WISCONSIN BANKERS ASSOCIATION

September 18, 2006

VIA EMAIL

Office of the Comptroller of the Currency
250 E Street, SW
Public Reference Room, Mail Stop 1-5
Washington, DC 20219
regs.comments@occ.treas.gov
Docket Number 06-07

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

Mr. Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Comments@FDIC.gov
RIN 3064-AD00

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
regs.comments@ots.treas.gov
No. 2006-19

Ms. Mary F. Rupp, Secretary
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314-3428
regcomments@ncua.gov
Proposed Rule 717, Identity Theft Red Flags

Federal Trade Commission/
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue NW
secure.commentworks.com/ftc-redflags
Project No. R611019

Re: Proposed Rule, Identity Theft Red Flags and Address Discrepancies, Sections 114 and 315 of the Fair and Accurate Credit Transactions Act.

Dear Sirs and Madams:

The Wisconsin Bankers Association (WBA) is the largest financial institution trade association in Wisconsin, representing approximately 300 state and nationally chartered banks, savings and loan associations, and savings banks located in communities throughout the state. WBA appreciates the opportunity to comment on the proposed rule addressing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act).

4721 SOUTH BILTMORE LANE
MADISON, WI 53718
P.O. BOX 8880
MADISON, WI 53708-8880
608-441-1200
FAX 608-661-9381
www.wisbank.com

The Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA), and Federal Trade Commission (FTC)(collectively, the Agencies) are required by Section 114 of the FACT Act to create guidelines for financial institutions and creditors to identify patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft. Section 315 of

the FACT Act requires the Agencies to create guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy. The proposed rule addresses both FACT Act Sections. To assist the Agencies in promulgating such rules, WBA offers the following comments.

Background

Section 114 of the FACT Act requires the Agencies to jointly issue guidelines for financial institutions and creditors regarding identity theft with respect to their account holders and customers. Within these guidelines, the Agencies are required to identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.

To fulfill this requirement, the Agencies propose each financial institution and creditor implement a written Identity Theft Prevention Program (Program) that contains reasonable policies and procedures to address the risk of identity theft based upon the risk assessment of the financial institution. Under the proposal, the institution's Program must be appropriate to the size and complexity of the institution; address the nature and scope of the institution's activities; and be flexible to address changing identity theft risks as they arise.

In addition, for credit and debit card issuers, Section 114 requires the Agencies' guidelines to specifically include requirements that an issuer must first follow to validate a change of address request before the issuer acts on a request for an additional or replacement card. An institution that is an issuer may incorporate this requirement into its Program.

The proposed rule also addresses Section 315 of the FACT Act. This section requires the Agencies to jointly issue rules that provide guidance regarding reasonable policies and procedures that a user of a consumer report (User) should follow when it receives a notice of address discrepancy. Specifically, the policies and procedures must facilitate a User's ability to: form a reasonable belief regarding the identity of the person on whom it has obtained a consumer report; and reconcile the address of the consumer with the credit reporting agency (CRA), if the User establishes a continuing relationship with the consumer and regularly and in the ordinary course of business furnishes information to the CRA.

General Comments to Section 114 Program Requirements.

Identity theft issues are a top concern for all financial institutions and other creditors, and each has already taken numerous steps to combat them. WBA itself recognizes the importance of preventing identity theft and routinely partners with financial institutions and other groups in Wisconsin to educate the public about identity theft. WBA fully supports the Agencies' attempt to implement a flexible, risk-assessment based Program; however, WBA is concerned that the proposed rules are not sufficiently flexible for an institution to create a Program that truly reflects the institution's own risk-assessment and risk-management of its particular products and services, customers and location(s).

Recently, financial institutions have conducted several rounds of Bank Secrecy Act (BSA) assessments to identify product and service risks relative to the institution's customer-base, demographics, and location(s). Institutions are also actively working to complete risk-assessments of their Internet services and other forms of electronic banking to comply with multi-factor authentication guidelines required to be in place by year end. In addition, institutions are currently operating under Customer Identification Program (CIP) requirements when opening new accounts. All three of these programs are ongoing requirements for institutions and must be monitored, reviewed, and modified as the

institution's products and services, customers, and location(s) grow and change. WBA is concerned that the proposed rule will result in the creation of yet another procedural checklist and monitoring policy, separate from these existing programs, and will not create a more effective or efficient method of combating identity theft. Instead, institutions already subject to these requirements will be burdened with duplicative policies, procedures and monitoring requirements.

WBA believes integration of the Red Flag guidelines with these existing programs is a better approach. The Agencies acknowledge that an integrative approach might be desirable but dismiss it because not all financial institutions are subject to these existing programs. Such an approach should not be dismissed just because other types of institutions have little or no current requirements to prevent financial crimes such as fraud and identity theft. WBA urges the Agencies to simplify the proposed rules to allow financial institutions already subject to these programs to take advantage of such programs in fulfilling their efforts to halt identity theft.

The Agencies have gone to great lengths recently to champion their efforts in allowing financial institutions to create risk-management procedures unique to each institution based upon its products and services, customers, and location(s). Yet, the Agencies propose in Appendix J a prescribed list of identity theft activities that all institutions must, at a minimum, use in their policy implementation. WBA does not see how this approach would afford the flexibility touted by the Agencies. In addition, WBA is concerned that a mandatory list will be quickly used by criminals as a teaching tool on how to structure identity theft scams and how to avoid appearing on a financial institution's "hot list". To combat these issues, WBA believes the best solution is to offer Appendix J as a list of examples of identity theft activities that an institution may review when crafting its identity theft procedures.

