AFSA
American Financial Services Association

30

September 6, 2002

Office of the Comptroller of the Currency
250 E Street, SW
Public Information Room
Mailstop 1-5
Washington DC 20219

Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

RE: Docket No. 02-11 (Comptroller), R-1127 (Board), 2002-27 (OTS).

Gentlemen and Ladies:

The American Financial Services Association ("AFSA") appreciates the opportunity to comment on the customer identity verification rule (the "Proposed Rule"), 67 Fed. Reg. 48290-48299 (July 23, 2002), recently proposed by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of Thrift Supervision (collectively, the "Agencies"), together with the Financial Crimes Enforcement Network of the Department of the Treasury ("FinCEN"), implementing the Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT"), Pub. L. 107-56 (October 26, 2001). The Proposed Rule would apply Section 326 of USA PATRIOT to banks.

We strongly support the goals of USA PATRIOT, which the Proposed Rule paraphrases as "facilitat[ing] the prevention, detection and prosecution of international money laundering and the financing of terrorism." Proposed Rule at 48291. We appreciate the enormous effort that the Agencies have put into crafting the numerous rules required to implement USA PATRIOT without imposing overwhelming new compliance responsibilities on the financial services

industry, particularly in light of the compressed implementation schedule laid down by Congress. It is with the intention of alerting the Agencies to the possible unintended effects of the final Section 326 regulation, which may include the chilling of credit practices important to U.S. consumers and the imposition of significant compliance costs without achieving significant results, that we write to comment on the Proposed Rule.

Our comments concern the possible effects of the Proposed Rule on credit card lending, both in general and with special reference to the practice of granting such credit instantly at the point of sale. Section 326 requires that regulations establish "reasonable procedures for ... verifying the identity of any person seeking to open an account [with a financial institution] to the extent reasonable and practicable." Pub. L. 107-56, Sec. 326(a), *codified at* 31 U.S.C. 5318(*l*)(2)(A). Credit cards are different from other financial products and services in many respects, and these differences should be taken into account in order to establish procedures that are reasonable and practicable for verifying the identity of credit card account holders. We therefore respectfully request that the Agencies consider making changes to the Proposed Rule that would:

- Establish a flexible, risk-based rule allowing credit card lenders to choose the data they will gather in connection with verifying the identity of applicants for credit card accounts;
- Limit the data gathering requirement to persons who actually open a credit card account;
- Preserve credit card lenders' ability to offer instant credit at the point of sale;
- Establish reasonable record-keeping requirements;
- Specify the government lists that credit card lenders must consult; and
- Give credit card lenders enough time to implement the new regulatory requirements to be able to avoid severe economic dislocation.

We discuss our proposed changes in greater detail below, after a summary of credit card lending that highlights the practices that we think the final Section 326 regulation should take into account.

Credit Card Lending

Credit card lending is of particular concern to AFSA because it constitutes a significant part of the business of our members – and a significant aspect of American consumer financial services. We represent diversified financial services companies, automotive finance companies, consumer finance companies, mortgage companies, commercial finance companies, credit card issuers and merchandise and department store retailers with significant financial businesses. Many of our members issue credit cards in one or both of the two most important forms:

- bank cards, linked to a credit card network such as Mastercard or Visa and usable to purchase goods and services from many merchants; and

- private-label credit cards, issued in the name of a merchant by a bank (which may or may not be affiliated with the merchant) and usable to purchase goods and services only from that merchant and its business partners.

Individuals and small businesses establish credit card accounts with our members through a wide variety of channels, including telephone applications, mail-in applications, and Internet applications. Moreover, millions of applications each year are made at the point of sale. Through credit card accounts established by these methods, our members provide most of the unsecured credit that American consumers routinely use.

Because credit card lenders usually do not provide this credit face-to-face, they generally have little direct contact with their customers. This is not universally true, of course. Some credit card lenders have significant non-credit card financial businesses, but even these more diversified financial services providers tend to conduct their credit card business through channels that have a relatively small "bricks and mortar" component. The competitive pressures associated with credit card lending mean that the systems involved in making credit card accounts available – including the customer identity verification systems – are more similar to one another than to the systems used in connection with other financial products and services. Because the issues raised by looking at the Proposed Rule from the perspective of credit card lending are so widely shared by all credit card lenders, we do not seek to differentiate between monoline credit card banks, diversified financial services providers that have credit card divisions, and the range of financial institutions in between. In this letter, we use the term "credit card lender" to denote the credit card lending operations of a bank.

