Missouri Bankers Association

207 E. Capitol Ave.
Jefferson City, MO 65102

September 15, 2006

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

RE: Joint Proposed Rulemaking Implementation of Sections 114 and 315 of the FACT Act Identity Theft Red Flag Guidelines; FRB Docket No. R-1255

Dear Ms. Johnson,

These comments are being submitted on behalf of almost 400 Missouri banks and savings and loan associations by the Missouri Bankers Association (MBA), a Missouri trade association. The MBA is responding to the joint proposed rulemaking issued by the federal banking regulators ("the Agencies") on implementation of Sections 114 and 315 of the FACT Act Identity Theft Red Flag guidelines.

The MBA and its members strongly believe that financial institutions must have broad flexibility to develop and implement appropriate controls to respond effectively to evolving financial crime threats faced by banks. While the Agencies state that the proposed Regulation is intended to be flexible and reflect a risk-based approach, we conclude that the proposed regulatory language in many cases falls short of these stated intentions. Instead, we believe that the proposal runs a high risk of creating an artificial, stagnant, mandatory checklist regime that will not effectively advance the goals of detecting and preventing identity theft and fraud. We fear that unless these shortcomings are addressed, the result will be a diversion of resources from effective detection, investigation, and corrective action and will necessitate wasteful expenditure on burdensome, paperwork-laden compliance exercises. Bankers' attention will be drawn into wasteful but obligatory drills to justify each judgment call made under a good faith effort to defeat identity thieves and fraudsters. For these reasons, we strongly recommend that the Agencies substantially simplify the final Regulation and re-cast it to meet the following principles to apply necessary flexibility in the common effort to fight identity theft and fraud:

- Regulate by objective, *not* prescription,
- Take advantage of synergies with existing regulatory standards and operational efficiencies,
- Avoid requirements not mandated by the statute,

• Keep compliance simple, and
• Recognize that *risk-based* considerations work best as guidance and allow for appropriate judgment, rather than rely on fixed rules.

Regulate by objective, not prescription.

Flexibility to combat identity theft is critical because of the changing nature of fraud practices. Fraud and fraudsters are dynamic, constantly altering methods and targets, as must be the fraud detection techniques and solutions. Fraudsters are continually seeking to detect any vulnerability to exploit: when they encounter an obstacle, they search for a way around it.

Similarly, we can expect the proposed Red Flags to become less effective with time. Like water, the crooks will try to find a way around obstacles once they are identified. The mere notoriety of a red flag is a major step towards its obsolescence as a reliable detector. Yet, under proposed Section __90(d)(2)(iii), financial institutions "must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft. . ." Any financial institution that chooses not to adopt one of the Red Flags from this list does so at its own peril. By insisting on this static, one-size-fits-all-or-tell-us-why standard, the proposed rule converts the Red Flags into a regulatory checklist of mandates regardless of their current effectiveness as fraud detectors.

We believe that this approach misses the purpose of the statutory Red Flag provision, which was to merge the strengths of regulators and financial firms to fight fraud more effectively. The regulators, as gatherers of industry-wide information on fraud experiences, were to share that information with financial institutions to inform the anti-fraud efforts of banks and other financial firms. Industry would use that information to keep design effective, up-to-date anti-fraud programs and keep them current. Instead, the proposal is a look behind approach that is more of an effort by the regulators to do what the financial industry can do best, namely design and maintain effective anti-fraud programs.

The proposed regulatory approach appears to be at odds with the Agencies' assertion in the Supplementary Information that they "are proposing Red Flag regulations that adopt a flexible risk-based approach similar to the approach used in the 'Interagency Guidelines Establishing Information Security Standards.... Like the program described in the Agencies' Information Security Standards, the [Identity Theft Prevention] Program must be appropriate to the size and complexity of the financial institution...and the nature and scope of its activities, and be ***flexible to address changing identity theft risks as they arise***." (Emphasis added.) We support that goal as presented in that description, and we believe that the proposal should be revised to be consistent with it.

Unlike the prescriptive language in the Red Flag Regulation, the Agencies' Information Security Standards present a more flexible, workable approach. The guidelines to that standard, the "Interagency Guidelines Establishing the Standards for Safeguarding Customer Information," set forth instead general objectives to "ensure the

security and confidentiality of customer information," "protect against any anticipated threats or hazards," and "protect against unauthorized access." Equally, the Guidelines' directives are focused on key desiderata: "identify reasonably foreseeable internal and external threats that could result in unauthorized disclosures, misuse. . . of customer information. . .," "assess the likelihood and potential damage of these threats. . ." The Guidelines require financial institutions to consider suggested measures, but only those the "the bank holding company concludes are appropriate."

