RUSSELL W. SCHRADER
Senior Vice President
Assistant General Counsel

VISA

May 4, 2005

By Electronic Delivery

Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Attention: Docket No. OP-1220

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Attention: EGRPRA Burden Reduction Comments

Public Information Room
Office of the Comptroller of the Currency
250 E Street, SW
Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 05-01

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 2005-02

Re: Request for Burden Reduction Recommendations

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa U.S.A. Inc. in response to the notice of regulatory review ("Notice") and request for public comment by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Office of Thrift Supervision (collectively, the "Agencies"), published in the Federal Register on February 3, 2005. The Notice seeks public comment concerning ways to reduce the burdens associated with regulations in the following three categories: "Money Laundering, Safety and Soundness, and Securities." Visa appreciates the opportunity to comment on this important matter.

The Visa Payment System, of which Visa U.S.A.[1] is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. For calendar year 2004, Visa U.S.A. card purchases exceeded a trillion dollars, with over 450 million Visa cards in circulation. Visa plays a pivotal role in advancing new payment products and technologies, including technology

[1] Visa U.S.A. is a membership organization comprised of U.S. financial institutions licensed to use the Visa service marks in connection with payment systems.

VISA U.S.A. INC.
Post Office Box 194607
San Francisco, CA 94119-4607
U.S.A.
Phone 415 932 2178
FAX 415 932 2525

initiatives for protecting personal information and preventing identity theft and other fraud, for the benefit of Visa's member financial institutions and their hundreds of millions of cardholders.

Visa is providing comments with respect to the Agencies' existing and contemplated requirements promulgated pursuant to the following rules:

- The Interagency Guidelines Establishing Information Security Standards ("Guidelines"),[2] promulgated under section 501(b) of the Gramm-Leach-Bliley Act ("GLBA");[3]

- The Customer Identification Program ("CIP") rule, promulgated under section 326 of the USA PATRIOT Act;[4] and

- The Identity theft prevention program ("ID Theft Program") rules, which the Agencies and the Federal Trade Commission ("FTC") will jointly propose under section 114 of the Fair and Accurate Credit Transaction Act of 2003 ("FACT Act").[5]

Visa appreciates that the Agencies have worked diligently to develop consistent approaches for these program rules, and notwithstanding the different purposes of these statutes, Visa believes that the Agencies are aware that these distinct regulatory frameworks impose substantial compliance costs on financial institutions. Accordingly, Visa believes that the Agencies can and should take additional steps to modify or eliminate unduly burdensome regulatory requirements in order to enable financial institutions, including Visa's members, to streamline their compliance efforts with respect to these rules. In particular, Visa believes it is important for the Agencies to amend these rules to expressly state that financial institutions can apply the measures used to comply with the requirements of one of these rules to comply with similar requirements under the other rules.

In addition, Visa believes that the Agencies can and should adopt, through a process of public comment, interagency guidance with respect to these rules. In this regard, interagency interpretive guidance would enable financial institutions to more effectively comply with these overlapping regulatory requirements in the context of particular situations; for example, recently issued interagency interpretive guidance regarding the application of the USA PATRIOT Act CIP rule assists financial institutions with various compliance issues that might arise in

---

[2] The Guidelines previously were entitled "Interagency Guidelines Establishing Standards for Safeguarding Customer Information." *See* 66 Fed. Reg. 8616 (Feb. 1, 2001). The Agencies recently changed the title of the Guidelines to reflect a financial institution's broader obligations to implement a program designed to accomplish other purposes, such as properly disposing of information about a consumer derived from a consumer report. *See* Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003, 69 Fed. Reg. 77,610, 77,611 n.7 (Dec. 28, 2004).

[3] 15 U.S.C. § 6801(b).

[4] 31 U.S.C. § 5318(*l*).

[5] 15 U.S.C. § 1681m.

connection with the CIP rule.[6] Visa urges the Agencies to seek public comment on any proposed interpretive guidance because these interpretations may pose far-reaching implications that can be addressed more effectively through a public comment process.

SIMPLIFY THE PROGRAM RULES FOR SAFEGUARDING AND USING INFORMATION

Visa believes that a regulatory framework that requires financial institutions to develop *risk-adjusted programs* designed to accomplish the objectives of the related rules is appropriate and Visa commends the Agencies for implementing such program rules under the GLBA and the USA PATRIOT Act. In contrast to detailed prescriptive regulations that inflexibly regulate every facet of a financial institution's security controls and verification methods, the Agencies' risk-adjusted program rules provide an appropriate degree of discretion for a financial institution to satisfy its legal obligations in a manner that is consistent with the particular features of that institution's business, customer base and operations.

