Received CFTC
Records Section

02-9
(6)

Susan M. Walter
Vice President

9/10/02

Government Relations
General Electric Company
1299 Pennsylvania Avenue, N.W., Suite 1100
Washington, DC 20004-2407
202 637-4450, Fx: 202 637-4164
susanwalter@corporate.ge.com

COMMENT

September 6, 2002

Financial Crimes Enforcement Network
Section 326 Bank Rule Comments
Section 326 Broker-Dealer Rule Comments
Section 326 Mutual Fund Rule Comments
Section 326 Futures Industry Comments
P.O. Box 39
Vienna, Virginia 22183

Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave., N.W.
Washington, DC 20551
Attention: Docket No. R-1127

Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance Corp.
550 17th Street, N.W.
Washington, DC 20429

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

Office of the Comptroller of the Currency
250 E. Street, S.W.
Public Information Room, Mailstop 1-5
Washington, DC 20219
Attention: Docket No. 02-11

National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314-3428

Secretary
Securities and Exchange Commission
450 Fifth Street, N.W.
Washington, DC 20549-0609
Attention: File No. S7-25-02
File No. S7-26-02

Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581
Attention: Office of the Secretariat

Re: *Proposed Rulemakings to Implement Section 326 of the USA PATRIOT Act on Customer Identification*

Ladies and Gentlemen:

General Electric Company and its subsidiaries (collectively, "GE") appreciate the opportunity to comment on the joint notices of proposed rulemakings that would implement the customer information identification requirements contained in Section 326 of Title III of the USA PATRIOT Act of 2001 ("PATRIOT Act"). GE supports the government's efforts to combat money laundering and international terrorism and agrees with the government that the customer identification rules should be risk-based to prevent the diversion of scarce and valuable public and private resources from measures that are more

effective in combating money laundering and terrorism. However, these provisions potentially would have a widespread and adverse impact on the affected financial institutions with little resulting benefit to law enforcement.1

GE is committed to taking reasonable steps to assure compliance with applicable anti-money laundering laws and regulations and to prevent the use of our products and services in criminal activity, including terrorism and terrorist financing. For many years, GE has implemented comprehensive anti-money laundering compliance programs. We are recognized as an industry leader in preventing and detecting money laundering and other criminal activity and in cooperating with government authorities. GE Consumer Finance is a member of the Treasury Department's Bank Secrecy Act Advisory Group, and GE has participated actively in government initiatives to address the problem of money laundering through the Black Market Peso Exchange system. Since September 11th, we have increased our efforts throughout the company to assure that we meet and exceed best practices and government expectations for compliance with all PATRIOT Act and Office of Foreign Assets Control requirements. We are in close contact with both the FBI and the U.S. Customs Service to ensure that our countermeasures are effective and current.

GE puts a premium on identifying and verifying the identity of our customers. However, we do not believe that the proposed requirements would enhance the quality of the measures which we currently take to identify and know our customers, and implementation of certain aspects of the proposed rules would be extremely costly and burdensome for our businesses, including our banks that issue credit cards. While the preambles to the proposals state that the requirements are risk-based, the proposed requirements, especially for banks, only apply a risk assessment with respect to the methods of customer identification verification and, in some respects, are not practical and treat identification in a narrow sense. Recent events have shown that identities and documentation can be easily forged and that persons using their true identities can conduct financial transactions for evil purposes. Instead of devoting compliance resources to attempt to meet mechanical requirements that would not serve the purposes of the PATRIOT Act, we believe that our resources should be channeled into true risk-based customer due diligence. Time and money should not have to be spent to comply with requirements that in the end will have little impact on combating terrorism, terrorist financing and other criminal activity.