Credit card lending is a wholesale business, whose administrative processes respond to the fundamental business need to keep direct, individualized customer interactions to a minimum. Soliciting and receiving new customer inquiries, underwriting account applications and granting credit are all automated to the maximum degree possible. Several of our members process more than one million applications per month, suggesting how strong the incentives are for credit card lenders to minimize human intervention in order to preserve data integrity and realize economies of scale. When direct customer service is required, credit card lenders leave as much as possible to the institutions that already deal with customers directly – such as the merchant who accepts an application for instant credit card approval at the point of sale. This has allowed our members to be remarkably efficient, and American consumers and small businesses have reaped the benefits of this efficiency in the form of low credit costs and easy access to credit, including sales financing. Underlying that efficiency, however, is the fact that our members use their automated systems to analyze discrepancies between the limited data they collect from consumers and the more complete data they obtain from trusted third parties, rather than to collect additional data directly from consumers.

Point-of-Sale Transactions

An example may clarify this important point. From the Proposed Rule itself, as well as conversations we have had with Treasury Department officials, we are aware that the Agencies consider "accounts designed to allow a customer to transact business immediately" to raise certain concerns in connection with the goals of USA PATRIOT. Proposed Rule at 48296 (Request for Comment No. 2). We think that this may arise out of the belief that applications for instant credit are subject to less scrutiny than applications for credit not intended to be used immediately. In our experience, however, credit card lenders treat all applications for credit basically alike. The steps a credit card lender goes through in granting instant credit at the point of sale give a good illustration of the characteristics of all credit card lending that the final Section 326 regulation should take into account.

Our members typically provide instant credit through private label credit card arrangements with retailers and other merchants. A merchant offers a consumer who is making a purchase the opportunity to open a credit card account, which the consumer can use to finance that purchase and any future purchases from the merchant. The credit card account generally is provided by one of our members under a private label credit card arrangement. The merchant may assist in resolving customer problems arising out of the use of the card, but the credit card lender actually underwrites and extends the credit, and the credit card lender generally incurs the risk of credit loss based on the standards used to underwrite the card.[1]

The in-store account opening process is highly automated and permits merchant employees with minimal training to perform all activities necessary to open the account in conjunction with processing the consumer's retail purchase. In virtually all instances, when a consumer seeks to open an account at the point of sale, a store clerk takes application information from the consumer and communicates that information to the credit card lender electronically. Within a short period of time, the credit card lender receives the information and matches it to a credit report and/or other information obtained from a trusted third party. The credit card lender verifies the consumer's identity by comparing the application information with the information it has obtained, evaluating similarities and discrepancies according to pre-established analytical criteria. Simultaneously, the credit card lender performs other anti-fraud routines, which if possible include an instant check of the consumer's name against the Office of Foreign Assets Control ("OFAC") list of specially designated nationals prohibited from receiving financial services under Executive Order 13224. If such an instant check against the OFAC list is not possible because of systems constraints, the bank "batches" the consumer's name with those of other applicants, running a comparison of new customer names against the OFAC list at regular intervals. (A number of our members have received assurances from OFAC that batching is permissible as a method of complying with the requirements of Executive Order 13224 and similar asset-freeze requirements in connection with all new accounts, not merely instant credit

[1] The merchant may be responsible for losses due to the merchant's failure to live up to its responsibilities under the arrangement, or for losses related to quality of the goods or services sold.

arrangements.) The credit card lender then evaluates creditworthiness and, if appropriate under the underwriting and fraud guidelines applicable to the specific credit program, approves an instant extension of credit to the consumer, usually to finance a purchase the consumer wishes to make at that time.

This is essentially the same process that other applications for credit cards – whether for bank cards or private label credit cards, and whether in response to telephone applications, mailed-in applications provided through direct mail solicitations, or Internet applications – all follow. The credit card lender's primary underwriting activities are (1) the automated evaluation of the consistency of an applicant's self-reported information with the information available from large, computerized databases such as those of the credit reporting agencies, and (2) the equally automated credit analysis of the applicant's credit report or credit score. The credit card lender's decision to grant credit is thus instantaneous and automated, regardless of the channel through which the application reaches the credit card lender. The only significant difference between the channels lies in how the information arrives at the credit card lender to be evaluated, not the speed or the outcome of the evaluation.

Credit card lenders developed these procedures in order to minimize fraud, assure payment for authorized charges and maintain customer relationships, motivated by the natural desire to ensure that the credit they granted would be repaid. They did not develop procedures specifically to deny terrorists and other money launderers access to revolving credit. Even so, the systems that credit card lenders have established for their own business purposes incorporate highly reliable and cost-effective customer identity verification procedures that can serve the purpose of compliance with credit card lenders' Section 326 responsibilities in connection with the opening of credit card accounts. Indeed, because credit card lenders have business incentives to continually improve their procedures to combat ever-changing fraud challenges – including identity theft – relying on credit card lenders' existing systems for Section 326 compliance aligns the credit card lenders' private interests with their regulatory responsibilities. This is only possible, however, if it is clear that the existing industry-standard account opening procedures and systems are a permissible way for credit card lenders to comply with the requirement to establish a reasonable belief that their customers are who they claim to be.

