29

NATIONAL RETAIL FEDERATION

September 6, 2002

Via Facsimile 202-874-4448 and email: regs.comments@occ.treas.gov Office of the Comptroller of the Currency Public Information Room Mailstop 1-5 250 E Street, SW Washington, DC 20219 Re: Docket No. 02-11	Via Facsimile 202-906-6518 and email: regs.comments@ots.treas.gov Regulation Comments Chief Counsel's Office Office of Thrift Supervision 1700 G. Street, NW Washington, DC 20552 Re: No. 2002-27
Via Facsimile 202-452-3819 and email: regs.comments@federalreserve.gov Secretary, Board of Governors of the Federal Reserve System 20th Street and Constitution Avenue, NW Washington, DC 20551 Re: Docket No. R-1127	Email: regcomments@fincen.treas.gov FinCen Section 326 Bank Rule Comments P.O. Box 39 Vienna, VA 22183 Attn: Section 326 Bank Rule Comments

RE: PROPOSED REGULATION 103.121 (CUSTOMER IDENTIFICATION PROGRAMS FOR BANKS, SAVINGS ASSOCIATIONS, AND CREDIT UNIONS)

Gentlemen and Ladies:

The National Retail Federation (NRF) appreciates the opportunity to comment on proposed regulation section 103.121 under the USA PATRIOT Act, which would require banks, savings associations, and credit unions to establish and maintain customer identification programs. The National Retail Federation is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including leading department, specialty, discount and mass merchandise stores, as well as catalog and the Internet.

The World's Largest Retail Trade Association

♦

Liberty Place, 325 7th Street, Suite 1
Washington, DC 20004
(202) 783-7971 Fax: (202) 737-2849

www.nrf.com

In its role as the retail industry's umbrella group, NRF also represents 32 national and 50 state associations. NRF's members offer credit to facilitate and encourage retail sales.

Retail credit card accounts may be established in several ways: A retailer may extend credit by issuing its own credit card in its own name. Alternatively, a retailer may accept credit card applications on behalf of an independent bank, which evaluates the application and issues a credit card with the retailer's logo. (These arrangements are often referred to as "private label" credit cards.) Finally, a retailer may be affiliated with a bank through common ownership or management. In that case, the retailer accepts applications for its affiliated card-issuing bank and forwards the application information to the bank for its evaluation. The affiliated bank evaluates the application and issues the credit card with the retailer's logo.

The distinction among retail credit card accounts is significant because the proposed regulation applies only to "banks" as defined in 31 C.F.R. § 103.11(c). Retailers that issue their own retail credit cards and retailers whose private label credit cards are issued by independent banks do not come within the definition of "banks" and are, therefore, not covered by the proposed regulation. Because the regulation would cover banks that issue credit cards for use at their affiliated retailers, NRF's comments discuss the proposal's effect on these banks. We refer to these banks as "retail credit card issuers" and to the cards they issue as "retail credit cards."[1]

Unlike those credit card issuers offering depository bank products (e.g., checking, savings, money market and similar currency based products), retail credit card issuers offer unique products to their customers and face unique challenges which distinguish them from non-retail credit card issuers. In the retail setting, the availability of "instant credit" at the point of sale allows customers who satisfy a rigorous credit fraud screening process (discussed more fully below), to open an account with a reduced initial credit line and immediately purchase products, often at significant savings. The availability of instant credit also allows the customer to manage his available credit line by making retail purchases on a retail credit card while reserving his other generally accepted credit cards (e.g., Visa, Mastercard, etc.) for non-retail purchases. Through instant credit, retail credit card issuers provide a singular benefit to their customers by allowing them to maximize their available spending power. The availability of instant credit also permits retailers to build lasting customer relationships, increasing the likelihood that customers will return to the retailer.

In making retail credit widely available to those who qualify, retail credit card issuers face unique market challenges. For the majority of retailers, the last quarter of the calendar year, representing the holiday shopping season, accounts for the vast majority of the revenue generated through retail shopping. As a consequence, it is also the period of time when business disruption through, for example, the implementation of newly mandated procedures, can have the most

---

[1] Many of NRF's members issue credit cards in one or both of the following forms:

- Private-label cards, issued in the name of a retailer by a bank (which may or may not be affiliated with the retailer) and usable to purchase goods and services only from that retailer and, in some instances, its business partners; and
- Bank cards, linked to a credit card network such as Mastercard or Visa and usable to purchase goods and services from many retailers and merchants.

harmful consequences. Retailers are particularly concerned about proposed changes to their customer identity verification procedures which may have to be implemented during this most vulnerable period of time. For this reason, and the others explained more fully below, NRF writes to comment on the proposed regulation.

1. The Proposed Regulation's Goals

By requiring banks to establish and maintain formal customer identification programs, the proposed regulation would discourage and hinder those who would fund terrorism or engage in money laundering activities. The regulation also seeks to make it easier to identify and trace the perpetrators of these offenses when they occur. NRF fully supports these essential goals. NRF also supports the regulation's flexible, risk-based approach, based on the bank's size, location and type of business, for the development and implementation of customer identification programs.