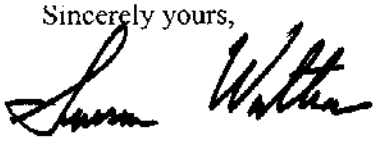
GE asks that you carefully review the attached comments on the various provisions of the proposals. After reviewing our comments and the many other comments that will be filed on the proposals, GE hopes that you will agree that the best course of action would be to revise the current proposals in favor of regulations with clear and more narrow definitions of "customer" and "account" and with requirements to obtain, verify, record and maintain customer identification information on a flexible, risk basis consistent with the statutory provisions of Section 326, but with substantially fewer compliance costs and burdens.

---

1 Among the GE companies that would be affected by the current proposed regulations are banks, securities broker-dealers and mutual funds. As other types of financial institutions under the BSA statute become subject to the anti-money compliance program requirement of Section 352 of the PATRIOT Act, Treasury has stated that those financial institution also may be subject to customer verification regulations. Therefore, in the future, customer identification requirements could be applied to many additional GE businesses, such as loan and finance companies (including certain leasing companies), certain investment companies (other than mutual funds), and some sellers of certain types of vehicles. If this were the case, those proposed rules could raise different issues which we would address at that time.

If you have any questions about any of the attached comments, please feel free to contact our outside counsel, Amy G. Rudnick, of the law firm of Gibson, Dunn & Crutcher LLP, at 202-955-8210 or arudnick@gibsondunn.com. We appreciate your careful consideration of these issues.

Sincerely yours,



Susan M. Walter

cc: Desk Officer for the Department of the Treasury
Office of Information and Regulatory Affairs
Office of Management and Budget
Paperwork Reduction Project (1506)
Washington, DC 20503

Amy G. Rudnick, Esq.
Gibson, Dunn & Crutcher LLP

GENERAL ELECTRIC COMPANY
COMMENTS ON PROPOSED RULEMAKINGS TO IMPLEMENT SECTION 326 OF THE USA PATRIOT ACT ON CUSTOMER IDENTIFICATION

A. Overview of Proposals

Under the various proposed regulations implementing Section 326 of the USA PATRIOT Act of 2001 ("PATRIOT Act"), banks, securities broker-dealers, futures commission merchants and their introducing brokers (together, "FCMs"), and mutual funds (collectively, "financial institutions") would be required to develop Customer Identification Programs ("CIPs") as part of their anti-money laundering programs under section 352 of the PATRIOT Act. At a minimum, prior to opening an account, a financial institution would have to obtain certain information about its customer, *i.e.*, name; date of birth (for individuals); residence (for individuals) or principal place of business address (for other customers) and mailing address, if different; and taxpayer identification number or number of a foreign government-issued document ("required information"). In addition, a financial institution would have to verify the identity of the customer under procedures set forth in the CIP within a reasonable time after an account is opened using documentary sources or other reliable sources of information to establish a reasonable belief that it knows the true identity of the customer and maintain records of all information obtained. In the case of banks and only banks, as proposed, *all* the required customer information would have to be verified; other financial institutions would be required to verify the customer's "identity" to the "extent reasonable and practical." Financial institutions also would have to determine whether a customer's name appears on lists of known or suspected terrorists provided by the federal government and, if there is a match, follow the government's instructions that accompany the lists.

B. General Comments

General Electric Company and its subsidiaries (collectively, "GE") commend the Department of the Treasury ("Treasury") and the federal functional regulators for adopting a risk-based and flexible approach to customer identification. GE agrees that a risk-based approach will result in effective compliance measures and focus compliance resources on those areas that pose the greatest money laundering and terrorist financing risks and believes that a consistent risk-based approach should be applied to all aspects of the rules. Our comments focus generally on issues related to: (1) the broad definitions of "account" and "customer;" (2) requirements to obtain, verify, record and maintain customer identification information; (3) requirements to check government lists of known or suspected terrorists; (4) the legal consequences of applying the rules to foreign branches of U.S. insured banks and (5) the need to provide a reasonable time to implement the rules.

