The PNC Financial Services Group, Inc.
249 Fifth Avenue
One PNC Plaza, 21st Floor
Pittsburgh, PA 15222-2707

412 768-4251 Tel
412 705-2679 Fax
james.keller@pnc.com

James S. Keller
Chief Regulatory Counsel

September 18, 2006

Office of the Comptroller of the Currency
250 E Street, SW
Public Information Room, Mailstop 1-5
Washington, DC 20219
regs.comments@occ.treas.gov
Attn.: Docket No. 06-07

Mr. Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Comments@FDIC.gov
Attn.: Comments/Legal ESS
RIN 3084-AA94

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
regs.comments@federalreserve.gov
Attn.: Docket No. R-1255

RE: Joint Notice of Proposed Rulemaking on Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003

Ladies and Gentlemen:

The PNC Financial Services Group, Inc. ("PNC"), and its principal subsidiary bank, PNC Bank, National Association ("PNC Bank"), both of Pittsburgh, Pennsylvania, are pleased to respond to the request for comments on the notice of proposed rulemaking regarding identity theft red flags and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003 (71 Fed. Reg. 40786 (July 18, 2006)) ("Proposal"). PNC Bank is the principal subsidiary bank of The PNC Financial Services Group, Inc., ("PNC"), Pittsburgh, Pennsylvania, which is one of the largest diversified financial services companies in the United States, with $94.9 billion in assets as of June 30, 2006. PNC engages in retail banking, institutional banking, asset management, and global fund processing services. PNC Bank has branches in the District of Columbia, Florida, Indiana, Kentucky, Maryland, New Jersey, Ohio, Pennsylvania and Virginia. PNC also has a state non-member bank subsidiary, PNC Bank, Delaware, Wilmington, Delaware, which has branches in Delaware.

PNC respectfully submits its comments to the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation (together, the "Agencies") and would like to thank the Agencies for the opportunity to

comment on the Proposal. This letter responds to the Agencies' request for comments on the proposal to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act").

American Bankers Association Comment

Initially, PNC would like to note that it has participated in industry meetings culminating in the creation of a comprehensive comment letter by the American Bankers Association ("ABA") on this Proposal, and that we support the recommendations made therein. In particular, we would like to reiterate the ABA recommendations that (1) the Agencies provide that a financial institution may take into account the cost and effectiveness of policies and procedures and the institution's history of fraud in creating its Identity Theft Prevention Program, and (2) the Agencies adopt an approach that will allow a financial institution more discretion and flexibility in the creation of its Identity Theft Prevention Program, rather than setting forth factors that an institution must consider in determining whether the Red Flags contained within the Proposal are relevant. We do consider many of the Red Flags in the process of opening accounts, but they may be factored into our credit scoring models or elsewhere in the account opening process, rather than separate stand-alone processes.

In addition to offering general support to the ABA's comment, we would like to emphasize several issues.

General Comments

PNC recognizes that the consumer credit reporting industry has become a very automated industry. However, the system logic and data analysis methodologies used to trigger notices regarding fraud alerts and address discrepancies differ substantially among the credit bureaus. While on the surface all three credit bureau repositories offer similar fraud warning detection services, each bureau utilizes differing proprietary logic to trigger the warning flag being sent. Additionally, since these services are voluntarily subscribed to, there could be significant disparity across lenders serving different customer markets regarding which flag warnings are being received. Accordingly, variances in these services could result in inconsistencies across users with respect to the proposed notification requirements, potentially causing confusion to the borrower, and creating competitive challenges for lenders.

The financial services industry is also a highly automated industry. We find that automated solutions reduce the level of human error and offer a level of consistency not inherent in manual processes. When the Proposal is adopted in final form, we will strive to implement automated solutions wherever possible to implement its requirements. We therefore request a reasonable period of time between the adoption of the final rule and

its mandatory effective date to ensure that banking organizations have sufficient time to analyze the applicable requirements and implement the best possible automated solutions that will benefit customers and the industry alike.

Specific Comments

1. **Subpart I ("Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal")**

Under proposed §41.82(d)(1)[1], users of consumer reports must develop and implement reasonable policies and procedures for furnishing to a credit reporting agency from which it has received a notice of address discrepancy an address for the consumer that the user has reasonably confirmed is accurate when the user (1) can form a reasonable belief that it knows the identity of the consumer; (2) establishes or maintains a continuing relationship with the consumer; and (3) regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy was obtained. Proposed §41.82(d)(2) further requires the user to "reconcile" the address it initially received from the consumer when it receives a notice of address discrepancy rather than simply furnishing the initial address it received from the customer to the credit-reporting agency.

We echo the concern of the ABA that these proposed provisions will add a new substantial burden on financial institutions to verify the address when doing so will not improve accuracy or prevent identity theft beyond what current practices do. And, we emphatically believe that such a requirement will have a major impact on the financial services industry. Under the proposed requirements, the time and expense required to approve applications for credit with an address mismatch is going to increase dramatically. Current underwriting practices at PNC Bank include reconciling address variances between the application stated information and the credit bureau file information. However, the important distinction between PNC's current, and we believe effective, practice and the proposed requirement is the level of judgment utilized by the loan underwriter regarding required due diligence performed to reconcile an apparent address discrepancy. Prior addresses, business or secondary property addresses constitute the most common, and vast majority of, examples when an address mismatch warning is received by a credit bureau. In cases where a simple reconcilement is not available, additional due diligence steps are appropriate. We suggest the proposed regulation should focus on those more limited circumstances.

[1] For purposes of this comment letter, we are using the proposed OCC regulatory citations.