Because of their own need for customer identification, retail credit card issuers' existing procedures for credit fraud prevention, customer identification, and identity verification already achieve the goals underlying the proposed regulation. In its August 2002 Report entitled *Money Laundering – Extent of Money Laundering Through Credit Cards Is Unknown,*[2] the General Accounting Office reported that bank regulatory officials agreed that credit card issuers' existing credit card application screening process, systems for monitoring credit fraud, and policies restricting cash payments, prevented credit cards from being a useful means to launder money.[3]

At the same time, there is no evidence that retail credit card issuers' accounts pose a terrorism or money laundering risk. NRF believes that some of the proposed provisions would inadvertently burden retail customers through the elimination of certain account opening opportunities (as explained below), and that the cost of these provisions would outweigh any incremental anti-terrorism or anti-money laundering benefit achieved by their implementation. We also believe that there are ways to accomplish the proposed regulation's goals without imposing these undue costs.

2. Current Retail Credit Card Issuer Practices

Customers currently open retail credit card accounts by one of the following four methods: (1) completing a retail credit card application at the point of sale; (2) mailing a completed retail credit card application to the card issuer; (3) telephoning the card issuer and providing the required retail credit card application information; or (4) completing an online retail credit card application which is then submitted to the card issuer.

The vast majority (up to 90%) of retail credit card applications are made at the point of sale are for "instant" credit; that is, if the application is approved, the customer is immediately given access to an account with a specified credit limit for immediate use in the store. Retailers may further incentivize "instant" credit applications by offering a discount on purchases made in the store the day that the new account is opened. For retailers, the instant credit opportunity is often the retailers' only chance to build a customer relationship which may lead to brand loyalty

---

[2] The report is available at the GAO's website. *See* <http://www.gao.gov/new.items/d02670.pdf>.

[3] *See* GAO Report at 29.

and a lifetime customer. Most instant credit applications are completed during the holiday shopping season (October through January) or during store-wide sale days. At these times, the customer volume is at its highest level and the need for efficient credit application processing is most urgent.

For retail credit applications that are completed at the point of sale, the vast majority of card issuers require the person taking the application to inspect a valid government-issued photo identification card provided by the customer.[4] Many of these card issuers also require that the person taking the application examine the government-issued identification, record the identification number, state of issuance, and, in some instances, affirmatively indicate on the application that the person has determined that the photograph on the identification matches the applicant. Where the instant credit applicant is unable to produce a valid government-issued photo ID, some retail credit card issuers deny the credit application. Other card issuers, under such circumstances, or where the applicant's current address shown on the ID does not match the address shown on the application, will require that the person taking the application obtain a second additional form of identification, such as a valid credit card issued in the name of the applicant.

After a valid government-issued photo ID has been obtained and, where necessary, a valid second form of identification has also been obtained, the card issuer completes a detailed identity verification process before the account is opened. Using the information provided by the applicant, the retail credit card issuer obtains a credit report to verify the identifying information provided by the applicant by comparing it to verifiable information obtained from third parties. This also affords the credit card issuer the ability to learn the applicant's current and prior billing addresses, current and prior employers, current status of other credit accounts, prior credit history, and the number of credit inquiries which have been made concerning that specific applicant. Retail credit card issuers also cross-reference the applicant's information against the Office of Foreign Asset Control's (OFAC) list of Specially Designated Nationals and Blocked Persons (SDN List) as well as those lists of persons for whom fraud alerts have been placed on their credit reports. If no credit report is obtained or no credit record is found, the retail credit application is almost universally declined. If a credit report is obtained, the card issuer's credit scoring process is completed to determine the risk that the account may not be paid, including the likelihood of credit fraud. Only then is a retail credit card issued to an instant credit applicant.

In extremely rare instances, some retail credit card issuers may approve credit for an applicant for whom no credit report could be obtained. On these rare occasions, issuance occurs only when the card issuer can verify the name and address of the applicant through other means, such as "Fast Data," a service provider that allows retail credit card issuers to match the applicant's provided name and address information with record information. Some retail credit card issuers often complete additional identity verification procedures in those circumstances, including investigating the applicant's employment and residential references. Finally, in those instances, the applicant is initially granted only a small credit limit.

---

[4] In some states, like New Jersey and Vermont, photographs are not printed on state driver's licenses.

The credit report plays a crucial role in verifying the identity of the retail credit applicant. By cross-referencing the information provided by the applicant with the corresponding information shown on the credit report, the card issuer is, before the account is ever opened, assured not only of the validity of the information provided by the applicant but also that the applicant has a credit history demonstrating a verified pattern and practice of paying credit debts. This verification process also insures that, in the event the card holder uses the retail credit for illegal purposes (whether credit fraud, terrorism or money laundering), law enforcement authorities have the means to trace the illegal activity to the responsible party, the very purpose underlying the Customer Identification Programs required by the proposed regulation.