C. Specific Comments

1. The Definition Of Account Is Overly Broad

a. The Bank Definition Of Account Should Be Limited To Accounts Through Which Customers Conduct Financial Transactions

In the proposed regulations for banks, the definition of account includes "each formal banking or business relationship to provide ongoing services, dealings or other financial transactions." We believe that this definition is overly broad and does not provide banks with sufficient guidance as to precisely what types of banking or business relationships would be subject to the customer identification requirements. As written, the term could be read to include relationships to provide services or dealings that do not involve accounts through which customers conduct financial transactions, *e.g.*, advisory services, referral services or third-party processing services. To be consistent with the proposed rules for broker-dealers and mutual

funds, which limit the types of transactions to financial transactions in securities and to provide clear guidance to banks, we would urge Treasury and the federal bank regulators to limit the bank definition of account to accounts through which customers conduct financial transactions. This could be done by keying the definition of account to definitions used in other banking regulations or in the Bank Secrecy Act ("BSA") regulations, *e.g.*, deposit account, transaction account and credit account.

We note that the definition of account for banks tracks the language contained in Section 311(c)(1)(A) of the PATRIOT Act. That definition, however, applies to Sections 5318(h) and (i) and 5318A of the BSA, which address customers, transactions and accounts that pose a money laundering concern. While we appreciate Treasury's and the bank regulators' desire to apply consistent definitions throughout the BSA, we do not believe that it is appropriate to use a definition intended for high-risk customers, transactions and accounts to all accounts at a bank. Consistent with the authority provided to Treasury and the regulators in Section 326, the regulations implementing Section 326 should take into consideration the various types of accounts maintained by the various financial institutions.

b. The Securities Broker-Dealer And Mutual Fund Definition Of Account Should Be Limited To Formal, Ongoing Relationships

Unlike the definition of account for banks, the definition of account in the proposed rules for securities broker-dealers and mutual funds is not limited to "ongoing" formal business relationships. Read broadly, the definition of account for broker-dealers and mutual funds could be interpreted to include isolated, one-off transactions where an account relationship with the broker-dealer or mutual fund is not established. To be consistent with the bank definition, Treasury and the Securities and Exchange Commission ("SEC") should limit the definition of account for broker-dealers and mutual funds to formal, ongoing relationships.

2. The Definition Of Customer Should Only Include Persons Who Open Accounts And Not Signatories Or Persons Authorized To Effect Transactions

a. The Bank Proposals Should Be Limited To Persons Who Actually Open An Account

In the bank proposals, the definition of customer is broadly defined to include any person "seeking to open an account." As discussed in more detail below, we believe that the bank definition should be limited to "any person who opens an account." This definition would be consistent with the proposed rules for securities broker-dealers, mutual funds and FCMs and the proposed rules' risk-based approach to customer identification. Moreover, any requirement to obtain information for customers who seek to open, but do not open an account, would be unreasonable, unworkable and impose substantial compliance costs and burdens on banks that would outweigh any law enforcement benefit.

While the statutory language of Section 326 refers to customers seeking to open an account, only the proposed bank rules track the statutory language. The proposed rules issued jointly by Treasury, the SEC and the Commodity Futures Trading Commission ("CFTC") for securities broker-dealers, mutual funds and FCMs, all limit the definition of customer to "any person who opens an account." We believe that it would be unfair and inconsistent with the regulators' intent to apply a different and more burdensome standard to banks than to other parts of the financial services industry covered by the proposals. *See e.g.*, 67 Fed. Reg. 48290, 48291 (July 23, 2002). Moreover, requiring banks to obtain information for customers who do not open accounts would be inconsistent with the rules' risk-based approach to customer identification. Customers who do not open accounts cannot effect transactions through the bank and, therefore, would not pose a risk of money laundering to the bank.

We also believe that it would be futile to require banks to obtain and verify identification information for customers for whom they do not open accounts. In many cases, the very reason that an account is not opened is because the person seeking to open the account did not provide the bank with all the required information or documentation or because the bank was unable to verify the information, *e.g.*, because the person does not have a driver's license or there is no credit report for the person. In other cases, the customer may have decided not to open an account or to obtain a credit card or a loan, because another bank or financial institution offered lower fees or better interest rates. Forcing a bank to expend valuable compliance resources to attempt to obtain information in these circumstances would be costly and wasteful.

