September 18, 2006

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

Office of the Comptroller of Currency
250 East Street, SW.,
Public Reference Room, Mail Stop 1-5
Washington, DC 20219
RE: Docket No. 06-07

Dear Mr. Feldman and Mr. Dugan:

Subject: Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003
RIN 3064-AD00 and Docket Number 06-07

As a community banker, I appreciate the opportunity to comment on the proposed Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 (12 CFR Part 334 and 364) regulation that was issued on July 18, 2006. Identity theft is a growing concern and issue in today's economy and needs to be dealt with. However, we do not think that financial institutions should be the patroller of the identity theft problem and certainly not regulated to be in charge of controlling identity theft. Financial Institutions can help to provide information to help stem the rise of Identity Theft but should not be the only controlling unit. Therefore, I would like to express my objection to this proposed Identity Theft Red Flags regulations.

Placing the requirements of the proposed Identity Theft Red Flags regulation on community banks will create a huge regulatory burden. Community banks have limited resources to develop and implement additional identity theft prevention programs that include policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts as described in the purposed Identity Theft Red Flags regulations. In addition, there is no clear guidance from the agencies on how to develop and implement an identity theft prevention program. Additional guidance from the agencies would be very useful. The more structured guidance from the regulators leaves less interpretation for the banks and the examiners. When there is too much flexibility and grey areas in a regulation there is too much interpretation left up the examiner who reviews the program. As a community banker I would much rather know what exactly we need to do to comply with a regulation than leaving it open for so much interpretation.

The proposed Identity Theft Red Flags regulation requires a bank to complete a risk assessment. It would create a regulatory burden to conduct an annual identity theft risk assessment of the degree required within the proposed Identity Theft Red Flags regulations. As community banks, we have limited resources available to create and maintain a risk assessment of this nature. In addition, there is no set guidance from the agencies as too how to conduct a risk assessment. Additional guidance on developing a scope of the risk assessment, how to conduct, and what all needs to be included in the identity theft risk assessment would be very useful. The more structured guidance from the regulator leaves less interpretation for the banks and the examiners. When there is too much flexibility and grey areas in a regulation there is too much interpretation left up to the examiner who reviews the program. As a community banker I would much rather know what exactly we need to do to comply with a regulation then leaving it open for so much interpretation.

Currently, Our Company has a very strong Customer Identification Program and Information Technology policies and procedures that provide adequate protection to our customers in the area of Identity Theft. If we were required to establish additional or expand our policies and procedures in the area of Identity Theft as purposed then it would place an undue burden and additional costs on us. As required by the USA Patriot Act customer identification requirements, we identify all *new* customers who open accounts with our company. The USA Patriot Act customer identification requirement only applied to new customers who opened an account with the bank after October 1, 2003. The purposed Identity Theft Red Flags regulation provides that compliance with the Patriot Act customer identification

requirements would satisfy the identification requirement under the identity theft prevention program if it is applied to any customer who opens any type of account with evaluated risk of identity theft. Therefore, the proposed Identity Theft regulation is only a duplication of the USA Patriot Act customer identification requirement and further tightening the requirements. It would be a huge regulatory cost to rewritten, managed, implemented, monitored, and retrain our staff on new customer identification requirements. I am afraid that this will create confusion among our staff as too when they need to obtain the customer identification requirement. It appears that the purposed Identity Theft Red Flags regulation is a back door to requiring the USA Patriot Act customer identification requirement to *all* customers of the bank.

Appendix J of the purposed Identity Theft Red Flags regulation list specific examples that could indicate possible identity theft and the 31 proposed red flags are to be included in the banks risk assessment. The following are red flags that need to be clarified or removed from the list of possible identity theft red flags:

→ 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. Accounts are opened all the time with the same address, home, or cell phone number. We have husbands, wives, and children that open accounts with the same address and home phone. This red flag should be removed or at least be changed to include "with no apparent reason".

→ 15. The person opening the account of the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report. What more information could the customer provide to further their identification (driver license, state ID card, etc) which is not in their wallet or purse? I can't think of any information beyond their identification information or consumer report that we need to request. It sounds like we would have to have finger print or other biometric identification for this requirement. This red flag should be removed or explain what more authenticating information is needed when opening an account then the customer identification information.

→ 20. An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors). What is reasonably lengthy period of time? Is it one year, two years, etc? One could think that it is one year and another would think it is three years. Reasonable lengthy period of time needs to be defined.

I thank you for your consideration of these concerns and hope that the final revision of the Identity Theft Red Flags and Address Discrepancies regulation will address them in a meaningful way.

Sincerely,

Scott Jennings
Chief Operating Officer
Summit Financial Group, Inc