September 18, 2006

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

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

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

Mary F. Rupp, Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314–3428
regcomments@ncua.gov

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

Federal Trade Commission/Office of the Secretary
Room H–135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Joint proposal rulemaking
Implementation of Sections 114 and 315 of the FACT Act
Identity Theft Red Flag guidelines
OCC Docket No. 06-07; FRB Docket No. R-1255;
FDIC RIN 3064-AD00; OTS No. 2006-19; NCUA (No Docket Number); FTC RIN 3084-AA94
71 *Federal Register* 40786, 18 July 2006

By electronic delivery

Ladies and Gentlemen:

The Illinois Bankers Association (the "IBA") appreciates this opportunity to comment on the proposed interagency regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 as proposed by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission. The IBA is a full-service trade association representing state and national banks, savings banks, and savings and loan associations of all sizes in the State of Illinois; collectively the IBA represents over 85% of all banking assets in our state.

OVERVIEW OF OUR CONCERNS

The IBA views the 31 "red flags" that have been proposed to aid in preventing, detecting, and mitigating identity theft to be excessive and overly burdensome. The enormous costs that the financial industry will incur in its compliance with the regulations far exceed the potential benefits to consumers. For example, "red flag" Number 19 in Appendix J requires the tracking of activity on an account that is inconsistent with established behavioral patterns, such as a "material increase" in the use of available credit. Smaller community banks that have limited resources (for both systems and personnel) would, at the very least, be required to purchase expensive new software from third party vendors in order to meet

this requirement, followed by added costs for integration, training, monitoring and reporting, ultimately resulting, we predict, in a preponderance of "false positives" produced every month due to legitimate account usage.

In addition, we are concerned that the overly-extensive "red flags" will encourage a false sense of security in consumers by suggesting that financial institutions are principally responsible for tracking and reporting events that are suggestive of identity theft. The consumer—who has full knowledge and control over his or her own financial transactions—is the first line of defense against identity theft. Consumers are in the best position to monitor their accounts and to identify unusual and potentially fraudulent activity. Yet the sheer number of standards that are being proposed for financial institutions—and the proposed "red flags" clearly are the functional equivalent of standards—inevitably will prompt consumers to expect their financial institutions to serve as the principle guardian against identity theft. We are concerned that financial institutions eventually may find themselves in costly litigation with customers over varying interpretations of their responsibilities under the proposed rules.

We also are concerned with the proposed migration of the role of the financial institution's board of directors from one of oversight to one of transaction monitoring. Board members are selected for their diverse business expertise. We submit that it would not be the wisest use of their time to be deluged with reports of "red flag" incidents before, during or after each board meeting. Management should bear the responsibility for ensuring the implementation of these rules, not the board.

COMMENTS ON § 334.82 - DUTIES OF USERS REGARDING ADDRESS DISCREPENCIES

This section of the proposed regulations requires a user of consumer reports to verify a consumer's identity in certain cases after it has received a "notice of address discrepancy" from a consumer-reporting agency. Following verification of the consumer's identity, a user would then need to report a "confirmed address" to the consumer reporting agency.

This requirement for identity verification and address confirmation should be risk-based. That is, if the address discrepancy reported by the consumer reporting agency appears to be insignificant in nature, such as the use of "avenue" instead of "street" in an address, verification of the consumer's identity and address confirmation should not be required.

In addition, the proposal does not give examples of what constitutes a "substantial difference" between addresses that would trigger the verification and addresses for the reporting requirement. Additionally, the terms "new relationship" and "reporting period" should be defined in the regulations.

COMMENTS ON § 334.90 - DUTIES REGARDING THE DETECTION, PREVENTION AND MITIGATION OF IDENTITY THEFT

This section of the proposed regulations requires the implementation of a written Identity Theft Prevention Program for the detection of "red flags" and the mitigation of the risk they present. Appendix J lists the proposed "red flags."

Appendix J, Number 12, would require a financial institution to treat a customer's use of an address, Social Security number, or home or cell phone number previously submitted by another customer as a "red flag." In most cases, there are valid reasons for the duplicate use of an address and telephone number, such as when different customers reside at the same address and share the same telephone number. Tracking the duplicative use of this information across different business lines would involve an enormous expense with limited benefits to consumers.

Appendix J, Number 15, is inconsistent with the existing Customer Identification Program ("CIP") rules set forth in 31 CFR §103.121. There currently is no requirement under the CIP rules for financial institutions to verify identity by "go[ing] beyond that which generally would be available from a wallet or a consumer report" as stated in the proposed regulations.

"Red flag" Number 17 in Appendix J suggests that there is a cause for concern when a customer's mail is returned as undeliverable although transactions continue to be conducted in connection with the customer's account. Customers often forget to report a change of address or delay in

reporting an address change. Consideration should be given to these failures and delays, so that only repeated instances of returned mail over a considerable period of time should be deemed to be a "red flag."

CONCLUSION

Although the IBA recognizes the important role that financial institutions play in the fight against identity theft, we do not support the proposed rules to the extent and for the reasons stated above. In addition, given the enormous amount of system enhancements, policy development and employee education required to implement the proposals, we recommend that, at a minimum, the mandatory effective date be delayed for up to 18 months following promulgation of the final regulations.

We appreciate your consideration of our comments.

Sincerely,

W. Alison Huszar
Vice President and Senior Compliance Officer