In addition, requiring banks to obtain information for potential customers who do not open accounts is unnecessary. The BSA already provides banks with an effective and efficient mechanism to report this information to law enforcement in cases that raise suspicion. Under the BSA regulations, if a person were to attempt to open an account and to conduct a transaction in an amount that meets the reporting threshold and the attempted transaction were to raise suspicion, the bank would be required under the BSA regulations to file a Suspicious Activity Report ("SAR") with the Treasury Department's Financial Crimes Enforcement Network ("FinCEN").

b. Financial Institutions Should Not Be Required To Obtain And Verify Customer Identification Information For Signatories Or Authorized Parties

In the various proposed rules, the definition of customer includes not only the individual or legal entity opening the account, but also any signatory (bank proposals) or person who is granted authority to effect transactions through the account (other proposals). We believe that a requirement to obtain and verify customer information for all authorized signatories would

contravene the proposed rules' risk-based approach to customer identification and be infeasible, raise privacy concerns and impose substantial costs and burdens on financial institutions.

Key to customer identification is the requirement that a financial institution know its customer, not that it know the signatories or persons authorized to use an account with whom the financial institution may have no business relationship. Consistent with the proposed rules' risk-based approach to customer identification, financial institutions should be given the flexibility to conduct appropriate due diligence on its customers commensurate with the financial institution's assessment of the risks posed by the type of customer, account, and transactions that are conducted through the account. For those customer accounts that do not pose a high money laundering or terrorist financing risk, information and verification should be limited to the accountholder or, for credit cards (other than corporate credit cards) and other personal loans, to the person primarily liable for the payment of debt on the account. For corporate credit cards and other commercial loans, financial institutions only should be required to verify the identity of the business; financial institutions should not be required to obtain or verify the identification information of officers, employees or others who participate in the corporate credit card or other commercial loan program.

For example, financial institutions generally should not be required to obtain required customer information or verify the identity of authorized signers of accounts for customers that are legal entities, because the financial institution will have verified the identity of, and conducted due diligence on, the business customer on a risk basis. In most cases, the financial institutions should be able to rely on the fact that the signatories or authorized persons on the account are directors, officers, employees or other representatives of the business and that the business has verified their identity. In certain instances, however, it also may be appropriate for the financial institution to obtain and verify the identity of principals of closely-held

corporations, but the need to do so should be determined by the financial institution based upon the money laundering risk.

Financial institutions also should not be required to obtain and verify identification information for employees of federal, state, local and municipal government agencies and instrumentalities, including the U.S. Postal Service.[1] These employees will have been subject to appropriate government background checks prior to employment.

We believe that it would be extremely burdensome, costly and unworkable to require financial institutions to obtain identifying information for, and verify the identity of, all signatories on an account or all persons with authority to effect transactions through an account, and to make the accompanying form and systems changes to accommodate the information. This is particularly true for business accounts that may have hundreds of authorized signers who change frequently and who have no management involvement in the business. Similarly, multiple employees may have authority to draw down lines of credit granted to businesses. Business credit card accounts also may have numerous cards and subaccounts for officers, employees and other representatives of the business which may change daily, and personal credit cards may include spouses and children who are added to the account as a convenience to the primary card holder. Requiring financial institutions to obtain and verify identification for all authorized signers or users in these cases would be unrealistic and of little value to law

---

[1] In addition, financial institutions should not be required to obtain and verify required identification information for federal, state, local or municipal government agencies or instrumentalities that open accounts. For these customers, it should be sufficient for financial institutions to obtain the name and an address of the government agency or instrumentality and a letter or other appropriate documents from the government agency or instrumentality authorizing the opening of the account.

enforcement. The costs of modifying systems to accommodate and store this additional information cannot be justified.