Section 114 of the FACT Act requires the Agencies and the FTC to jointly prescribe a rule "requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines established [by the Agencies and the FTC regarding identity theft]."[7] In doing so, Visa urges the Agencies and the FTC to jointly prescribe a similar risk-adjusted program rule to implement the requirements of section 114 of the FACT Act, rather than prescriptive regulatory requirements. An ID Theft Program that is consistent with and builds on a financial institution's GLBA information security program and USA PATRIOT Act customer identification program would allow the institution to develop and maintain policies and procedures designed to protect individuals against identity theft in ways that are appropriately tailored to the risks that the institution has identified as relevant to its particular business, customer base and operations.

STREAMLINE THE PROCESSES FOR CONDUCTING RISK ASSESSMENTS

A key component to both a GLBA information security program and a USA PATRIOT Act customer identification program is an assessment of the reasonably foreseeable risks that affect the financial institution's customer information, customer information systems and accounts that might be susceptible for use in money laundering. Although the purposes of the requirements and the risks that pertain to an institution's information security program and its customer identification program may vary in certain respects, both risk assessments essentially cover the same product lines. In this regard, no provision in the GLBA Guidelines or the USA PATRIOT Act CIP rule specifically precludes a financial institution from consolidating the processes it uses to conduct these risk assessments where appropriate, but the Agencies have not issued any interpretations or other guidance that would make it clear that an institution may combine its efforts to develop and update the risk assessments required by these two rules.

---

[6] *See* FAQs: Final CIP Rule (April 2005), *available at* http://www.occ.treas.gov/ftp/release/2005-42a.pdf. Visa believes that this interagency interpretive guidance also may have been enhanced by a public comment process.

[7] 15 U.S.C. § 1681m(e)(B).

Visa believes that the Agencies can and should clearly state in writing that financial institutions are permitted to use a single process to identify and assess the reasonably foreseeable risks that relate to this combination of compliance programs, instead of undertaking separate processes for each program that require institutions to replicate these processes. Conducting a risk assessment for each such program that consistently assesses various aspects of each product or service—classifying the types of existing and future customers, creating an inventory of the information used or stored in connection with providing the product or service, ascertaining which services providers are associated with the product, and so on—involves substantial resources and time. In many cases, an institution must assemble staff from various affiliates, divisions or business units in order to do so. As a result, Visa urges the Agencies to expressly state in each of these rules that a financial institution is permitted to use a single risk assessment developed to comply with the applicable set of requirements under one rule, to satisfy the applicable requirements of another rule. More specifically, Visa urges the Agencies to propose a joint rule that expressly allows a financial institution to use the same risk assessment process that it uses for its GLBA information security program to satisfy the requirements of its other compliance programs, such as those required for the USA PATRIOT Act customer identification program and the FACT Act ID Theft Program.

JOINT RULE FOR ID THEFT PROGRAMS SHOULD INCORPORATE EXISTING REQUIREMENTS

Visa also believes that the Agencies should seize the opportunity presented by the rulemaking that will be initiated under section 114 of the FACT Act to avoid the potential burden associated with maintaining various programs for safeguarding customer information and customer identification and verification.

Visa believes that financial institutions already are substantially required under the GLBA Guidelines to establish "reasonable policies and procedures" regarding certain aspects of "identity theft with respect to [their] account holders [or their] customers," as described in section 114 of the FACT Act. These aspects include the protection of information about existing customers under the GLBA Guidelines and the identification of new customers under the USA PATRIOT Act CIP rule. As a result, additional regulatory requirements, if any, should be carefully designed so that financial institutions can streamline their compliance efforts by adopting ID Theft Programs that operate efficiently for all of their customers, regardless of whether those individuals reside, and are consistent with and not duplicative of, existing requirements under the GLBA Guidelines and the USA PATRIOT Act CIP rule.[8] For example, the joint rules under section 114 of the FACT Act should make it clear that financial institutions may use, as part of their ID Theft Program, the identification and verification methods currently used in their customer identification programs to detect the possible existence of identity theft. Similarly, the joint rules should make it clear that financial institutions may use the customer

[8] Other than the following examples, Visa is not offering specific comments on the particular requirements under section 114 of the FACT Act that the Agencies will propose for public comment. Visa believes that the appropriate time and forum for providing comment on the particular requirements under this section of the FACT Act is in the course of the upcoming rulemaking proceedings.

notification procedures currently used in their response programs, as required under the GLBA Guidelines,[9] to mitigate the potential harm to their customers due to identity theft.