We recommend that the Agencies adopt similar language in the Red Flag Regulation that will allow financial institutions the discretion and flexibility necessary to have up-to-date effective programs that best fit the needs of their customers and their activities. As the Supplementary Information succinctly states, "Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent and mitigate identity theft." This fundamental objective may be most effectively pursued by describing the regulatory duty to establish an Identity Theft Prevention Program by the simple directive paraphrased from the Bank Secrecy Act, of "developing and providing a program reasonably designed to detect, prevent and mitigate identity theft."

Take advantage of existing synergies.

The proposed regulation pursues the goal of taking advantage of synergies with existing regulatory standards and operating efficiencies in two noticeable ways that ABA applauds.

First, the Supplementary Information suggests that a financial institution may wish to combine its program to prevent identity theft with its information security program, "as these programs are complementary in many ways."

Second, the proposed regulation implements the statutory directive of conforming to the existing Customer Identification Program (CIP) requirements by stating that banks in compliance with the CIP rules satisfy the proposed Regulation's requirement "to obtain identifying information about, and verify the identity of, a person opening an account."

MBA supports both of these policy positions and encourages the Agencies to recognize that financial institutions have other existing fraud prevention, suspicious activity detection, and security risk management practices and procedures that play a valuable role in detecting, preventing, and mitigating identity theft. To realize the synergies of these existing efforts, the Agencies and their examiners should not expect the Identity Theft Program to be represented as a written document separate and apart from a financial institution's overall financial crime risk management processes as long as such over-arching programs contain the elements appropriate for detecting, preventing and mitigating identity theft.

Avoid requirements not mandated by the statute.

MBA believes that the proposed regulation unnecessarily insists on requirements not mandated by statute. These requirements limit flexibility, impose undue costs, and get in the way of effective identity theft and fraud prevention.

Among the non-mandated regulatory requirements are the following:

- Overreaching scope of Regulation's application
- A written Identity Theft Prevention Program
- A specified obligation for boards of directors that is inequitable

First, since the task at hand is to implement part of the FACT Act, MBA considers the proper scope of the proposed Regulation to be limited to consumer financial services, not business financial services. The statute does not need a definition of "account" to give effect to its terms, let alone a definition that expands coverage to business purpose credit or services.

Second, while the statute calls for reasonable procedures for implementing Red Flag guidelines, it does not demand the formality imposed by requiring a written Identity Theft Prevention Program. As previously noted, identity theft prevention is an initiative seamlessly integrated in institutions' financial fraud and crime risk management processes. Carving out a separate writing for a capital "I", capital "T", capital double "P" –Identity Theft Prevention Program—exalts form over the very real substance of efficient, broad-based fraud deterrence systems and will only lead to examiners and auditors insisting on dotted "I"s , crossed "T"s, and well-rounded "P"s.

Third, no whisper of board involvement is mentioned in the law, yet the proposed Regulation creates a novel definition of board of directors that ends up imposing a management duty on boards of directors for financial institutions (yet leaves this responsibility to the lowly "designated employee" in companies lacking formal boards). Further, blurring of responsibilities between management and board was wisely not mandated by Congress and is a distraction from the important goal of fighting identity theft.

In addition, flexibility may be further reduced by the requirement that the board of directors approve the program. By nature, programs requiring board approval demand extensive documentation and very deliberate drafting as well as very particular administrative review. Yet, also by nature, fraud and identity theft pop up quickly and demand a nimble, quick, and sometimes discrete response. Management may be reluctant to respond by taking an action not yet contained in the official, board-approved Program, especially if it is different from the current Program. Requiring board approval of a Program hinders change, which is critical when addressing fraud. Boards do not shoulder such detailed approval obligations for fraud systems today, and no case has been presented demonstrating the need to involve boards in the details of any one specific class of fraud threat. Notably, in the Supplementary Information the Agencies excuse their own

inability to coordinate their respective formal regulatory structures to meet the statutory mandate to update the Red Flags "as often as necessary" or "quickly enough to keep pace with rapidly evolving patterns of identity theft," but then would impose a non-statutory requirement for more administrative procedure on banks. (See e.g., 71 Federal Register at 40791, text and footnote 20.) MBA believes these invented requirements and other non-mandated aspects of the proposed Regulation are unnecessary and in fact harmful to effective programs to address identity theft.

Keep compliance simple.

As proposed, the Regulation erects a number of burdensome compliance exercises that limit flexibility and add costs, which in turn sap resources from the ultimate objective of combating identity theft. In addition to the non-mandatory elements of the proposed Regulation, the rigidity of the Red Flag implementation process is also riddled with unnecessary compliance hurdles.