Moreover, the requirement to obtain and verify the identity of the employees of a business customer raises legitimate privacy concerns about whether the employees should be required to disclose personal information and potentially their own credit histories to their *employer's* financial institutions. For instance, GE would not want to compromise the privacy of its employees who might be signatories to or have authority to conduct transactions through GE's accounts at financial institutions. In addition, supplying such information on GE's employees located in Europe and other jurisdictions with respect to GE accounts at U.S. financial institutions or foreign branches of U.S. banks may violate the privacy laws of those jurisdictions.

Finally, we note with concern that increasing the flow of personal information to banks and other financial institutions -- broadly defined in the BSA -- could have the unintended consequence of increasing the risk of compromising such information and, therefore, increasing the risk of identity theft.

3. Customer Identification

a. Financial Institution Should Be Given Flexibility To Obtain Identification Information Based Upon The Money Laundering Risk

All of the proposed rules would require financial institutions to obtain the customer's name; residence or principal place of business address and mailing address, if different; social security or other taxpayer identification number, or number of a foreign government-issued document; and date of birth. Consistent with the proposals' risk-based approach, we believe that the final rules should provide financial institutions with flexibility to determine what information should be obtained based upon the money laundering and terrorist financing risks posed by the type of customer, account and transactions to be conducted through the account. Financial

institutions should not be required to refuse to open an account if some information is missing but the financial institution otherwise is able to establish that it has a reasonable basis for knowing the customer. In particular, we do not believe that financial institutions should be required to obtain two addresses for a customer as a condition to opening an account.

b. Financial Institutions Only Should Be Required To Obtain One Address

All of the proposed rules would require financial institutions to obtain a residence address for an individual or a principal place of business address for an entity and a mailing address, if different. We believe that it should be sufficient for a financial institution to obtain one address for a customer.

Currently, the systems of some of GE's businesses only provide for one address. To facilitate communications with the customer, that address generally will be the customer's mailing address, which could be a residence or business street address for an individual; a principal place of business, local or other address for a business; a rural route number; or a post office box. In these cases, we believe that, so long as the financial institution can obtain and confirm sufficient identification information for its customer, it should not be required to obtain a residence or principal place of business address.

The burden and cost of obtaining two addresses and making accompanying systems changes to accommodate the information cannot be ignored. We estimate that it would take some of our businesses up to twelve months to modify and test their systems, including any interfaces with other systems, to add a second address field to record this information and to provide additional room to store the information. We do not believe that this cost or burden can be justified by the law enforcement benefit. However, if the final regulations were to require two addresses, we would urge Treasury and the other regulators to permit financial institutions to

accept a residence, business or rural route address for an individual or a principal place of business, local, route or other address where a business has a physical location for a business.[2] We also would strongly urge Treasury and the regulators to provide financial institutions with at least twelve months to make these changes.

4. Verification Of Customer Information

a. Banks Should Not Be Required To Verify All Required Customer Information

Unlike the other proposals, the proposed rules for banks appear to require the verification of *all* required customer information. We believe that it would be unreasonable and unfair to require *only* banks to verify all customer information. Such a requirement also would be inconsistent with the proposals' risk-based approach to customer identification and would pose practical problems for banks, particularly for accounts that are not opened in person.

Despite Treasury's stated purpose to impose standard identification requirements on all affected financial institutions, the proposed rules for banks require that every item of required customer information must be verified (*i.e.*, customer name, date of birth, residence or business address, mailing address, and taxpayer or foreign government-issued identification number). On the other hand, the proposed rules for securities broker-dealers, mutual funds and FCMs only require verification of the customer's identity to the extent reasonable and practical. We believe that it would be unfair to subject banks to a more onerous standard and to prohibit them from establishing or maintaining accounts in circumstances where other financial institutions would be able to have relationships. Like the other proposals, banks only should be required to verify the

---

[2] If the final regulations require a principal place of business address for an entity, a financial institution should be able to rely on a business customer's representation about which address it considers to be its principal place of business. Particularly for large complex businesses, the principal place of business may be difficult for a financial institution to determine.

customer's identity to the extent reasonable and practical; the reference to "verifying the information obtained pursuant to paragraph (b)(2)(i)" should be deleted from the bank rules.