2. Definition of Customer

The Agencies are proposing a broad definition of "customer" as a person that has an account with a financial institution or creditor. This definition would include not only consumers, but also businesses. We strongly believe this definition should be narrowed to include only natural persons using credit for personal, family or household purposes, who are typically the targets of identity theft. It should be made clear that the term does not apply to any other legal entities.

We agree with the ABA that most of the proposed Red Flags deal more with consumer identity theft: e.g., use of someone else's photo identification, social security number, date of birth, and personal address. The type of fraud experienced by businesses relating to their bank accounts usually does not involve another person using a business's identity.

We also agree with the ABA that businesses are in a better position to monitor fraudulent activity involving their bank accounts, particularly, when such activity is committed by dishonest employees. Businesses entrust certain employees to handle their financial transactions. Banks rely on the representations made by businesses via authorizing resolutions and other similar documents that these employees are authorized to act on their behalf. Thus, when dishonest employees initiate fraudulent transactions, such as wire transfers to their personal accounts or other similar payments, banks are helpless to prevent such transactions when the employees are authorized to act.

Furthermore, most banks offer cash management services, such as positive pay and other similar services, to assist businesses in reducing the occurrence of fraudulent activity on their bank accounts. These services enable businesses to take a proactive role in monitoring the activity on their accounts. Businesses today are more sophisticated, regardless of their size and type, and are involved in more complicated financial transactions and relationships. Requiring banks to determine if certain business transactions are Red Flags when banks already have fraud detection software and other procedures to reduce fraudulent transactions on business accounts would be unduly burdensome, costly and time consuming.

3. **Establishing an Identity Theft Program**

The regulation unnecessarily calls for establishing reasonable identity theft practices and procedures not mandated by statute. These requirements will limit flexibility and create undue expense.

4. **Section 40. 90(d)(1)(ii)**

This section indicates that institutions must consider particular factors in identifying whether certain Red Flags are relevant. Placing this requirement in the regulation would result in financial institutions creating a checklist based on the Red Flags without advancing the existing identity theft programs.

5. **Customer Identification Programs**

The regulation should clearly state that the practices required for Customer Identification Programs ("CIP") satisfy the requirements under this regulation.

6. **Definition of a Red Flag**

Red Flag should be defined as "a pattern, practice, or specific activity that indicates **significant** possibility of identity theft."

7. **Assessment of Red Flags in Section 40.90(d)(2)(iii)**

PNC recommends that the requirement that a financial institution assess whether the Red Flags "evidence a risk of identity theft" as this could result in devoting valuable resources to an exercise with few benefits.

8. **No Civil Actions**

The FACT Act provides that the provisions regarding civil liability do not apply to the Red Flag guidelines and the regulation required thereunder. We recommend that, for the purposes of clarity, a statement to this effect be included in the regulations.

9. **Appendix J—Red Flags**

We request that the agencies clarify whether particular red flags apply only to particular types of accounts. For example, in Red Flag number 18, the Agencies refer only to "revolving credit account." The Red Flag requires the monitoring of a new revolving credit account to determine whether it is used in a manner commonly associated with fraud, such as whether "the majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry)." Although this would seem only to apply to a credit card account, there are other types of revolving credit accounts, such as personal unsecured lines of credit and home equity lines of credit, which are accessible by check and which cannot be monitored unless a financial institution employs numerous people to scrutinize each check. If the Agencies

believe that any of the 31 Red Flags apply only to a particular product type, we ask the Agencies to make that clear. Otherwise, we will have to make that decision ourselves and then justify that decision.

Red Flag 3 - *A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:*

a. A recent and significant increase in the volume of inquiries
b. An unusual number of recently established credit relationships
c. A material change in the use of credit, especially with respect to recently established credit relationships
d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

We echo the ABA's recommendation that this proposed Red Flag be deleted. In our automated approval process, if an application is approved we do not specifically review the pattern of activity. Rather, those factors are integrated into our credit scoring models. Further, all the factors listed as potential risks of identity theft could clearly be the result of any number of factors, varying from a significant increase in income to a new car purchase to a change in family circumstances. If this Red Flag is not deleted altogether, we ask the Agencies for clarification as to whether it would be sufficient under the Proposal to integrate these factors into a scoring model, or whether there has to be an individual review of each of the factors listed.

Red Flag 12 - *The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customers.*

We agree with the ABA that this Red Flag should be deleted. We have no way to verify or track whether a phone number or address has been used on a different application, nor whether applicants would have a valid reason for sharing a phone number or address. To keep track of all this information for separate applicants would require the compilation of such information into another internal database.

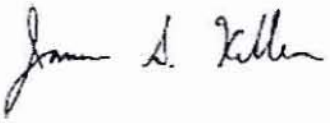
Red Flag 17– PNC does not believe undelivered mail is an indicator of identity theft. This red flag, if it remains should be clarified to reflect that it is not referring to a single piece of mail.

Red Flag 30 – PNC recommends deletion of this Red Flag, as large check orders by a single customer do not indicate identity theft.

Conclusion

Thank you for providing this opportunity to comment. While we have commented on particular facets of the proposal, we would like to reiterate that we are fully supportive of the comment letter submitted by the ABA. If you have questions about this comment letter, please feel free to contact Melinda Turici, 412-762-2280, Senior Counsel, or the undersigned.

Sincerely,



James S. Keller

cc: Gary TeKolste
Office of the Comptroller of the Currency

Michael Carroll
Federal Reserve Bank of Cleveland

Melinda B. Turici
John J. Wixted, Jr.
The PNC Financial Services Group, Inc.