Permit Flexible, Risk-Based Data Gathering and Verification Policies

The final Section 326 regulation should make clear – in the regulation itself as well as the supplementary materials – that a bank's customer identity verification procedures can and should take into account the special characteristics of the bank's business. Section 326 itself, as the supplementary information to the Proposed Rule notes, "states that the [identity verification] procedures must be both reasonable and practicable." Proposed Rule at 48293. The supplementary information for the Proposed Rule suggests that a bank can establish a Customer Information Program ("CIP") "appropriate given the bank's size, location and *type of business*." Proposed Rule at 48292 (emphasis added). This appears to us to be the single most important principle for a Section 326 regulation to embody, and it must be clearly and consistently stated

throughout the regulation. The nature of a bank's predominant business activities should play the decisive role in determining the shape of the CIP that the bank adopts in order to achieve the goals of Section 326. Credit card lending is a fundamentally different business from providing savings accounts, checking accounts, secured loans and other products, and it is neither reasonable nor practicable to require customer identity verification procedures in connection with credit card accounts to be the same as those procedures for other bank products and services. To the degree that a bank is engaged in credit card lending, its CIP should reflect the risks associated with credit card lending and the capabilities of the processes developed by the credit card lending industry to address those risks.

This should apply in particular to the process of gathering data from customers. As noted in the Proposed Rule, Congress intended that "the verification procedures ... make use of information currently obtained by most financial institutions in the account opening process." Proposed Rule at 48296 (quoting H.R. Rep. No. 107-250, pt. 1, at 63 (2001)). The Proposed Rule should more clearly and consistently reflect this clear Congressional intent to rely on financial institutions' existing data gathering practices. We are confident that this will permit our members to achieve the goals of Section 326, because – as we have explained in detail above in the case of credit card lenders – financial institutions' existing data gathering practices, though perhaps not developed with this intent, in fact amount to reasonable and practicable customer identity verification procedures.

These procedures do not always involve collecting the specific pieces of information that the Proposed Rule has identified as an irreducible minimum, nor do we believe it necessary for them to do so.

- *Social security numbers.* New customers are reluctant to provide social security numbers unless expressly required to do so, inspired by increasing concerns about identity theft. Because our members so often are unable to collect information in person, but must rely on receiving applications by mail, Internet or other channels, they cannot prohibit applicants from simply leaving blank the social security number section of applications. Moreover, federal and state legislatures have recently begun to debate possible legal restrictions on institutions' ability to require the transmission of social security numbers. We therefore think that banks should be given the discretion to collect identifying information other than social security numbers when appropriate in light of consumer privacy/security concerns and applicable law. Providing banks this flexibility will create less consumer resistance and ultimately lead to more success at data collection, while avoiding regulatory compliance disputes.[2]

---

[2] If the final Section 326 regulations mandated collection of social security numbers, and if that mandate were deemed consistent with the statutory grant of authority to your agencies to write such regulations, inconsistent state laws at least would be deemed preempted and would pose no legal barrier to the collection of social security numbers consistent with the regulations. It would remove lingering legal doubts, however, if the final Section 326 regulations coupled any such mandate with an express preemption of inconsistent state laws. Even then, the difficulty in persuading consumers to disclose their social security numbers on the basis of a federal

- *Residence address.* We also think that the final rule should eliminate the requirement to collect the consumer's residence address. New customers are reluctant to give more than one address, and credit card lenders have not had compelling reasons to request such information. At the time of application, credit card lenders collect the information they need to identify the consumer, make a credit decision, and administer the customer's account if credit is granted. In practice, credit card lenders have one opportunity to obtain information from the consumer, and they are sensitive to the need to request appropriate information rather than make unreasonably intrusive requests. Credit card lenders therefore do not routinely collect information on both the consumer's mailing and residence addresses, but rather simply the mailing address. Collecting this information is sufficient for credit card lenders to be able to establish a reasonable belief as to the consumer's identity by determining whether all of the information provided by the consumer is consistent with the information concerning the consumer available from trusted third parties. Adding a requirement to collect and verify residence address does not enhance the certainty of the verification process, as verifying the accuracy of a residence address other than the mailing address is difficult, given that credit reports and other sources of information available to our members generally simply provide one "principal address" or "current address." This additional data collection requirement is, however, extraordinarily burdensome, as it would require many of our members to make significant systems changes in order to accommodate an additional application data field for "residence address." As this information will be difficult and expensive to acquire, in the face of consumer reluctance to provide it and a complete absence of existing systems for credit card lenders to acquire and retain it, we think the requirement to collect and verify a separate residence address should be eliminated.