In addition, verification of each item of required information would be impractical and, in some cases, impossible. For instance, credit bureau checks may verify some, but not all, items of required information. They may confirm the person's name and an address and that the social security number or taxpayer identification number matches information provided to the reporting agency, but not necessarily the person's date of birth or current address. Other commercial databases may verify customer name and a current or prior address and indicate that a social security number appears valid, but they may not confirm the customer's date of birth. A driver's license may confirm a customer's name, address and date of birth, but not the person's social security number. The lack of verification of a social security number, a date of birth or a current address should not prevent a bank from maintaining an account so long as it has a reasonable basis for confirming the customer's identity.

A requirement for financial institutions to verify each item of required customer information also would be inconsistent with the proposals' risk-based approach to customer identification. Consistent with that approach, a financial institution should be given the flexibility to determine how and what information it will verify to confirm the identity of its customers. This could be achieved by incorporating into the rules the language in the current preambles which states, *inter alia*, that a financial institution should verify information to the extent reasonable and practical to establish that it has a reasonable basis for knowing the true identity of its customer. The preambles to the final rules should make clear that there is no requirement to verify all required information.

b. It Currently Is Not Feasible To Require Verification Of Social Security Or Other Taxpayer Identification Numbers

Currently, there is no reliable, efficient or effective means of verifying a customer's social security or other taxpayer identification number. Because it would not be feasible to require verification of social security numbers at this time, we believe that the final rule should not mandate verification of social security numbers or other taxpayer identification numbers.

The proposals seem to suggest that a social security number could be verified by reference to a person's driver's license. However, in many states, the driver's license number is not the driver's social security number. Increasingly, for privacy reasons, states permit drivers to elect not to use their social security number as their driver's license number. Thus, if the driver's license did not include a social security number, however low the risk posed by the customer, a bank would be required to use a second source to confirm the person's social security number.

Currently, there is no other reliable method of verifying social security numbers. While commercial databases and credit bureau reports can be used to check social security numbers, generally they cannot confirm that a specific social security number has been provided to a particular person. Moreover, although the Social Security Administration ("SSA") has announced plans to develop a reliable service to allow financial institutions to verify taxpayer identification numbers, that system presently is not available. Until and unless the SSA can develop and make available an efficient, effective and secure system to "verify" social security numbers and other taxpayer identification numbers, financial institutions should not be required to verify social security numbers or other taxpayer identification numbers.

5. Document Collection And Retention

a. The Final Rules Should Make Clear That Financial Institutions Are Not Required To Retain Copies Of "Documents" Or Records Of The Results of Credit Bureau Reports Or Anti-Fraud or Other Automated Checks

The proposed rules would require financial institutions to keep a copy of any documents relied on to verify a customer's identity as well as a record of the methods and the results of any other measures taken to verify identification and to resolve any discrepancies. This would mean that identification documents would have to be copied and stored in paper form or imaged and stored in electronic form for five years after the account is closed. If other verification sources were used, *e.g.*., an Internet search or on-line review of press services were conducted, copies of the results of the search also might have to be maintained. Copying and storage of all this information, whether in paper or electronic form, would be burdensome, difficult to retrieve, expensive and of questionable law enforcement utility.

We believe that financial institutions should not be required to keep copies of any documents used to verify identification or copies of the results of any database or similar searches. Rather, financial institutions should be able to satisfy the recordkeeping requirement by recording the type of document or other method used to verify identity, for instance, by making a notation in its automated customer information files or other records and, where applicable, indicating the number and issuer of any document used to verify identity, *e.g.*, a driver's license. In those infrequent cases when a law enforcement agency seeks this information, law enforcement could obtain a copy of the underlying document from the government agency that issued the document, *e.g.*, the Department of Motor Vehicles.