PRESCRIPTIVE REQUIREMENTS OF THE BANK SECRECY ACT RULES SHOULD BE AMENDED OR ELIMINATED

Visa commends the Agencies for working with officials from the Department of the Treasury ("Treasury") and the Department of Justice in an effort to enhance the understanding of those agencies on the efforts of banks and federal banking officials to ensure compliance with the Bank Secrecy Act ("BSA"). Nevertheless, the Agencies and the banking industry can continue building productive relationships with federal and state law enforcement authorities only if law enforcement officials truly understand the compliance obligations and efforts of financial institutions.

In addition, Visa urges the Agencies to work together with the Treasury and the Financial Crimes Enforcement Network ("FinCEN") to streamline or eliminate many of the existing prescriptive regulatory requirements of the BSA. Visa believes that these requirements are costly and duplicative in light of the corresponding obligations of financial institutions to maintain risk-based anti-money laundering ("AML") programs designed to prevent and detect money laundering and other crimes. Various components of a financial institution's AML program can adequately achieve the purposes of the existing BSA prescriptive regulatory requirements, and accordingly, the Agencies should work with the Treasury to streamline or eliminate those BSA regulatory requirements.

Foremost among the steps that the Agencies should take to streamline compliance with the BSA and the implementing regulations is a common framework for conducting examinations. Visa applauds the ongoing interagency efforts to jointly develop standards for conducting BSA exams, such as the recently issued interagency interpretive guidance on BSA compliance requirements when providing services to money services businesses.[10] Visa believes that the Agencies should build on their efforts in this area to develop guidance that, at a minimum, can assist financial institutions in taking practical steps to prepare for the complex aspects of BSA exams, such as the procedures recommended to be used to assess whether customers should be classified as "high risk."

RAISE DOLLAR AMOUNT THRESHOLDS AND SIMPLIFY REQUIREMENTS FOR FILING REPORTS

Visa also believes that the thresholds should be raised for filing a suspicious activity report ("SAR"), a cash transaction report ("CTR"), and the recordkeeping requirements for monetary instruments. The amounts that trigger filing and maintaining these respective reports

---

[9] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (to be codified as Supp. A to the Agencies' respective rules for the Guidelines), 70 Fed. Reg. 15,736, 15,751 (Mar. 29, 2005).

[10] Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States (Apr. 26, 2005), *available at* http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20050426/attachment.pdf.

might have been appropriate years ago, but the thresholds now are too low. As a result, financial institutions file reports that, in many cases, do not provide benefits to law enforcement agencies commensurate with the time and resources required to prepare, file and analyze those reports.

Visa recommends that the Agencies work together with the Treasury and FinCEN to establish higher thresholds, such as $15,000 for a SAR and $30,000 for a CTR. Similarly, Visa supports amending the BSA to delegate to the Treasury the authority to establish higher thresholds for maintaining records of certain monetary transactions, and Visa believes that the Treasury should exercise such delegated authority to establish the threshold for requiring records for certain monetary transactions at not less than $15,000.

BIENNIAL RENEWAL OF EXEMPT CUSTOMERS IS UNNECESSARY

In addition, Visa believes that the requirement to file biennial reports to continue to treat a customer as an exempt person should be modified. Instead of prescriptive regulatory requirements for certification forms to be filed every two years, the rule should simply allow a financial institution to maintain an exemption so long as the person satisfies the applicable requirements. Correspondingly, the amended rule should require an institution to terminate the exemption for any person when that person no longer qualifies for one. For example, if after a period of time a financial institution observes that a commercial enterprise which is exempt for withdrawals for payroll purposes infrequently withdraws more than the threshold amount, then the institution can conclude that the person no longer qualifies for the exemption.[11] Even after the Agencies amend the BSA regulations in this fashion, financial institutions still would be required to monitor transactions with their customers to detect and prevent money laundering. Financial institutions should be permitted appropriate discretion to periodically assess, as part of their AML programs, whether customers continue to qualify for exemptions from filing a CTR.

Visa appreciates the opportunity to comment on this important matter. If you have any questions concerning these comments, or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me, at (415) 932-2178.

Sincerely,

Russell W. Schrader
Senior Vice President and
Assistant General Counsel

[11] 31 C.F.R. § 103.22(d)(2)(vii)(B) (exempting a person solely with respect to payroll purposes if, among other requirements, the person "[o]perates a firm that regularly withdraws" more than the threshold amount).