- *Physical address.* As noted above, credit card lenders require an applicant to provide her mailing address. It is irrelevant to the process of identity verification whether that mailing address is a physical address or a post office box. We are aware, of course, that a number of the September 11 hijackers opened bank accounts providing post office boxes as addresses. Financial Crimes Enforcement Network, SAR Activity Review (August, 2002), 18. The Agencies may be imposing the requirement to obtain residence and mailing addresses – which will discourage the provision of financial services to customers unable or unwilling to provide a physical address – in order to make a repetition of this sort of infiltration more difficult. Such a requirement, however, and its likely consequences, would have a number of problematic consequences. First, it would run counter to other federal initiatives intended to encourage the provision of financial services to the previously "unbanked." If the Agencies determine to impose such a requirement – which we think would be the preferable way to accomplish the intent that

---

requirement with which they may disagree strongly, would mean that even an express requirement to collect social security numbers in connection with account openings would be likely to meet with consumer hostility.

appears to underlie this requirement – it is imperative that the final Section 326 regulation protect financial institutions complying with that rule from possible liability under fair lending and equal credit opportunity laws. Second, consumers may have legitimate reasons for handling correspondence through post office boxes rather than providing their physical addresses. An individual strongly attached to privacy may want to limit the risk of intrusions of any kind into the solitude of her residence. A person with multiple part-time residences may conclude that it is easiest to handle all correspondence through a single site. A victim of identity theft may wish to make sure that she cannot again be victimized by having someone intercept mail left at her insecure home mail box. (It is our understanding that law enforcement agencies routinely advise victims of identity theft to establish post office box addresses for exactly this reason.) Finally, some consumers may have no alternative but to receive mail through an address other than a discrete physical address. These consumers include active-duty military and some diplomatic personnel who must receive mail through APOs and FPOs, and inhabitants of rural areas served through the rural route system. We do not think it appropriate that the final Section 326 regulation should in effect limit the access to credit, as well as to other financial services, of this wide variety of groups.

- *Principal place of business.* In connection with commercial accounts, we do not think the requirement to obtain information concerning a "principal place of business," proposed 31 C.F.R. 103.121(b)(2)(i)(3)(ii), is workable. Determining what constitutes a principal place of business can be a complex process, with no clearly right answer when the applicant is a geographically or organizationally autonomous division of a larger entity. The principal place of business of a multi-office organization may be irrelevant to a credit card lender, if the lender deals only with the business office from which the requests for credit are made or to which the account statements are delivered. Credit card lenders should not be put in the position of having to determine what constitutes a principal place of business, simply in order to verify a business customer's identity. Rather, they should be able to take the steps to achieve such verification that they consider reasonable in relation to the risk posed by the application.

Section 326 itself does not require obtaining specific pieces of information. The programs that financial institutions must establish under Section 326 must meet minimum standards established by the Agencies for "verifying the identity of any person seeking to open an account to the extent reasonable and practicable" and "maintaining records of the information used to verify a person's identity, including name, address, and other identifying information[.]" Pub. L. 107-56, Sec. 326(a), *codified at* 31 U.S.C. 5318(*l*)(2)(A), (B). As noted above, the Proposed Rule states that those standards should be adapted to banks' businesses. To the extent not required by other regulations, then, the bank should be able to determine what information is necessary to "enable the bank to form a reasonable belief that it knows the true identity of the consumer" of a particular financial product. Proposed Rule at 48292. In connection with the establishment of deposit accounts, share accounts and certificates of deposit, banks have long been required to

collect social security numbers. *See* 31 C.F.R. 103.34(a)(1). In connection with the establishment of other accounts, however, such as credit card accounts, banks are under no such obligations and should be able to collect the information they deem useful in establishing identity, based upon their assessment of their businesses. We therefore suggest that proposed 31 C.F.R. 103.121(b)(2)(i)(A) be changed to read as follows:

> The Program must contain procedures that specify the identifying information that the bank must obtain from each customer. Except as permitted by paragraph (b)(2)(i)(B) of this section, a bank must prior to opening an account obtain the customer's name, address, and other identifying information sufficient to enable the bank to form a reasonable belief that it knows the true identity of the customer. Such identifying information shall include any information required to be collected by 31 C.F.R. 103.34(a)(1), if that section applies to the account being opened.

Such a flexible standard would, we think, yield a far more workable regulation than the Proposed Rule, without sacrificing the security of the financial system against terrorist infiltration.

Limit Data Collection to Persons Who Actually Open Credit Card Accounts

Gathering data on appropriate persons is as important in keeping the Section 326 regulation workable as gathering appropriate data. The Proposed Rule would have our members collect and verify information about all "customers," defined to include both "any person seeking to open a new account" and "any signatory on the account" both when opened and at any time thereafter. Proposed 31 C.F.R. 103.121(a)(3). Both of these parts of the definition of "customer" are overbroad, unclear and in need of revision.