For those retail credit card applications that are received by mail, telephone and the Internet, card issuers follow the procedure described above for instant retail credit applicants, except that no government-issued photo identification is examined at the time the account is opened. However, many card issuers supplement the credit report identity verification process by requiring that the card holder provide a government-issued ID number and/or activate the account by calling the card issuer from the home telephone number provided by the applicant, which can be cross-referenced with the home number shown on the credit report. Further, many retail card issuers also require the card holder to present a valid government-issued photo ID card when using the newly issued retail credit card for the first time.

Using the information provided by the applicant, the retail credit card issuer obtains a credit report which allows the card issuer to verify the identifying information provided by the applicant and to learn the applicant's current and prior billing addresses, current and prior employers, current status of other credit accounts, prior credit history, and the number of credit inquiries which have been made concerning a particular applicant.

Some of the applications retail credit card issuers receive by mail are the result of prescreened solicitations. These solicitations are sent to consumers based upon a consumer reporting agency's review of their criteria in accordance with the provisions of the Fair Credit Reporting Act. Thus, prescreened solicitations are sent only to individuals with established credit histories. Credit card accounts based upon direct mail prescreening are not established until the consumer has signed and returned, by mail, the information requested in the solicitation. Usually, the requested information pertains to identity verification, employment and income. When consumers respond to prescreened solicitations, the retail credit card issuer still undertakes the detailed identity verification process described above for mail-in applications, including obtaining a complete credit report concerning the applicant and verifying all of the identity information provided by the applicant against the record information received from the credit bureau. Only if the applicant satisfies the retailer's rigorous identity verification and credit fraud prevention procedures is a credit card account actually opened.

Thus, current retail credit card issuer procedures include gathering applicant identity information, verifying that information, screening applicants and denying credit to applicants who do not meet the rigorous criteria used by card issuers. Much of this system is automated, that is, following the data entry of the applicant's information into the card issuer's computer system, the credit report is obtained, the review is initially made electronically and, where necessary, there is additional review by additional trained personnel, and the account opening

decision is completed. The customer benefits when the reduced cost of the automated system is passed on to the customer in the form of reduced credit costs. Additionally, the process subjects those whose identification is not readily verifiable or is incomplete to further scrutiny and prevents all but those whose identities can be verified from obtaining retail credit.

3. Risk Assessment for Retail Credit Cards

The proposed regulation requires that a bank's identification program be "tailored to the bank's size, location and type of business" and that the identity verification program be "based on the bank's assessment of the risks presented by the various types of accounts maintained by the bank, the various methods of opening the accounts provided by the bank, and the type of identifying information available...."

Although not specifically aimed at retail credit card use, the GAO's Report followed extensive interviews with U.S. bank regulatory officials, law enforcement officials, and major credit card issuing banks. Law enforcement and regulatory officials repeatedly indicated that, in their opinion, credit cards presented little or no risk of money laundering and, in fact, could not identify a single instance in the U.S. where credit cards had been used to launder money.[5] As explained by the GAO, the Federal Reserve Board and the Federal Deposit Insurance Corporation "noted that there was no evidence to suggest that credit cards were at high risk for being used for money laundering."[6] The only significant risk of money laundering identified in the GAO report concerning credit card use involved the use off shore banks in jurisdictions with weak anti-money laundering laws,[7] a consideration that is not an issue for retail credit card issuers.

In addition to the credit fraud prevention practices of credit card issuers, regulatory and law enforcement officials credited the difficulty of using credit cards for money laundering as a reason for the absence of any evidence of such use. According to GAO, money laundering occurs in three stages: (1) "placement" where cash is converted into monetary instruments (e.g., money orders, traveler's checks, or deposits); (2) "layering" where the funds are transferred or moved into other accounts to obscure their illicit origin; and (3) "integration" where the funds are used to purchase assets in the legitimate economy.[8] GAO concluded, based on information received from bank regulatory and law enforcement officials, that credit cards are not likely to be used in money laundering activities because of credit card issuers' restrictions on cash payments for credit balances.[9]

---

[5] GAO Report at 3, 15-16, 29, 33.

[6] *Id.* at 33. In NRF's experience, its members have obtained identity verification information for all of their retail credit card applicants, and retained this information for varying periods of time, no law enforcement agency has ever made use of such information for the purpose tracking terrorist or money laundering activities.

[7] *Id.* at 21.

[8] *Id.* at 6.

[9] *Id.* at 15.

The retail credit card business presents little or no risk of terrorist use or money laundering. The average retail credit card transaction totals only $64.[10] While some retail credit card accounts permit customers to obtain limited credit in the form of cash advances, the available amounts are generally small. Many retail credit card issuing banks simply do not permit cash advances, and/or reserve credit limits over a few hundred dollars for those customers with long-established credit histories Further, in NRF's experience, more than 75% of its credit granting members open retail credit accounts that have initial credit limits of less than a couple thousand dollars. For those accounts which are opened with larger initial credit limits, the vast majority of such accounts are opened for the purpose of making a particular "big ticket" retail purchase (e.g., furniture, carpet, home theater systems, etc.) that immediately utilizes the credit line, leaving minimum credit availability for further purchases until the balance is paid down.

