September 21, 2006

South Shore Savings Bank
1530 Main Street
So. Weymouth, MA 02190

Re: RIN 3084-AA94

Dear Sir:

South Shore Savings Bank is an $830mm asset size, 14 branch mutual savings bank, located in Weymouth, Massachusetts. The Bank appreciates the opportunity to comment on the proposal to implement section 114 of the Fair and Accurate Credit Transactions Act of 2003 [FACTA] – the Red Flag Regulations.

The proposal for Red Flag Regulations would require financial institutions and creditors to have a written program that is based upon the institution's risk assessment and includes controls to address the identity theft risks identified. The program must be appropriate to the size and complexity of the institution and nature and scope of its activities, and be flexible to address changing identity theft risks as they arise.

Proposed additional requirements include verifying the identity of persons opening accounts, training staff, overseeing service provider arrangements, program approval by the board of directors and reporting to the board, a committee or senior management at least annually.

The Agencies will issue periodic *Red Flags in Connection with an Account Application or an Existing Account*, which an institution should use as a basis for identifying which Red Flags are relevant based upon its risk assessment. The Red Flags would be compiled from literature on the topic, information from credit bureaus, financial institutions, creditors, designers of fraud detection software, and the Agencies' own experience. The proposal also indicates a financial institution may wish to combine its program with its information security program, clearly a very similar program.

The Agencies specifically invite comment on the impact of the proposal on community bank's finances and available personnel with necessary expertise and ask if the goals of the proposal could be accomplished using another approach.

Community Bank Expertise:

In order to protect their customers and the safety and soundness of their banks, for many years community banks have maintained fraud investigation and prevention programs.

The "Security Officer" position that had generally been responsible for implementing the requirements of the Bank Protection Act has also fulfilled the role of fraud investigator, with identity theft identified as a fraud method well before the regulatory emphasis it is now receiving. Membership in fraud prevention groups, working with law enforcement, or security newsletters, the "security officer" remains the expert on identity theft activity. All Departments of the Bank are sensitive to this type of activity and with heightened awareness and many layers of quality control; any suspicious events are reported to the Security Office.

With the advent of the Information Security Program required by Section 501(b) of the Gramm Leach Bliley Act, followed by the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, the Privacy Officer, at this Bank also the Security Officer, has learned about fraud prevention and, coordinates with the information security officer (CIO) to address traditional identity theft and technology-related breaches. A Customer Incidence Response Team exists and monitors any "breaches" which in turn are reported to the Risk Committee.

Community Banks have historically demonstrated their commitment and expertise in the area of identity theft/fraud prevention.

Community Bank Resources:

South Shore Savings Bank urges you to consider the burden imposed by the administrative requirements of these Guidelines.

Due to their limited resources, community banks have had to maintain flexible fraud and identity theft prevention programs that protect their customers, promote safety and soundness and comply with regulations. We train staff, educate customers, maintain expertise, monitor numerous daily reports to support these efforts, and communicate with the Board of Directors

As noted above, there already exist regulations, extensive guidance and a strong system of internal controls regarding protecting consumers and bank customers from identity theft.

The bank is concerned that the administration of an identity theft prevention program in addition to existing regulations would add to the administrative burden of community banks, which have limited resources. The proposal does indicate that the requirements of the Guidelines could be integrated with existing policies and procedures. However, we feel that a community bank that has policies and procedures in place to protect the identity of its customers should ONLY have to demonstrate that their policies and programs are effective. Banks have checks and balances and quality controls in place to prevent risk, these are well documented and in standard operating procedures. Improving procedures in conjunction with the Red Flag guidelines should be <u>all that is required by this proposal</u>.

Alternative Approach:

This Bank recommends using the *Red Flags in Connection with an Account Application or an Existing Account* [Appendix J] as a resource. Please consider focusing Agency efforts on maintaining and communicating current Red Flags so that financial institutions can depend on the Red Flags as a resource when performing their various bank wide risk assessments and FDICIA internal controls assessments, which have always included loss prevention and the security of our customers' information.

Thank you for the opportunity to comment on this proposal.

Sincerely,

Gail K. Faring
Vice President
Compliance Director
Security Officer