Persons Opening New Accounts

The Proposed Rule would require a bank to collect, verify and retain information about any person *seeking* to open a new account, even if that person does not actually obtain any financial product or service from the bank. Other financial institutions are not subject to such a broad requirement: the proposed Section 326 regulations for securities broker-dealers, mutual funds and futures commission merchants all define a customer as "any person who *opens* a new account with a broker-dealer" (emphasis added), not any person who seeks to open such an account. 67 Fed. Reg. 48317, 48327, 48337 (July 23, 2002). We see no reason to impose a blanket obligation on banks that is so much broader than that imposed on other financial institutions – and we wish to stress how much more intrusive and expensive it is to attempt to verify the identity of every person inquiring about a financial service than to verify the identity of every person actually obtaining that service. For reasons of policy and in order to limit the harmful economic impact of the Section 326 regulation, therefore, we think proposed 31 C.F.R.

103.121(a)(3)(i) should be changed to read as follows: "any person who opens a new account with a bank[.]"

If the Agencies insist on retaining the broad requirement of the Proposed Rule, it should be left to the banks to determine what activities constitute "seeking to open an account." This is the approach the Board has adopted in implementing the Equal Credit Opportunity Act ("ECOA"), 15 U.S.C. 1691 *et seq.* The Board's implementing regulations distinguish between an "application" for credit and a mere "inquiry." *See* Board Official Staff Commentary to Regulation B, Comment 202.2(f)-3. These regulations make clear that making the distinction is in the creditor's hands, as an application is a "request for an extension of credit that is made in accordance with procedures established by a creditor for the type of credit requested[.]" 12 C.F.R. 202.2(f). The final Section 326 regulation for banks should make clear that, if banks must collect and verify information on persons seeking to open accounts, banks may determine who is seeking to open an account by reference to their procedures applicable to the type of account at issue, perhaps by having proposed 31 C.F.R. 103.121(a)(3)(i) read as follows: "any person making a request to open an account in accordance with procedures established by the bank for the opening of the type of account requested[.]"

Signatories on an Account

The requirement of the Proposed Rule to collect customer identity information on all "signatories" on an account is also extremely broad with respect to credit card accounts, if the term is interpreted to mean all non-account holders to whom a credit card account holder grants account signing privileges. Credit card lenders do not generally treat information concerning persons granted signing privileges in the same way that they have treated information concerning the account holder. Requiring credit card lenders to obtain and verify information concerning persons granted signing privileges comparable to that concerning account-holders would involve significant additional costs – to the degree that credit card lenders would actually be able to obtain such information from account holders.

A credit card account belongs to its account holder, which is ultimately responsible for all debts legitimately incurred under the account. Credit card lenders obtain significant information concerning account holders and verify it against credit report information or other information. But they have concluded that it is reasonable to rely on account holders themselves taking appropriate steps to grant signing privileges only to trustworthy, responsible individuals, given that it is the account holders who will ultimately be responsible for the signatories' activities. This is particularly true for business accounts, where the business conducts its own review of employees before granting them signing privileges on a corporate credit card. In the absence of evidence that this is not a reasonable practice, we think that credit card lenders should be able to continue to rely on a business account holder performing its own diligence, rather than collecting additional data themselves.

With regard to consumer accounts, signatories on consumer accounts, such as college-age children authorized to sign on a parent's account, are often granted such privileges for brief periods purely as a convenience to the account-holder. A consumer account holder seeking to add a signatory to the account may simply not provide the requisite identity information about the signatory, acting on the reasonable understanding that it is the account holder's account, and the account holder should manage it as she sees fit. Benefits would arise from such a requirement only in the rare situations where a bona fide account holder unwittingly gave signing privileges to a terrorist or other criminal. The cost of managing the flow of information collected in connection with persons with signing privileges on consumer credit card accounts would in our opinion far exceed this small benefit.

We therefore suggest that proposed 31 C.F.R. 103.121(a)(3)(ii) be deleted, and that the first sentence of proposed 31 C.F.R. 103.121(b)(2) be changed to read as follows: "The Program must include procedures for verifying to the extent reasonable and practicable the identity of the customer who is the primary holder of the account." This change would authorize a bank to verify the identities of all signatories that the bank deems significant, based on the bank's analysis of the risks posed by extending signatory powers to those persons. Credit card lenders could then determine whether to collect information on signatories in connection with accounts with large average balances, large available credit lines, or other criteria deemed appropriate.

Preserve Instant Credit

In connection with instant credit, the Agencies are well aware from numerous examinations that banks making instant credit available through point-of-sale applications have long-established policies and procedures for managing the account opening process. It is important that the final Section 326 regulation confirm that banks can use that knowledge and experience to establish USA PATRIOT compliance structures appropriate to the customer identity verification risks associated with the process.