Considering the nature of the retail business and the type of accounts offered by retail credit card issuers, the only possible risk is that the goods or services sold by retailers may be used for illegal purposes, a risk, which though remote, does not depend upon the existence of a retail credit account. For example, a tool might be purchased on credit from a retail store and used to construct a terrorist device. The same tool used for the same purpose could also be purchased by check or for cash. A product might be bought on credit from a retail store and then sold for cash, but the same is true for a cash or check purchase of the product. Moreover, given the security measures already employed by retail credit card issuers, applying for and using a credit account is far more difficult that simply paying by check or cash. It is not the existence of a retail credit account which presents the risk, rather it is the availability of consumer goods themselves, something that is outside the scope of the proposed regulation.

The use of retail credit accounts to launder money is demonstrably inefficient and so cumbersome as to be useless. First, the amount of credit typically available for a retail credit account means that in any one month an account holder could purchase only a very small amount of goods to be laundered for cash. To purchase additional goods in subsequent months, the existing balance would first have to be paid down. Second, because any goods purchased for sale would be bought at retail prices and presumably sold at a discount, the entire effort to launder money using retail products purchased on credit would ultimately cost the launderer more than 100% of what it would produce, a significant factor undercutting any money laundering risk posed by the availability of retail credit accounts. Thus, in the remote likelihood that funds were to be laundered through retail purchases, using cash would be much more expedient than credit.

Retail credit card issuers have a compelling financial interest in insuring that their credit cards are issued only to credit applicants whose identities can be verified and who have verifiable payment histories. Absent procedures which would permit such verification, credit fraud would threaten these creditors' economic survival. This compelling interest has led to the development and implementation of detailed identification and identity verification methods designed to prevent credit fraud. In addition, retail credit card issuers have developed and currently use sophisticated computer software to identify unusual account activity or discrepancies in account information. For example, current procedures include: monitoring unusual buying patterns (e.g., multiple unit purchases of the same expensive retail item when the

[10] In its Report, the GAO concluded that the average credit card transaction totals only $70.

typical customer purchases only a single unit); monitoring unusual payment patterns (e.g., the customer's continued maintenance of a high account credit balance by overpaying on the account); monitoring unusual return activities (e.g., the customer's repeated return of an item or similar items); flagging accounts which have been opened under different names for persons living at the same address; and flagging instances where the same account is being used by two different people in two different locations.

Thus, the risk that retail credit card accounts will be used for terrorism or money laundering purposes is negligible or non-existent. Moreover, the risk of credit fraud has already prompted card issuers to adopt identity verification procedures which satisfy the "know your customer" goals of the proposal and which provide a means by which law enforcement can trace any illegal activity to the account holder, the very purposes underlying the proposal.

4. The Proposed Regulation

Although the proposed regulation states that its risk-based approach will depend upon the bank's business, some of its provisions appear to be written only with depository banks in mind. In fact, some of the terminology is more appropriate for depository banks, than for credit card issuers (e.g., the use of the term "signatory," on an account). We believe that the apparent focus on depository banks may have resulted in some proposed identification requirements that would be appropriate for depository institutions but create serious problems for retail credit card issuers.

A. Identification verification procedures for retail credit card issuers

The proposed regulation requires that a bank's Customer Identification Program contain procedures describing when the bank will verify identity through documents and setting forth the documents that will be used for that purpose. § 103.121(b)(2)(ii)(A). For individuals seeking to open accounts, the proposal requires that the bank use an unexpired government-issued identification bearing a photograph as a document which may be used to verify applicant identity. § 103.121(b)(2)(ii)(A)(1). The proposal also requires that a bank's program contain procedures that describe non-documentary methods the bank will use to verify identity in addition to, or instead of, relying on documents. § 103.121(b)(2)(ii)(B).

As explained above, even when the application is completed at the point of sale for "instant credit," the account is opened only after the application is forwarded to the card issuing bank, which completes a detailed identity verification process, including obtaining a credit report on the applicant, before opening the account. We believe, therefore, that the proposed regulation does not require a bank to retain a photocopy of the photo ID for identity verification purposes under these circumstances because the retail credit card issuer will have relied upon "non-documentary verification methods," such as the credit bureau report. The proposed regulation is not entirely clear on this point.

Clarification is important because point-of-sale, "instant credit" applications account for up to 90% of the new accounts which are opened by retail card issuers. Consumers overwhelmingly choose to open their retail credit card accounts at the point-of-sale, because of its convenience and often because it allows consumers to benefit from in-store discounts offered to promote an on-going customer relationship with the retailer. If the person taking the credit application at the point-of-sale, were required to copy a photograph-bearing, government-issued

identification card as part of the identity verification process, instant credit programs would likely be eliminated as a convenience to consumers because consumers simply will not be able to tolerate the burdensome intrusiveness and delay. If maintaining a copy of the government-issued identification card were the only method of document-based identity verification for individuals permitted under the proposed regulation, then retailers taking applications at the point-of-sale would be required to either maintain copy machines at numerous payment locations in the store to copy the ID, require sales people to leave the sales floor to make a copy of the ID, or centralize the instant credit application process at a single location in the store, eliminating the very convenience that consumers seek.