Moreover, financial institutions should not be required to maintain records of credit bureau reports or internal or external anti-fraud checks or other automated processes, particularly

where the checks do not disclose any negative information or routine checks resolve discrepancies. In these circumstances, it should be sufficient to include in the financial institution's CIP the steps that are required to confirm customer information and to record the results of any additional steps that may be taken to resolve any significant discrepancies.

b. Identification Documentation Should Not Be Required To Be Recorded Or Maintained For Credit Cards Issued At The Point Of Sale

Any requirements to record and retain identification documentation for credit cards issued by banks to customers who are present at retail stores, such as department stores, pose particular problems. Most of the credit cards issued by GE banks are issued while the customer is present at the retail store. For many of these stores, 90% or more of GE's credit card accounts are opened at the "point-of-sale," enabling immediate purchases. There is a critical need for speed and efficiency in the point-of-sale credit application process in order to facilitate retail sales. We are concerned that the proposed rules for banks could be read to require that the issuing bank or retail store record and maintain a copy of an identification document for the customer, such as a drivers license, thus unduly slowing down and hindering the retail sales process.

Under an arrangement with issuing banks, retail store customers can open "instant credit" accounts for immediate and future purchases at the "point of sale," *e.g.*, at the sales counter at any register in the store, generally by filling out a short application form. The information on the application form then is relayed electronically to the bank which will evaluate creditworthiness, verify that the information provided by the customer is consistent with the information in the customer's credit report, and perform a number of other anti-fraud checks. This review is consistent with the review conducted of our other credit card applicants, including persons who obtain credit cards through the mail or over the Internet. In all cases, credit card issuers have an

inherent incentive and need to identify and verify their customers' identity to ensure that their accounts will be repaid and to prevent possible fraud. Because credit card accounts opened at the point-of-sale can be used for immediate purchases, however, the sales associate also is required to confirm the customer's identity by viewing an identification document. However, this information is not always retained by the sales associate or relayed to the credit card bank.

Even though the bank is not provided with information about the document used by the sales associate to confirm the customer's identity, we are concerned that the proposed regulations could be read to require that either the bank or the retail store record and/or maintain a copy of any identification document viewed by the sales associate. In the case of credit cards opened at retail stores, we believe that the bank should be able to rely on the information that it uses to confirm identification, *i.e.*, a credit bureau report and other fraud checks.[3] We do not think that retail stores should be required to forward the identification that it uses to confirm the customer's identity to the bank or to copy and maintain the identification document itself. Requiring the store to obtain and forward the information electronically would require extensive systems changes, and requiring stores to copy and retain the document used to verify identification would be burdensome, costly and unworkable in practice and could result in lenders sharply curtailing or eliminating the availability of instant credit in retail transactions, which would have an adverse impact on retail sales and consumer spending. In addition, retail customers would encounter long waits to make a purchase while customers in front of them have their information copied and their transaction completed. There also is a concern that a proliferation of copies of

---

[3] This could be accomplished by modifying the language of the proposed rule to read that the bank retain "a copy of any document that *the bank* relied on" in the performance of its CIP.

identification documents or records used to verify identity, however carefully maintained, could fall into the wrong hands and facilitate identity theft or other fraud.

6. The Regulations Should Specify What Government Lists Must Be Checked And Provide A Mechanism For Communicating That Information

Consistent with the statutory provisions of Section 326, financial institutions will be required to check names of customers against government lists of known or suspected terrorists and follow the instructions accompanying the lists. Financial institutions other than mutual funds will be required to check names against lists provided by any federal government agency; mutual funds will be required to check names against lists prepared by any federal government agency and made available to the mutual fund. None of the proposals, however, identifies which government lists financial institutions must check or whether they must check any list provided by any federal government agency. Financial institutions should not be held to such a vague regulatory standard and should not have to check customer names against a myriad of lists coming from numerous government sources.