Instant Analysis of Data Provides Reasonable Security

The Proposed Rule should make clear that credit card lenders can continue to analyze the information they receive, and act on that analysis, in the ways they have been doing. Our members universally want to help accomplish the main goals laid out by USA PATRIOT – preventing terrorists and other criminals from using the American financial system, and identifying those who attempt to do so. We think our contribution should be based on the analytical abilities and systems we have already developed in the course of our business, which we will continue to refine in the light of new technologies. Our members' primary method for verifying customer identity consists of comparing the customer's self-reported information for consistency with information available to us from credit reporting agencies or other sources. It is unclear which of the categories of verification endorsed by the Supplementary Materials this process falls into – "positive verification" or "logical verification." *See* Proposed Rule at 48294. It is clear, however, that this method of verification meets the basic requirement: it allows our

members to form a reasonable belief that they know the true identity of their credit card account holders.

Because this verification method can be performed rapidly without loss of accuracy, the common practice of making "instant credit" available following such an analysis should pose no problem from a USA PATRIOT perspective. Whether credit is applied for at the point of sale for instant use, or through another channel for later use, the credit card lender will make the same decision. Systemic protections against fraud and other threats, including threats of use by suspected terrorists, are the same for all new accounts. We therefore think there is no reason to single out instant credit arrangements for special scrutiny, and certainly not for special limitations. This could be made clear by changing proposed 31 C.F.R. 103.121(b)(2)(ii)(B) so that the clause that currently states that among the acceptable methods of verifying customer identity is "independently verifying documentary information through credit bureaus, public databases or other sources" will read as follows: "independently verifying customer identity through comparison of information provided by the customer with information stored by credit bureaus, public databases, or other sources[.]" This will make clear that the fully automated customer identity verification procedures that credit card lenders actually use in connection with credit card accounts, and that are fundamental to the ability to provide instant credit, are in fact acceptable to use.

No Need to Keep Copies of Documents Examined by Merchants

The Proposed Rule raises other troubling issues in connection with instant credit arrangements, in particular having to do with the collection of information at the point of sale. We are concerned that the record keeping requirements, particularly proposed 31 C.F.R. 103.121(b)(3)(I)(A), when read in the context of the other requirements in the Proposed Rule, could be interpreted to require retail sales clerks to copy driver's licenses or other documents presented at retail sales registers in connection with the process of granting instant credit. Such a requirement would be unworkable and could result in lenders sharply curtailing, if not eliminating, the availability of instant credit in retail transactions, causing significant disruption to the American retailing system and the economy. Tens of millions of accounts have been opened in this fashion, and both large and small retailers rely on instant credit to generate sales. Eliminating this process could dramatically alter the market for retail credit and affect the way in which retail transactions are conducted. In the short term it could constrain retail sales at a time when the economy is looking to the consumer to continue the economic recovery.

During the credit-granting process, the store clerk takes certain steps as part of the merchant's own fraud control program. Often, the merchant will be permitting the customer to leave the store with merchandise purchased with this instant credit. In addition, the merchant may be providing the customer with a temporary credit card, such as a paper card, that the consumer can continue to use until the more permanent card is mailed to the customer's address by the credit card lender. It is therefore in the merchant's own interest to assure itself that the person applying for instant credit is in fact the person on whose behalf the credit is being requested. In order to

establish this identity, many merchants require that the clerk inspect one or more documents in order to confirm that the person physically making the application is in fact the consumer on whose behalf credit is being requested.[3]

The credit card lender does not require the examination or submission of this information in order to verify the consumer's identity for purposes of the credit card lender's own decision to grant credit. The credit card lender can easily reach a credit decision without such information, as is shown by the fact that accounts are opened by mail, over the telephone, or through the Internet, where such documents cannot be examined. Because the review of identifying documents in the store is not necessary for the granting of credit, we think it should be viewed as separate from the process of identifying the consumer for the purpose of the ongoing credit card relationship, even if the credit card lender is aware that the merchant engages in this review as an account opening procedure.

If this distinction is not made clear, and if the identifying documents reviewed in-store are instead construed to be documents on which the *credit card lender* relied to verify the customer's identity, we are concerned that the credit card lender could be required to obtain and retain a copy of any such identifying documents reviewed. Realistically, this would mean that the credit card lender would have to require the merchant to do so on the credit card lender's behalf. While we can understand that the Agencies may wish to maximize the collection of information about individuals opening accounts, and therefore may prefer that a copy of any document reviewed in the store be retained, such a requirement is simply not practicable to implement. Consumers can typically submit applications for instant credit at any sales register in a store. Copy machines typically are not present anywhere near most sales registers. Requiring copying of identifying documents would require that accounts only be opened at particular registers or at a central customer service desk. Having to endure the long delays created by such a requirement would cause significant consumer dissatisfaction.