The burden on retailers is perhaps best illustrated by considering a single NRF member, Marshall Field's, as an example. In this retailer's flag ship Chicago, Illinois store, there are ten retail floors, 800,000 square feet of retail shopping space, and 527 registers at 292 points of sale. During the peak holiday shopping season, there are 2,500 retail employees in the store in a single day. If copiers were required at all the points of sale, then for this one store, this retailer would be required to buy 292 or more copiers. Assuming an initial cost of at $1,000 per point of sale for the copiers, installation and possible reconfiguration of the point of sale layout, the estimated initial cost would be at least $292,000. This initial start-up cost does not include maintenance, the cost of copying or training for personnel. Nor does it include the lost sales which would likely result from customer dissatisfaction with having to wait in long lines while IDs are copied, particularly during the busy holiday shopping period or on sale days, the same time periods when the majority of instant credit accounts are opened. Nor does it include the delay and expense which would result from ordinary copier breakdowns during peak sale periods, resulting in additional customer frustration and lost sales. Moreover, these concerns are only multiplied if a store, such as Marshall Field's, were to centralize the instant credit application process, either on a store-wide basis or floor-by-floor. Such centralization, during peak periods when Marshall Field's may receive several thousand instant credit applications per day, could well result in unmanageable personnel shortages and customer congestion.

When this one store from a single example retailer is multiplied by the number of retailers in the U.S. and the hundreds of thousands of consumers who apply for retail credit each day, the burden on the retail customer (in addition to the compliance burden for the retailer) could force retail card issuers to discontinue point-of-sale, instant credit applications, all to the harm of consumers who find this to be the most convenient method of opening retail credit accounts.

The agencies are aware that some segments of the population have been less trustful of banking institutions due to a perceived history of discrimination against those members of the public. Indeed, the issue of "unbanked" consumers is of continuing concern. By necessity, retailers attempt to maintain a close and trusting relationship with their customers. At present, credit decisions, which are essentially automated and dependent on credit scores and other objective factors, are transparently made without regard to a particular customer's status. The customer typically enters or dictates appropriate information to the sales person and a credit granting decision is made. If retailers were required to take a driver's license away from the customer, either for copying in a remote location, or the copy of the driver's license were attached to a customer's credit application, the customer may view the credit decision as having

been based on a the customer's status (race, ethnicity, etc.). NRF is extremely concerned about this possible customer perception and asks the agencies to be sensitive to the question of whether the limited utility of a photocopied driver's license truly outweighs this unintended consequence and the others discussed in this comment.

Moreover, in NRF's experience, credit applicants are particularly sensitive to the disclosure of the personal information which is currently required as part of an application for a retail credit card. Often, when an applicant is denied credit, he demands the return of his application, or the destruction of the application in his presence. The proposed regulation, if read to require the retention of the application, and the copying and retention of a government-issued ID, will likely cause disruption in the retail store, particularly in those instances where the applicant is denied credit and then informed that the retail credit card issuer must retain not only the application but also a copy of the ID bearing much of the applicant's most sensitive personal information. [11]

It is evident from the agencies' comments on the proposal that the recordkeeping requirement was not intended to impose the type of burden described above. The agencies estimate that each financial institution will require 10 hours per year to comply with the recordkeeping requirement. 67 FR 48290. This calculation is based upon the assumption that the requirement will have little effect on existing practice "because such recordkeeping is the usual and customary business practice" for banks. *Id.* As explained above, this assumed minimal burden is incorrect if retail credit card issuers are required to generate and retain photocopies of government-issued identification cards. The burden on affected retail credit card issuers would number in the thousands of hours annually if the document-based identity verification requirement is read to require the copying and retention of photo IDs.

Moreover, a requirement that copies of photograph-bearing, government-issued identifications be copied and retained would present an irresistible lure for identity thieves and could thwart the very purposes underlying the USA PATRIOT Act and the proposed regulation. For example, each step in the identity verification process (e.g., when the ID card is copied, retained for storage at the retail location, moved for consolidated storage, imaged for electronic storage, and extracted for destruction) would present an opportunity for identity theft.

If the proposed regulation is not modified to make clear those circumstances under which a bank (or retail credit card issuer) is required to obtain a government-issued identification bearing an applicant's photograph for identity verification purposes, the proposal may impose customer identification requirements which may impinge upon existing state law limitations on

---

[11] The federal Equal Credit Opportunity Act (ECOA) makes it unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction on the basis of race, national origin, sex, or age. 15 U.S.C. § 1691(a)(1). Retail credit card issuers do not currently record any applicant race information in connection with the opening of a account. By requiring, as a condition of opening an account, the copying of a photo ID, the proposed regulation subjects retail credit card issuers to discrimination claims by those denied credit. The copy of the government-issued photo ID required by the proposed regulation would serve as evidence that the card issuer sought and obtained race data before making a credit granting decision. The proposed regulation provides no insulation for retail credit card issuers against such claims.

the collection of such information and may create unintended exposure to lawsuits by consumers for retailers and credit card issuers who attempt to collect the required identity information or verify the identity information provided by the applicant.

