connection with opening an account. The customer's expectation that this will occur has perhaps even heightened given the general concerns about identity theft and related fraud. Furthermore, it is extremely unlikely that a customer would object to verifying his or her identification and therefore halt the account opening process. In the end, such a notice does not appear to be justified unless it is provided in connection with a customer being obligated to comply with the identification verification procedures.

If the OTS nonetheless retains the notice requirement in the Final Rule, we urge the OTS to keep the general approach it has taken with respect to delivery of the notice in the Proposal. In particular, FDS will not be able to post a sign in a branch or at each of the 32,000 cash registers in use by Federated in order to provide customers with the notice, and will therefore need to rely on the ability to provide notice through other written or oral communications. Therefore, we strongly urge OTS to retain the guidance permitting notice to be provided in another written or oral form in the Final Rule. We also urge the OTS to modify the Supplementary Information to clarify that a bank may provide the notice electronically if the customer communicates information electronically to the bank in connection with the opening of an account, and not just in instances when the account is opened electronically. For example, if the customer provides information via the Internet, but the account is not actually opened through the Internet, the bank should still be able to provide the notice electronically.

Compliance Date

The OTS notes that, by statute, the regulations implementing Section 326 of the PATRIOT Act must be effective by October 25, 2002. It should be obvious that banks, including FDS, would not be able to develop a CIP, have it approved by their respective boards of directors, and have it implemented by October 25, 2002. For this reason, we request the OTS to allow banks adequate time to develop and implement a CIP before compliance with the Final Rule is required. Aside from determining the verification procedures that should be undertaken for the different types of accounts opened and the methods for opening them, FDS would also likely need to amend its applications, alter its current systems requirements, and redesign its recordkeeping procedures. In order to accomplish this task, we believe, based on our initial evaluation of the Proposal, that FDS could need up to 12 months once a Final Rule is published to develop and implement a CIP that meets the requirements of the Proposal.⁵

⁵ Amendments to the Proposal may also shorten or lengthen the time needed to comply.

Conclusion

FDS again thanks the OTS for the opportunity to comment on this important Proposal. We appreciate the OTS's apparent effort to develop a Proposal that remains true to the statutory requirements of Section 326 without creating unreasonable or impractical requirements for banks. We hope that our suggestions will assist the OTS in meeting this goal. If we may be of further assistance in this matter, or if you have any questions regarding this letter, please do not hesitate to contact me at (513) 579-7870.

Sincerely,

[signed]

Ellen R. Dugan
Secretary, FDS Bank
9111 Duke Boulevard
Mason, OH 45040