We believe that such a radical change in the account-opening process would have a significant negative impact on both customers and merchants, and would harm retail sales by dissuading customers from opening retail credit accounts. Many merchants would stop checking customer identification entirely – accepting the likely resulting increase in losses from ordinary fraud – rather than have to copy identification documents. Some merchants have informed us that they would stop offering point-of-sale credit entirely.

In order to make clear that record retention requirements apply only to information the credit card lender relies on, not to information the merchant relies on, and in order to eliminate burdensome copying requirements, we urge that the language of proposed 31 C.F.R.

---

[3] Merchants typically require similar identification when cashing checks, or when permitting a customer to charge purchases to an existing credit card account in the absence of the customer's actual credit card. These documents are reviewed in order to establish the identity of the individual present in the store or to prevent that individual from misrepresenting his or her identity, rather than to verify the identity of the account holder.

103.121(b)(3)(i)(B) be changed to require that the bank retain "a *record* of any document that *the bank* relied on" in the performance of its CIP (emphasized language substituted).[4] It should be made clear that such a record can consist of a notation that the merchant has examined a particular document, and a transcription of the document number. This would be fully as useful as actually obtaining a copy of the document itself. For example, a transcribed driver's license number, noting the state issuing the driver license, should enable law enforcement representatives to access department of motor vehicle files concerning the individual as effectively as a copy of the driver's license. It would have the advantage of being a significantly easier requirement to implement.

Establish Reasonable Record-Keeping Requirements

From the above, it should be clear that the sorts of records obtained in connection with credit card lending are significantly different from those obtained in connection with the provision of other financial services, such as for example the making of loans secured by real property or chattels. The credit card applicant's file generally contains no title searches, verification-of-assets letters, pay stubs verifying employment or income or other similar documents. It appears to us that there is no reason to treat the information the credit card lender obtains in connection with a credit card application – chiefly the application form itself and the credit report on which the credit decision is based – as though they were the sort of document-heavy file associated with a secured loan or similarly documented financial product.

It is therefore our belief that the record keeping requirement of the Proposed Rule should provide enough flexibility so that a credit card lender does not have to retain valueless documents for punitively long periods. Proposed 31 C.F.R. 103.121(b)(3) requires a bank to retain, until five years after the closing of the account, a customer's identifying information, copies of any documents relied on in verifying customer identity, "methods and results of ... measures undertaken to verify the identity of the customer," and information concerning the resolution of any discrepancy in identifying information obtained. Proposed Rule at 48299. Credit card accounts often remain open for years or even decades. We see no reason to retain credit report information, obtained at application, for this amount of time. The information itself is stale within months after a credit card lender obtains it. Moreover, it is the correspondence between

---

[4] This permits the bank to make its own decisions as to how to ensure that meeting its obligations under Section 326 does not entail liability under ECOA. Regulation B permits a creditor to retain in its files information that is prohibited by Regulation B in evaluating applications, such as information about the applicant's race, if the information is required to monitor compliance with federal or state statutes or regulations. 12 C.F.R. 202.12(a). We understand that the Agencies thought requiring the retention of certain documents would shield creditors under this provision: to the extent that the Proposed Rule requires a creditor to retain a copy of a driver's license or other identifying documents with photographs, the creditor can do so without fear of ECOA liability. *See* Complaint of the United States in *United States v. First Fidelity Bank, F.S.B.*, No. CV-01-03906 (E.D.N.Y., July 8, 2002). The change we have proposed would still permit creditors to shield themselves from ECOA liability in this way, but it would leave the determination of how to deploy that shield, if at all, to the creditors themselves.

the applicant's self-reported information and the credit report information, rather than the credit report information itself, that forms the basis for the credit card lender's conclusion that it is reasonably certain of the customer's identity. Nor do we see why a credit card lender should retain a customer-by-customer record of the processes the credit card lender uses to verify customer identity, if the processes and verification standards do not vary from customer to customer. Given this, we propose four changes to the record retention requirement:

- *Limited duration of record retention.* In general, the period of retention for any documents or other materials should be no greater than that of any record retention requirement that already applies to such documents or other materials. In the case of credit card accounts, "[a] creditor shall retain evidence of compliance with [Regulation Z, implementing the Truth In Lending Act] for two years after the date disclosures are required to be made or action is required to be taken." 12 C.F.R. 226.25(a). Unless there are compelling reasons to require the retention of certain specific items of information for a longer period, the Proposed Rule should adopt this time period for the information collected in connection with the performance of the CIP. If the Agencies wish to impose a common record retention requirement for all identity verification records, rather than conforming the requirement to various pre-existing regulatory requirements, five years from the time the account is opened is more manageable and should be an ample period.

- *Impersonal records of verification processes.* When and to the extent that the credit card lender relies on automated processes, it should at most be required to keep institutional records of what those processes were. The credit card lender should only have to keep customer-by-customer records where there is a resolution of any discrepancy by non-automated means.