California's prohibition against the collection of identification information by anyone who accepts a credit card illustrates how sensitive state governments have become to the collection of their citizens' personal identifying information. California law prohibits "any person, firm, partnership, association, or corporation from requiring the cardholder, as a condition to accepting the credit card as payment" from recording any of the identification information contained on a state driver's license, or state identification card, or another form of photo identification in connection with a credit card transaction. Cal. Civ. Code § 1748.8(d).

To provide the needed clarification, NRF proposes the following modest revisions to subsection 103.121(b)(2)(ii)(B) and 103.121(b)(3)(i)(B) (the suggested additions are shown in **bold-underline** and language struck from the existing draft is shown in [*bracketed italics*]):

> (B) Non-documentary verification methods. The Program must contain procedures that describe non-documentary methods the bank will use to verify identity and when these methods will be used in addition to, or instead of, relying on documents. [*These procedures must address*] **Instances in which the bank may rely solely upon non-documentary verification methods include**: situations where an individual is unable to present an unexpired government issued identification document that bears a photograph or similar safeguard; the bank is not familiar with the documents presented; the account is opened without obtaining documents; the account is not opened in a face-to-face transaction **between the bank and the customer**; and the type of account increases the risk that the bank will not be able to verify the true identity of the customer through documents. Other **non-documentary** verification methods may include contacting a customer; independently verifying documentary information through credit bureaus, public databases, or other sources; checking references with other financial institutions; and obtaining a financial statement.
>
> (3) Recordkeeping. (i) The Program must include procedures for maintaining a record of all information obtained under the procedures implementing paragraph (b)(1) of this section. The record must include:
>
> * * *
>
> (B) A **record of the information** [*copy of any document*] that was relied on pursuant to paragraph (b)(2)(ii)(A) of this section that clearly evidences the type of document and any identification number it may contain;

The suggested revision to proposed regulation 103.121(b)(3)(i)(B) to permit the retention of "a record of the information" rather than the copying of the ID card itself is consistent with other federal law permitting the retention of record information in lieu of the actual document.[12]

---

[12] *See e.g.*, 12 U.S.C. § 1953 (permitting the retention of bank record information in electronic or automated form).

B. Authorized users and joint account holders

The proposed regulation defines "customer" to include, not only the person seeking to open a new account, but also "[a]ny signatory on the account at the time the account is opened, and any new signatory added thereafter." § 103.121(a)(3). The use of the term "signatory" implies that it is meant to cover only signatories on deposit accounts. (For example, a deposit-account opening card will have a place for the account holders' signatures, against which withdrawal requests may be compared.) The term "signatory" is not generally used for credit card accounts because, in many instances, the account holder's signature is not necessary to obtain credit under the account. This is particularly true for retail credit cards, which may be used to make purchases by mail, telephone and over the Internet.

Nonetheless, it is possible that the term "signatory" could refer to any person who may access the account by signing his or her own name. In that case, an identity verification requirement that may only be minimally burdensome for traditional banks offering depository accounts would create undue hardship for retailers and their customers. For customer convenience, retail credit card issuers often permit existing account holders to authorize another person to use the account to make retail purchases of goods or services from the retailer. The account holder remains liable for any obligations incurred. Additionally, retail credit card issuers may permit an account to be opened by two joint account holders. In such instances, both account holders are liable for the obligations incurred.

Most often, the authorized user of a retail credit card account is the spouse, child or other relative of the account holder. Before opening the account, the retail credit card issuer has completed a detailed and documented identity verification process. The account holder, under the retail credit card agreement, remains liable on the account when it is used by a person authorized to use the account. Thus, the account holder's information serves the law enforcement purpose underlying the proposed regulation. To impose additional detailed identity verification requirements would require a repetitive identity verification process, which would provide no better means of tracking the person responsible for the account. However, the cost to retail credit card issuers would result in the elimination of a program that U.S. consumers have used for decades as a convenient means of permitting family members, who may not otherwise qualify for credit, to obtain needed goods and services.

At the same time, there is no reason to believe that the additional identity verification requirements for authorized users would have *any* effect on terrorism or money laundering activities. An authorized user could simply use the card in the account holder's name to make the illicit purchases by telephone and over the Internet, and the card issuer would have no opportunity to prevent the illicit use. Moreover, creditors' acceptance of authorized users on credit card accounts is simply a convenience. If the effect of the regulation were to eliminate this feature, those who would use the card for illicit purposes might be inconvenienced along with the rest of the public, but their illegal activities would not be eliminated because of the ready availability of other, more convenient, means of completing the purchase.

The important thing is that, whenever an account is available to an authorized user, the retail credit card issuer has obtained identity information and verified the identity of the account

holder before the account is opened. As a result, the retail credit card issuer and, if necessary, law enforcement authorities, have a means of tracing any illegal activity to the account holder and, through the account holder, to the authorized user or joint account holder, the very purpose underlying the proposed regulation.