Specific Comments to Section 114 Program Requirements.

Proposed § __.90(b) Definitions.

The Agencies propose the definition of "account" to include not only consumer accounts, but also business accounts. The Agencies also seek comment on whether the account definition should include relationships that are not "continuing". WBA strongly opposes the inclusion of business accounts and relationships that are not continuing in this definition. To require financial institutions to gather and maintain information on non-customers and businesses is simply too broad. Creation of policies and procedures to monitor those accounts makes these new requirements costly and compliance-report laden.

The Agencies propose the definition of "customer" to mean "a person that has an account with a financial institution or creditor." This would include individuals and businesses. WBA urges the Agencies to exclude businesses from the definition of customer. Financial institutions have other anti-fraud vehicles in place to correctly identify a business customer. CIP procedures currently require that the identity of a new business be verified via documentary or non-documentary methods. Most financial institutions have access to State filing offices that can independently verify the existence and status of business customers.

The Agencies propose the definition of "Red Flags" as "a pattern, practice, or specific activity that indicates the possible risk of identity theft." WBA is concerned that the use of "possible risk of identity theft" is too broad. Nearly any activity could potentially be considered a "possible risk." This extremely broad term makes it impossible for financial institutions to draw a line between legitimate activity and activity perceived as peculiar to

some, but after investigation proves legitimate. To require financial institutions to micro-manage every transaction for the "possible risk" of identity theft is unrealistic. As an alternative, WBA urges the Agencies to replace "possible risk" with "significant possibility" as suggested by American Bankers Association (ABA) for the reasons outlined in ABA's comment letter.

Proposed §__.90(d)(5) Involvement of Board of Directors and Senior Management.

The proposed rule would require the board of directors and senior management to be responsible for developing and implementing the Section 114 Program. Yet for those financial institutions or creditors who do not have a formal board of directors, the entity is permitted to select a "designated employee." WBA finds this requirement inconsistent and not prescribed by statute. WBA believes a board member is too far removed from the day-to-day management of identity theft issues. Board management, while necessary, is generally a slow moving process as each board member is required to analyze the details and effects of each issue presented for their review and direction, while identity theft and fraud events can occur at any given instant. A financial institution needs an immediate response to identity theft issues from employees directly involved in frontline activities. As such, WBA recommends the Agencies not require board member involvement with the direct oversight and implementation of Program management. Instead, the Board should be involved in the overall development and approval of the policies and procedures, but personnel directly involved with the institution's other fraud prevention efforts should be responsible for the oversight and management of the Program.

Card Issuer Requirements.

As previously outlined, Section 114 also requires the Agencies to issue rules requiring credit and debit card issuers to first assess the validity of change of address requests before issuing a requested additional or replacement card.

Under the proposal, if a card issuer receives a change of address request, and then within a short period of time of at least 30 days after it receives the request, it receives a request for an additional or replacement card, the issuer may not grant the card request unless it first assesses the validity of the request by using one of the following three methods: (1) notifying the cardholder of the request at the former address and providing the cardholder with means of promptly reporting incorrect address changes; (2) notifying the cardholder of the request by any other means of communication that the cardholder and the card issuer have previously agreed to use; or (3) using other means of assessing the validity of the change in address. The notice must be clear and conspicuous and provided separately from regular correspondence with the cardholder.

WBA recommends the Agencies simply require financial institutions to verify the address at the time an address change is requested by the customer for any change of address request. Institutions already have procedures in place to document and verify the validity of such requests. WBA recommends the Agencies allow financial institutions to verify address change requests through verification of the customer's identity and not require additional duplicative procedures.

Comments to Section 315 Reports to CRA by Users.

Proposed §__.82(c) Requirements to Form a Reasonable Belief.

The proposed rule would require the creation of policies and procedures that would enable the User to form a reasonable belief regarding "the identity of the person to whom the consumer report pertains" when the User receives a notice of address discrepancy. The proposed rule would allow existing CIP procedures to satisfy the requirement to verify the identity of the applicant so long as the User applies the CIP procedures to all situations where it receives a notice of address discrepancy.

WBA believes CIP procedures are sufficient to identify the consumer. Many consumers move frequently and a CRA may not have the most recent address for the consumer. If a new account is opened, and the financial institution has an address discrepancy as compared to the CRA's reported address, the banker would simply verify the correct address with the new customer via the institution's CIP requirements and the correct address would be reported to the CRA pursuant to the financial institution's general reporting procedures. Extra procedures would be duplicative because of these existing CIP requirements.

Conclusion

Financial institutions are already actively working to protect consumers from identity theft. Policies and procedures have already been implemented through financial institutions' BSA, security information systems, and CIP procedures. WBA strongly recommends the Agencies craft final rules which: permit financial institutions already subject to the above-noted policies and procedures to utilize such policies and procedures to fulfill the requirements of Sections 114 and 315. Doing so would avoid unnecessary duplication of efforts while still retaining the benefits of risk-based assessments the Agencies already claim to support.

Once again, WBA appreciates the opportunity to submit comments on the interagency proposed rule.

Sincerely,

Kurt R. Bauer
President/CEO