- *No additional records on rejected or withdrawn applications.* We have noted above our concerns about requiring the collection and verification of information about applicants whose applications are rejected on ordinary credit underwriting grounds or are withdrawn. We feel the same arguments apply to the retention of records concerning such applications. Except to the extent that such records must be maintained pursuant to other regulatory requirements, such as those of ECOA, or to the extent that the rejection or withdrawal involves any suspicious activity and thus gives rise to record keeping requirements under Suspicious Activity Reporting requirements, we think records concerning such applications should not have to be kept.

- *Record retention by agent.* If it is necessary that records pertaining to a merchant's examination of identity information for the merchant's own purposes (see above) be retained, it is important that the credit card lender be able to satisfy the requirement by having the merchant retain this information on the credit card lender's behalf. For the foreseeable future, it may be impossible to reconfigure all merchant automated systems to be able to capture this additional information and send it to the credit card lender. As

long as this is the case, the information will have to be recorded on paper. Transferring paper documents from separate retail outlets to credit card lenders is costly and error-prone. It may also raise security issues, creating opportunities for identity theft through the interception of copies of identifying documents.

Specify Government Lists to be Consulted

The Proposed Rule requires a bank to check customer names against "any list of known or suspected terrorists or terrorist organizations provided to the bank by any federal government agency." Proposed 31 C.F.R. 103.121(b)(4). The Proposed Rule, however, does not establish what constitutes "providing" a list to a bank; as a result, the checking requirement may not cover the OFAC list, which is made available to banks at the exercise of banks' own initiative, and may not cover other lists of interest to the Agencies. To provide our members with some certainty as to the scope of this requirement, the final Section 326 regulation should at a minimum specify the agencies that are permitted to provide such lists and the mechanisms by which such lists may be provided. For example, the final regulation could provide that FinCEN alone has the power to provide lists to financial institutions, and that FinCEN must provide those lists in accordance with the information sharing mechanism of Section 314 of USA PATRIOT. Alternatively, proposed 31 C.F.R. 103.121(b)(4) could be changed to specify the lists to be checked, for example by requiring a check against "the list of specially designated nationals and blocked persons maintained by the Department of the Treasury, Office of Foreign Assets Control, pursuant to Executive Order 13224." By creating more specificity, such a change would make effective compliance far easier to achieve.

Delay Mandatory Implementation

As we hope this letter has made clear, the Proposed Rule raises complex issues for credit card lenders. Resolving these issues will be a challenge in terms of both formulating compliance strategies and implementing them. Attempting to implement such complex requirements is difficult at any time of year, and it will be particularly difficult in the last quarter of the calendar year. Few, if any, financial institutions or merchants will be prepared to make system changes that might jeopardize the economically crucial holiday business by imposing new obligations on consumers, slowing down transactions, or otherwise discouraging retail sales. Moreover, implementing compliance strategies that have not been approved in advance can impose significant re-programming costs if the strategies have to be changed.

If the final Section 326 regulation imposes requirements less onerous than those embedded in the Proposed Rule, it may be easier for our members to implement those requirements. If the final regulation makes clear, for example, that credit card lenders can rely on their existing processes for customer identity verification purposes, it may be possible to implement such a final regulation within six to nine months. If, on the other hand, a final regulation roughly in the form of the Proposed Rule is published, we urge the Agencies to provide for a significant delay in mandatory compliance with such a final regulation, and to adopt a two-step compliance

approach. We propose that credit card lenders be given until April 26, 2003 to prepare compliance strategies and secure the approval of their boards of directors, and then until April 26, 2004 to implement those compliance strategies. This will be the minimum time necessary for our members to develop, implement and test their new compliance systems.

In crafting and implementing compliance strategies, our members would also appreciate the Agencies making clear through an unambiguous statement in the final Section 326 regulation that the customer identity verification requirement applies only to accounts opened after the mandatory compliance date, and does not apply to continuously active accounts established before that date that merely experience an action such as an increase in the available credit line.

Conclusion

The changes we have recommended all stem from our appreciation that the business of credit card lending is significantly different in many respects from the business of providing other sorts of financial products and services. Allowing for those differences in the Section 326 regulation will produce a rule that will protect credit card lending against infiltration by potential terrorists and other criminals without disrupting the credit card industry.

We appreciate the opportunity to comment on the Proposed Rule. If we can provide any additional information about any of the issues we have raised in this letter, please do not hesitate to call Monique Gaw, AFSA's Vice President for Federal Government Relations, at (202) 296-5544.

Very truly yours,

AMERICAN FINANCIAL SERVICES ASSOCIATION

Cc: Charles D. Klingman
Office of Consumer Affairs and Community Policy
Department of the Treasury