In order to retain the identity verification requirements for the account holder while removing the burden on retail credit card issuers and other banks relating to authorized users, NRF proposes the following modest revision to subsection 103.121(a)(3) (NRF's suggested language additions are shown in **bold-underline** and language struck from the existing draft is shown in [*bracketed italics*]):

(3) *Customer* means:

(i) Any person seeking to open an account; and

(ii) [*Any signatory on the account*] **Any person who is primarily obligated on the account**. [*at the time the account is opened and any new signatory added thereafter.*]

C. Recordkeeping

The proposed regulation requires that banks retain "all records for five years after the date the account is closed." § 103.121(b)(3)(ii). Unlike traditional banks who regularly service their account holders' accounts on a day-to-day, week-to-week, or month-to-month basis, retail credit card issuers often do not interact with their account holders for months or even years at a time. Some retail credit card holders have maintained open accounts for as long as thirty years.

The purpose of the proposed regulation is to provide a means, through identity verification, of eliminating the use of accounts for terrorist or money laundering purposes or, where such use occurs, to provide a means by which law enforcement can locate those responsible for the illegal activity. This is achieved by tying the account to a particular identified person at a particular location. Because a retail credit card account typically remains open until closed by the retailer due to inactivity or at the request of the customer, the requirement that the identity verification records be retained until five years after an account is closed imposes burdens upon the card issuers without achieving the purpose underlying the regulation and the USA PATRIOT Act.

Most consumers will move a number of times during the period any one retail credit card account is opened. For that reason, retention of the identity verification information provided when the account is opened provides little or no assistance to law enforcement authorities who will attempt to locate the customer after a terrorist or money laundering incident has occurred. Rather, to the extent that the regulation is intended to provide a record of the identity verification information provided when then account was opened, it should require that the information be retained for a time running from the date the account is opened. This change would recognize that such information becomes inaccurate over time as account holders move.

In order to retain the information provided by the customer for a period of time which would be most useful to law enforcement while limiting the recordkeeping burden upon retailers, NRF proposes the following modest revision to subsection 103.121(b)(3)(ii) (NRF's suggested

language additions are shown in **bold-underline** and language struck from the existing draft is shown in [*bracketed italics*]):

> (ii) The bank must retain all records for **twenty-five months from the date the account is opened.** [*five years after the date the account is closed.*]

The above modification provides for the retention of required records for the period of time during which it is useful. Moreover, because retail credit card issuers currently update account holder information when the customer moves, changes telephone numbers, or obtains a new job, and retain the updated information for twenty-five months, the updated information provides the best means of locating a customer should that become necessary and remains available to law enforcement under appropriate circumstances.

D. Effective date

If applied to retail credit card issuers, the proposed regulation's October 25, 2002 effective date would have devastating consequences. For retailers, the period between October 1 and February 1 is the busiest time of year as it includes the holiday shopping season and the post-holiday return period. Under the current regulatory schedule, comments on the proposed regulation must be submitted by September 6, 2002, leaving only a few weeks for those comments to be considered by the regulatory agencies and incorporated into the final rule. If the regulation becomes effective on October 25, banks (and affected retail credit card issuers) will have no time during which they can seek guidance regarding the interpretation, train their personnel, modify existing software, and test their compliance procedures. For retailers, this compliance burden is particularly difficult because it comes during a time when operational changes are traditionally kept to a minimum to avoid disrupting the holiday shopping season, the retailers' most important time of the year.

Moreover, to the extent that the proposed regulation requires that retail credit card issuers provide notice to account holders of their customer identification procedures, § 103.121(b)(5), retailers are at a singular disadvantage because they include retail credit card account applications in their catalogues, many of which are printed months in advance. Because retail credit card issuers currently provide notice to account applicants that they may obtain credit reports and other information to verify the applicant information provided, some period of accommodation will have to be allowed for the existing printed account applicant information so that retailers and retail credit card issuers are not left with catalogues which cannot be mailed during their busiest time of year.

Finally, given the time of year during which the proposed regulation will become effective, a delayed compliance deadline is necessary for affected retail credit card issuers to permit them to complete the holiday shopping and return season and implement the required procedures at a time when their limited resources can be devoted to the process. NRF believes that a compliance deadline on or about September 30, 2003 would provide retailers and retail credit card issuers with the appropriate period of time to implement the Customer Identification Program contemplated by the proposed regulation.

5. Practical Considerations

A. Required addresses to be obtained by retail credit card issuers

The proposal would require banks to obtain the current residence address and current mailing address, if different, for all customers. § 103.121(b)(2). This requirement presents serious concerns for retail credit card issuers and for their customers who may be concerned about the disclosure of private address information.

Many retail credit card issuers currently obtain only the applicant's mailing address for billing purposes. The card issuers' existing identity verification procedures, relying upon the existence of credit reports, permit the verification of existing and previous billing addresses. If required to obtain more than the billing address, credit card issuers will have to modify and test existing computer software, install the modified software at retail point-of-sale locations, and train personnel to obtain the additional information. Customers who use mailing addresses, as opposed to residence addresses, for legitimate purposes (e.g., active duty military personnel on overseas assignment; or those who share a multi-family dwelling with others and want to maintain the privacy of their financial information) will be required to disclose otherwise private information.

