(716) 841-5733

September 18, 2006

Office of the Comptroller of the Currency
250 E Street, S.W.
Public Reference Room, Mail Stop 1-5
Washington, D.C. 20219
Docket No. 06-07

Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551
Docket No. R-1255

Re: Identity Theft Red Flags under the FACT Act

Dear Sir or Madam:

HSBC North America Holdings Inc. ("HNAH") submits this comment letter in response to the Proposed Rule ("Proposal") issued by the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System (the "Board"), the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision (together, the "Agencies"), regarding identity theft red flags and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003. HNAH is a registered financial holding company with various U.S. banking and nonbanking subsidiaries, including two national banks, HSBC Bank Nevada, N.A. and HSBC Bank USA, National Association that would be subject to the Proposal. We appreciate this opportunity to submit comments.

Summary of Comments

The Agencies have stated their intent, in promulgating the proposed rules (the "Proposal"), to provide a "flexible risk-based approach" to implement the Red Flag Regulations similar to that used in the "Interagency Guidelines Establishing Information Security Standards (the "Information Security Standards"). We agree that this should be the goal of the Red Flag regulations. By following the approach used in the Information Security Standards, the Agencies will permit a financial institution to implement a comprehensive identity theft prevention program tailored to the risks specific to that institution. We are concerned, however, that the Proposal is overly prescriptive and will, in fact, complicate the efforts of financial institutions to detect and prevent identity theft by requiring them to spend time on procedures that do not necessarily address high risk factors.

The following summarizes our comments on specific portions of the Proposal.

Definitions.

The term "account" is defined as a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in a financial activity under § 4(k) of the Bank Holding Company Act. Since the term "account" is already defined in the Fair Credit Reporting Act as a demand deposit or similar consumer asset account, we believe that the Proposal should avoid using the same term to address a broader concept. The term "continuing relationship" has been proposed as an alternative by other commenters and we agree that this term could be used in place of "account" without affecting the substance of the Proposal.

The Supplementary Information indicates that the term "account" is intended to include business accounts, and that the term "customer" includes partnerships, corporations, trusts, and government entities. We strongly urge the Agencies to exclude business purpose accounts from the application of the Red Flag regulations. Many of the Red Flags listed in Appendix J are related to consumer reports and personal identification information. While this information may be obtained for principals in a business transaction, it is not used as a means of verifying the identity of the business that is obtaining the account relationship. In our experience, commercial accounts, including small business accounts, are at much less risk of being the target of identity theft. By expanding the scope of these definitions to include commercial accounts and entities other than individuals, the Proposal will require financial institutions to create procedures to address Red Flags for transactions where the risk of such fraud is relatively low and for which those Red Flags have limited application. Financial institutions should be allowed to direct their fraud prevention resources to the areas of highest risk.

The Agencies have requested comment on whether the definition of "account" should include relationships that are not continuing. Accounts that are not continuing should not be included if: 1) a customer cannot re-establish a relationship with a financial institution solely at its request and, 2) a credit review by the institution is required to re-establish the account. The risks of identity theft on relationships that are not continuing are mitigated through controls established in the credit review process to detect fraud.

Identity Theft Program

We agree with the Agencies that the approach provided in the Information Security Standards should be used as a model for development of the Identity Theft Prevention Program (the "Program"). While the Information Security Standards identify

some specific considerations for management and control of identified risks, they generally permit financial institutions to make their own assessments of information security risks and develop policies and procedures appropriate to those risks. They do not dictate procedures that must be implemented to meet the required objectives.

The requirement that institutions develop policies and procedures to detect Red Flags that pose a "possible risk of identity theft" implies that institutions must identify all risks and develop procedures to prevent or mitigate them, without regard to the significance of the risk. This requirement seems inconsistent with the Agencies' intent to create a flexible risk-based approach.