For example, under proposed Section __90(d)(1), "At a minimum, the Program must incorporate any relevant Red Flags" from the proposed Appendix J as well as from other sources, including supervisory guidance, incidents of identity theft the financial institution has experienced, and new methods of identity theft the financial institution has identified. While the proposal qualifies this requirement with "relevant" Red Flags, the provision in effect imposes a mandatory review, analysis, and report of the Red Flags proposed in Appendix J and elsewhere, and of virtually any new identity theft incident or trend and potential fraud prevention measure, regardless of likely continuation, application, or impact on the financial institution or its customers. And these reviews, analysis, and reports are continuing.

Similarly, under proposed Section __90(d)(1)(ii), financial institutions "must consider" certain factors in identifying whether particular Red Flags are relevant. Many institutions may, in fact, consider these factors, but they may be indirectly factored into an overall design or categorized differently, for example. Some with effective identity theft and fraud prevention programs may not use these factors at all while relying on others just as—or even more—relevant or reliable. As a compilation in an official regulation, however, they achieve a priority status, becoming an artificial checklist for the financial institutions ***and their examiners***, requiring financial institutions to reconstitute their approach to the Identity Theft Program, when doing so does not advance the goals of the Program. Identity Theft Programs are thereby drawn to a uniform average that the Agencies themselves admit that they themselves cannot keep current and up to date. Identity Theft Programs in practice become hobbled by a backward looking ball and chain, when, ironically, the provision in the law was enacted to direct the Agencies to provide the information that financial institutions could use to keep their Identity Theft Programs forward looking and ahead of the crooks. Under the proposal, too much attention by financial institutions will be directed toward regulators in a distracting compliance exercise.

The proposal assumes that all the Red Flags are relevant to every financial institution and puts the burden on the financial institution to research, analyze, document, and then persuade examiners that a particular Red Flag does not apply to a product. In many cases, it will be self-evident that a Red Flag does not apply, but the financial institution will nevertheless have to justify and document its exclusion. This is contrary to Congressional intent, which was that Red Flags be an aid to industry, not a nuisance.

Moreover, financial institutions will have to incur costs to re-design identity theft and fraud programs into artificial packages in order to fit into the regulatory scheme examiners will expect. In practice, many identity theft and fraud prevention components are integrated throughout the institution, from the teller to the back office, and not neatly set out to conform to the proposed regulatory list. To ensure that financial institutions retain the ability to design the most effective solutions, which they have a substantial incentive to do, since they usually suffer on average a $10 loss for every $1 lost by their customers—added to which is very understandable customer dissatisfaction—it is critical that they have broad discretion in designing their Programs and that they not be expected to navigate an arbitrary checklist with their examiners.

As prescriptive as the proposed regulation is, it invites examiner and internal auditor micro-managing and potentially pointless criticism— not because a bank's program does not detect or prevent identity theft, but because it does not have all the required regulatory paperwork justifying each and every element either contained or not contained in the Program.

The regulations should emphasize risk-based consideration.

MBA endorses true risk-based compliance. There is wide latitude in such an approach for banks to conduct their business. MBA believes that risk-based judgments by banks about their identity theft practices and procedures should receive deference by the Agencies, not just lip-service. The key to any risk-based approach is the ability to evaluate the likelihood and severity of adverse events and to prioritize one's response in a manner that applies greater resources to the event of greater expected significance and fewer resources to events of lesser significance. In other words, control programs are to be tailored to expected experience.

Too often of late, "risk-based" has become a label for a supervisory expectation that banks must identify all the risks and build elaborate controls, with equally elaborately documented evaluations, for every one of them. A genuine risk-based approach should lead to prioritizing the importance of various controls, addressing the most important risks first and accepting the good faith judgments of banks in differentiating among their options for conducting safe, sound and compliant operations.

How financial institutions go about a risk-based approach varies widely, as do the risks themselves and the environments in which they occur, and can be just as successful informally in modest risk circumstances as when formally conducted in diverse, complex

operations. Accordingly, the regulation itself should stress the risk-based aspect of Red Flag Programs.

The Agencies should adopt an Official Staff Commentary.

In keeping with the goal of providing assistance to industry risk-based judgment, we also strongly recommend that an Official Staff Commentary accompany the final Regulation, as is the case with many other regulations. We believe that a Commentary will be critical to financial institutions for implementation of the Regulation as well as for continued compliance. A Commentary will ensure that financial institutions have convenient access, in an understandable format, to important guidance related to the final Regulation. Further, the Agencies will have a mechanism for providing additional guidance as the need arises.

Conclusion.

The MBA and its members strongly advocate simplifying the Regulation and revamping the Red Flag guidelines to put the emphasis where it belongs—on reasonably designed procedures that assist banks in fighting identity theft prevention, rather than on new regulatory programs with reams of identity theft compliance documentation that divert resources from the problems we all wish to solve.

Thank you for the opportunity to comment on the above notice of inquiry. If I can be of additional assistance, please let me know.

Sincerely,

/Signed

Max Cook, President