B. Promoting a paperless account opening process

To minimize the opportunities for identity theft, for customer convenience and to reduce transaction costs which can be passed along to account holders, retail credit card issuers have continued their adoption of automated and computerized account opening and servicing procedures. To the extent that they require the copying and maintenance of physical documents, the proposed regulation risks losing the advantages of these automated processes without providing any benefit in the reduction of terrorist or money laundering activities. As described above, each step in the proposed identity verification process exposes account holder information to theft and possible misuse. To the extent that this information can be retained electronically in secure computerized systems, as is the current procedure for virtually all retail credit card issuers, the customer's information is protected and the detailed identity verification information currently relied upon by retailers is securely retained.

C. The customer notice requirement

The proposed regulation requires banks to provide their customers with "adequate notice that the bank is requesting information to verify their identity." § 103.121(b)(5). Retail credit card issuers currently provide notice to account applicants in their application forms that the card issuer will obtain credit reports and, in some instances, other information to verify the applicant's identity. The proposed regulation could ease the anticipated compliance burden on retail credit card issuers by making clear that the required notice may be provided in or with the application and that such notice is alone sufficient to satisfy the adequate notice requirement.

6. Suggested Alternative Procedures

A. Existing procedures could be modified on a case-by-case basis

Although existing credit card issuer procedures adequately address the general risk of potential illegal use of retail credit accounts, NRF recognizes that on a card issuer-by-card issuer basis, the risk of illegal account use may vary. When such a risk is determined to be significant

by a regulator for a particular card issuer, NRF suggests that the required identity and identity verification procedures can be tailored for the particular risk posed. This could be accomplished during consultations between the affected retail credit card issuer and the agency following periodic reviews of the card issuer's practices. Such a procedure would further the risk-based approach underlying the proposed regulation without unduly burdening those card issuers whose accounts do not present a similar risk of terrorist or money laundering use.

B. Card issuer certification that a photo ID has been inspected

If it is determined that obtaining a government-issued photo ID should be a requirement for all point-of-sale, instant credit, retail credit account applications, NRF believes that it is sufficient for the person taking the account application to record specific information, either in writing or electronically, that would satisfy the identity verification requirements.[13] As mentioned, some retail credit card issuers currently require the person taking the application to record the identification number from a government-issued photo ID, the address shown on the ID, and date of issuance. Other card issuers require that the person taking the application compare the photograph on the ID to the person presenting it and indicate on the application processing form whether the comparison results in a match. The benefit of this type of procedure is that it minimizes the risk of identity theft while preserving the necessary information. Further, it permits the card issuer to retain all of the information securely in electronic form.

C. Recordkeeping for twenty-five months after account opening

The five year after account closing recordkeeping requirement in the proposed regulation appears to mirror the five year record retention requirement for documents relating to Suspicious Activity Reports. *See* 31 C.F.R. § 103.18. Many retailers currently retain the written application at the store location for twenty-five months and would be effectively required to retain the applications indefinitely under the proposed regulation. The value of the information provided to a retail credit card issuer at the time the account is opened diminishes over time as the account holder moves, obtains other employment, marries, etc. Other consumer oriented federal law, such as the Equal Credit Opportunity Act and Truth In Lending Act, recognize the immense burden placed on creditors by requiring that credit transaction related documents be retained for only twenty-five months. Imposing a recordkeeping requirement that is tied to the date the account is opened provides certainty for both the retail card issuer and law enforcement. Moreover, even if the information used to verify customer identity at the time the account is opened is discarded after twenty-five months, the retail card issuer will still maintain the account holder's most current billing information until the account is closed. This information, under appropriate circumstances, can be made available to law enforcement.

D. Delayed identity verification

If the inspection of a government-issued photo ID is determined to be a necessary identity verification requirement, retail credit card issuers should be able to complete such an inspection at the point-of-sale when the credit card is first used. This would allow card issuers to

---

[13] NRF emphasizes that some states drastically limit the type identifying information a retailer may record as part of a credit transaction. *See* Cal. Civ. Code § 1785.14. Before the regulation is finalized, potential conflicts with existing state law must be reconciled.

complete the detailed identity verification process currently employed while preventing the use of the account for any purchase until a person at the retail point-of-sale has requested, obtained, and inspected a valid photo ID. Such a procedure would allow retail card issuers to continue with their existing procedure of permitting the efficient extension of consumer credit while satisfying any requirement that a photo ID be inspected prior to the use of the account. The inspection could be certified electronically without the need to copy the ID card, thereby limiting the potential for identity theft and harm to retail credit customers.

7. Conclusion.

NRF recognizes that the regulatory process is on-going and that cooperation between regulators and those parties affected by the proposed regulation is essential to the successful implementation of the USA PATRIOT Act. We are ready to assist in any way to further explain the concerns highlighted above or to describe in greater detail the current procedures employed by retail credit card issuers who may be affected as "banks" under proposed regulation section 103.121.

Sincerely,

Mallory B. Duncan
Senior Vice President, General Counsel
National Retail Federation

Monica Anderson
Senior Corporate Counsel
National Retail Federation