The list of Red Flags identified in the Appendix may be useful examples of current Red Flags, but the Proposal should clearly state that the list is provided only for purposes of illustration. Without that clarification, we are concerned that the list may be used by examiners as a required list for consideration by all institutions in their Programs. Institutions should be permitted to use their own experience and expertise to identify the Red Flags most relevant to their business. The focus on this portion of the Program should be assessment of risk factors based on likelihood and significance of those risks to the assessing institution, rather than mere enumeration of all possible risks.

As is the case with the Information Security Standards, the Proposal should state the objective of the Program and give financial institutions sufficient flexibility to achieve that objective, without dictating a specific process.

Oversight for Service Provider Arrangements

The Agencies have requested comment on whether the objectives of the Program can be fulfilled if service providers are permitted to implement a Program that differs from the programs of the financial institutions for which they provide services. We believe that the Proposal correctly addresses the role of service providers. A service provider must have flexibility to meet the objectives of the Proposal without having to tailor its services to the Program requirements of each company for which it provides service. A similar approach is taken in the Information Security Standards, and we believe that it is the correct approach for the Final Rule.

Involvement of Board of Directors or Senior Management

The Proposal requires that the board of directors or an appropriate committee of the board approve the Program. It also requires the board, an appropriate committee of the board, or senior management, to oversee the development, implementation and maintenance of the Program. We are concerned that this level of board oversight will inhibit the ability of financial institutions to respond quickly to new fraud schemes by delaying implementation of appropriate Program modifications. Documents requiring

board or board committee approval require extensive and time-consuming preparation. The board approval process is therefore not appropriate for policies and procedures requiring rapid response. Moreover, the Agencies recognize that not all financial institutions have a board of directors and permit those institutions to designate an employee to fill that role, thereby inequitably assigning the burdensome board approval requirement to some, but not all, institutions. We request that this portion of the Proposal be revised to permit all institutions to appoint an appropriate member of senior management to be responsible for the development and implementation of the Program.

Duties of Users of Consumer Reports Regarding Address Discrepancies

Section 605(h) of the FCRA requires a User of consumer reports to form a reasonable belief that the User knows the identity of the consumer. We support the Agencies' inclusion in the Proposal of the statement that a User that employs the procedures set forth in the Customer Identification Program ("CIP") rules of the USA Patriot Act Section 326 satisfies the requirement to verify the identity of a consumer for whom it has received a notice of an address discrepancy. However, the Agencies should clarify the statement in the Supplementary Information that reliance on its CIP for compliance with the rule applies only if the User applies its CIP policies in all situations where it receives notice of a discrepancy. Since reliance on CIP may not be necessary in all cases, we do not understand why a choice to not use CIP in some cases would negate a process that is otherwise deemed compliant.

Duties of Card Issuers Regarding Changes of Address

The Proposal requires credit and debit card issuers to implement reasonable policies and procedures to assess the validity of change of address requests. We urge the Agencies to give financial institutions broad discretion in verifying address changes. For example, verification of the customer's identity through use of CIP is an effective means of verifying the validity of an address change and should be considered a reasonable means of meeting this obligation. Requiring additional procedures to assess the validity of the change would be redundant in cases where the institution has confirmed the identity of the customer that is making the request. In addition, the financial institution should have the discretion to rely on its experience in determining whether an address change is valid. For example, a request of address change within the same rural geographic area is, in our experience, a low fraud risk and may not require further investigation. On the other hand, a change from a rural address to an address with a high known incidence of fraud requires a different level of investigation.

Effective Date

We request that the Agencies provide institutions with sufficient opportunity to review and implement the Final Rule. We believe it would be appropriate to establish an

immediate effective date of the Final Rule with mandatory compliance required at least one year after it is published in the *Federal Register***.** This will give institutions the ability to conduct an inventory of existing operations while developing new programs that may be necessary for compliance.

We appreciate the opportunity to comment on the Proposal.

Sincerely,

Patricia N. Grace
Deputy General Counsel
HSBC Bank USA, National Association
(716) 841-5733

PNG\PRIVACY TASK FORCE\Red Flag comments