To provide certainty to financial institutions as to what federal government lists must be checked and the appropriate actions to be taken, Treasury and the federal functional regulators should specify in the final rules the lists that financial institutions must check, *e.g.*, the Office of Foreign Assets Control ("OFAC") lists of terrorists or the FBI Control List, and require that any federal government agency that provides a list include specific instructions as to what actions financial institutions should take if a name of a prospective or existing customer matches a name on one of the lists, *e.g.*, if there is a match with the FBI Control List, state whether the financial institution is required or permitted to refuse to open the account or whether the financial institution must or may close or maintain an existing account. In addition, the final rules should identify which federal government agency or agencies may provide lists of known and suspected

terrorists to financial institutions and through what mechanism. For instance, the rule could provide that only FinCEN may provide the lists to financial institutions and that those lists must be provided in accordance with the information sharing mechanism provided in Section 314 of the PATRIOT Act. The rules also should indicate whether there will be a continuing duty for financial institutions to check all new customers against the lists and existing customers against updated lists, similar to OFAC requirements or only when supplements to the list are provided to the financial institution.

Because GE consists of many different businesses, GE also seeks confirmation that a financial institution only is obligated to check those lists provided to it by the federal government. Affiliates of financial institutions should not be required to check the lists unless the affiliate is provided with the list by an appropriate federal government agency.

8. The Rules Should Not Apply To Foreign Branches Of U.S. Insured Banks

The proposed customer identification rules for banks would apply to all foreign branches of U.S. insured banks. We think that it would be unreasonable and unnecessary to apply the rules extraterritorially to require foreign branches of U.S. insured banks to comply with U.S. rules, at least in countries that are members of the Financial Action Task Force on Money Laundering ("FATF") or countries that have comparable customer verification requirements. Moreover, as Treasury and the agencies recognize in the preambles to the proposed rules, compliance by foreign branches with U.S. requirements may cause practical difficulties and conflict with local laws, particularly privacy laws and laws that limit the use of government identifiers. We do not believe that U.S. banks should be put in the untenable position of having to violate either local or U.S. law. For this reason, rather than requiring U.S. banks to apply their CIPs globally, we would urge Treasury and the bank regulators to permit U.S. banks to develop

and implement CIPs for their foreign branches that comply with local laws, at least for those branches that are located in countries that are FATF members or that have similar requirements. If a branch is located in a jurisdiction that is not a FATF member or that does not have comparable laws, the branch only should be required to comply with U.S. requirements to the extent that the U.S. requirements do not conflict with local laws. In no case should a U.S. bank be required to comply with U.S. requirements that conflict with local law.

9. The Effective Date Of The Final Rules Should Be Delayed To Permit Implementation

Regulations under Section 326 are required to be in effect by October 25, 2002. While the final regulations may be issued by that date, it is unlikely that financial institutions will have sufficient time to develop, modify and implement new policies, forms and systems by October 25th. As discussed above, some systems of GE businesses' currently can accommodate only one address for a customer and, consequently, would not be able to accommodate both a residence or principal business address *and* a mailing address or an address for a secondary accountholder. Moreover, GE's banks and other financial institutions typically do not obtain or include in their systems customer information or verification for authorized signatories or users. As a consequence, application forms would have to be changed, fields would have to be added to current systems to record customer identification information and the method used to verify a customer's identification, and systems would have to be expanded to provide room to store additional information.

While GE businesses will take steps promptly to comply with any new requirements, it is important that they be provided with a reasonable period of time to make the necessary changes to policies, procedures, forms, systems, document retention procedures and training programs. Particularly, given the extensive systems changes that would be involved in complying with the

rules as proposed, the moratorium many financial institutions' service providers put on systems changes at the end of the year, and the impact that such changes would have on retail stores during the holiday season, GE urges Treasury and the regulators to provide financial institutions with six months from the effective date of the final rule to develop a CIP plan for implementing the new rules and at least 12 months to implement the main elements of the CIP thereafter.

70219623_11.DOC