STILLWATER NATIONAL BANK
P.O. Box 1988, Stillwater, OK 74076

September 18, 2006

Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

RE: Identity Theft Red Flag Guidelines
FRB Docket No. R-1255

VIA E-MAIL: regs.comments@federalreserve.gov

Ladies and Gentlemen:

I am writing to submit comments related to the proposed regulation implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act").

A $2.2 billion organization, Stillwater National Bank and its affiliates are committed to our information security programs and are certainly concerned about the increasing incidents of identity theft and fraud on a national basis. However, we are disturbed about aspects of the regulation as proposed.

Speaking generally, all other issues aside, we are perplexed as to how we can possibly comply with the far-reaching and all-encompassing aspects of the proposal. We do not currently have systems and resources to accomplish the requirements that appear to be mandated by the proposal. Further, our initial analysis indicates implementing such systems will be very costly, with no readily apparent compensatory benefit.

As noted, we are already committed to our information security protection and fraud prevention programs. We believe we react to emerging threats and adjust our procedures as necessary to respond to our environment. We identify persons opening accounts under our Customer Identification Program (USA PATRIOT Act §326), and we already reconcile noted discrepancies. We monitor accounts for suspicious activity as required by the Bank Secrecy Act and related laws and regulations. We have a risk-based customer information security program that provides a framework for ensuring the protection of customer information. We train front-line staff to be aware of people and situations, both customers and non-customers. We identify individuals and entities when checking against Office of Foreign Assets Control lists and when Bank Secrecy Act recordkeeping thresholds are met. We have a fraud investigator who monitors appropriate reports and follows up when necessary. We attempt to educate our

customers about emerging threats, including placing warnings on our website. It is not only in our customers' best interest for us to do these things, but in many cases, we also reap the benefit. We do this because it is the right thing to do and because from a business perspective, fraud identification is a prudent thing to do. However, to burden us with additional layers of regulation and paperwork will not improve those processes. In fact, it may serve to hamper our processes as we are required to address issues of form over issues of substance.

Banks already have a responsibility to our customers, and consumers already enjoy significant protections under various regulations. While financial institutions are called upon to subsidize more and more due diligence, there is little corresponding requirement for personal accountability. For example, Regulation E provides considerable protection for consumers in electronic fund transfers. However, there is no negligence standard. Consumers may recklessly write their personal identification number on their card and if someone uses that card to obtain funds or goods fraudulently, the bank may have to accept the financial loss.

Overall, we are concerned about what appears to be a rigid and regimented, checklist-type approach to an issue that requires the ability to react quickly. In addition, some areas of specific concern are addressed below.

1. Definitions of "account" and "customer"

   The proposal considers expanding the definition of "account" to include relationships that are not continuing. We do not believe this would be of any material assistance in identifying or deterring identity theft. Further, the requirement to validate information about individuals with whom we may have one contact will cause substantial burden. We already retain identifying information in certain circumstances (e.g., cash sales of monetary instruments and wire transfers), but the encumbrance of additional verification would in all probability ensure the few banks remaining who, like us, continue to provide services for non-customers will cease to provide such services.

   The proposal also expands the definition of "customer" to include business customers. One of the primary concerns of the Fair Credit Reporting Act is <u>consumer</u> reports. However, our bank's due diligence related to business customers primarily involves processes and investigation <u>not</u> related to consumer reports. Further, we believe businesses are less likely to be the victim of identify theft and that businesses should be held to a higher standard than consumers for having their own internal controls in place. While we believe personal accountability should be expanded across the board, there should certainly be an added expectation that business entities will have their own controls in place. We request "customer" be limited to consumer accounts.

2. "Prevent" identity theft

While possibly only an issue of semantics, we are concerned about the verbiage contained in several areas of the proposal. It is impossible for any organization to develop a program that will ensure the PREVENTION of identity theft. The proposal states the program "…must include policies and procedures to ***prevent identity theft from occurring***…." (emphasis added). We cannot possibly meet that standard. While we will certainly support a program that will strive to ensure the deterrence and detection of identify theft, we can in no way guarantee that identity theft will be prevented. We do not have ultimate control of our customers, their lives, and their information. We will continue to try to deter and detect identity theft or other fraud, but cannot be held accountable for instances where customers are careless or negligent with their personal information. Further, we believe this level of responsibility is not mandated by the FACT Act, where the regulatory agencies are directed to prescribe regulations requiring banks to "establish reasonable policies and procedures" for implementing "guidelines….regarding identity theft". Therefore, we request the verbiage be amended to reflect the ultimate goal of identification of possible instances of identity theft.

3. Anomalous account patterns

We are a $2.2 billion organization with offices in three states. Given our size and geographies, we are too big to monitor accounts for anomalous usage on a manual basis. However, we are too small to afford the multi-million dollar software programs used by big banks to identify anomalies. In this case, not big and not small does not result in "just right". This proposal would require we monitor all accounts – from home equity lines of credit to checking accounts. Our initial inquiries have indicated detection tools are not currently available in a reasonable price range for our size. In fact, many vendors do not yet have a product available. At this point, we cannot identify the specific cost, but believe it to be substantial. Further, under this proposal, even if we could acquire the technology to identify anomalies, this would not be the end of our responsibilities. We would then be required to investigate such instances, with a considerable increase in human resources in order to find out our customers are vacationing in Europe, paying for an elaborate wedding, or doing some early Christmas shopping. We already have risk-management tools and processes in place and review reports such as those related to large items. However, we cannot (without considerable and unreasonable expense) monitor as described in the red flag guidance. We request the regulatory agencies amend the

guidance to clarify and ensure examiners will not expect all banks to include all red flags – regardless of size, risk, or other already existing controls.

4. Risk-based compliance

We recognize the proposal discusses risk-based compliance efforts determined by an assessment of those risks. However, anecdotal information from our peers across the country suggests that in areas where we are already required to perform risk assessment, examiners often second-guess the bank's own analysis. The bank's assessment is sometimes even disregarded in favor of examiners' opinions or checklists. As noted above, we request the proposal clearly outline and support a risk-based approach, removing such language as "must" from the discussion of incorporation of red flags, for example.

5. Additional regulatory burden

We believe the regulation as proposed will have a significant impact on our institution. To implement such a program will require sizeable investment in technologies and additional human resources. While we understand the directive to identify possible risks to our customers and for the regulatory agencies to provide guidelines regarding identity theft, we maintain we already have processes in place addressing those issues. These processes have been developed over time in response to our markets and the risks we perceive, and have been integrated into our existing business lines and processes. However, we believe the proposal presented will require us to layer additional structure that would provide little, if any, corresponding additional control. We request the regulatory agencies reconsider the rigidity and structure required by the proposal.

Thank you for the opportunity to comment on this proposal.

Respectfully,

Priscilla J. Barnes, CRCM
Vice President
Regulatory Risk Management