



919 18th Street, NW
Suite 300
Washington, DC 20006

September 18, 2006

VIA Electronic Mail

Office of the Comptroller of the Currency
250 E Street, SW
Public Reference Room
Mail Stop 1-5
Washington, DC 20219

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

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

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 2006-19

Mary F. Rupp, Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428

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

Re: Red Flags Rule - Comments

OCC Docket No. 06-07
Board Docket No. R-1255
FDIC RIN 3064-AD00
OTS No. 2006-19
NCUA Comments on Proposed Rule 717
FTC The Red Flags Rule, Project No. R611019

Ladies and Gentlemen:

The American Financial Services Association ("AFSA") hereby submits this comment letter in regard to the proposed Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 (the "Red Flags Rule" or "Rule") issued for public comment on July 18, 2006 by the Board of Governors of the Federal Reserve System ("Board"), Federal Deposit Insurance Corporation ("FDIC"), Office of Thrift Supervision ("OTS"), Office of the Comptroller of

September 18, 2006

Page 2

the Currency ("OCC"), National Credit Union Administration ("NCUA") and Federal Trade Commission ("FTC") (collectively, the "Agencies").

AFSA is the trade association for a wide variety of market-funded providers of financial services to consumers and small businesses. AFSA members are important sources of credit to the American consumer, providing approximately over 20 percent of all consumer credit. AFSA member companies offer or are assigned many types of credit products, including mortgage loans.

As financial services providers, AFSA's members will be directly and materially impacted by the Red Flags Rule. Although AFSA generally supports the Agencies' proposal, there are a number of revisions and clarifications that we believe will be critical to ensuring that the Red Flags Rule implements the relevant Fair and Accurate Credit Transactions Act's ("FACT Act") requirements without unnecessarily burdening the financial services industry. Our comments follow.

I. General Comment

The Red Flags Rule will create a substantial set of new compliance obligations for the financial services industry. In many instances, complying with the new requirements will be expensive and burdensome, and will inconvenience consumers by increasing the time - and potentially the costs - involved in obtaining financial products and services. Although AFSA acknowledges the need for the Rule, we believe it is extremely important that the Agencies impose only those requirements that are essential to accomplishing their goals.

While AFSA strongly supports the goal of mitigating and/or preventing identity theft, we are concerned that many of the requirements in the Red Flag Rules, if adopted, would not really accomplish that objective. If the Rules as proposed are not modified, financial institutions and creditors will be forced to expend considerable resources on complying with many requirements that will not accomplish the ultimate goal of substantially reducing identity theft. We are confident that the industry is fully committed to devoting resources toward combating identity theft. However, we urge the Agencies to provide institutions with the flexibility to implement measures that they know will effectively deal with the issue, as opposed to expensive procedures that they know will result in little or no actual benefit to consumers.

II. Comments of Specific Provisions

A. Definitions of “Account” and “Customer”

In Red Flags Rule Section __.90 (b),¹ the definition of “account” – the term the Agencies use to describe the relationships covered by FACT ACT Section 114 – specifically includes extensions of credit for business purposes and demand deposit, savings or other asset accounts for business purposes. Similarly, the Rule’s definition of the term “customer” – the term used to describe the account holders and customers covered by the Rule – refers to any “person,” which the preamble indicates is intended to cover various business entities as well as individuals. See 71 Fed. Reg. 40786, 40790 (July 18, 2006).

AFSA believes that the Red Flag Rule should apply only to accounts established for personal, family and household purposes and to customers who are individuals. Limiting the Rule to personal, family and household purposes is consistent with the Fair Credit Reporting Act’s (“FCRA”) general applicability and the Fact Act’s legislative history. Furthermore, the benefit gained by expanding the Rule’s applicability to businesses will not be justified by the increased burden on financial institutions.

To begin with, the FTC’s Official Staff Commentary to the FCRA (“Commentary”) defines the term “consumer” to mean “an individual entitled to the Act’s protection” and “consumer reports” to mean “reports about consumers.” 16 C.F.R. § 600, App. (discussing section 603(a)). Furthermore, the Commentary emphasizes that the term “consumer” “includes only “a natural person,” and not artificial entities (e.g., partnerships, corporations, trusts, estates, cooperatives, associations...” Id. Moreover, the legislative history to the FACT Act clearly indicates that Congress intended the statute’s provisions to protect consumers. See e.g., House Committee of Financial Services Press Release (Nov. 21, 2003) (“House and Senate negotiators reached an historic agreement today on legislation to protect consumers from identity theft. The bill . . . gives consumers unprecedented tools to fight identity theft . . . “This is the most significant consumer protection and financial literacy legislation passed by Congress in decades.) (emphasis added).

¹ In referring to specific sections of the Red Flag Rule in this letter, we have used the shared numerical suffixes and Appendix reference of the OCC, Board, FDIC, and OTS. See 71 Fed. Reg. 40786, 40789 (July 18, 2006).

September 18, 2006

Page 4

In addition, the FCRA Commentary supports the proposition that FCRA does not extend to situations involving the extension of credit for business purposes. In fact, the Commentary expressly excludes reports on businesses for business purposes from the scope of the FCRA:

Reports used to determine the eligibility of a business, rather than a consumer, for certain purposes, are not consumer reports and the FCRA does not apply to them, even if they contain information on individuals, because Congress did not intend for the FCRA to apply to records used for commercial purposes (see 116 Cong. Rec. 36572 (1970) (Conf. Report on H.R. 15073)).

Id. (discussing section 603(d)). Additionally, in discussing FCRA Section 604, the Commentary defines the term “business transaction” to mean “a business transaction with a consumer primarily for personal, family or household purposes. Business transactions that involve purely commercial purposes are not covered by the FCRA.”

Id. (discussing section 604(3)(E)). Thus, the Red Flag Rules go beyond the intention of Congress and the FTC, as expressed in the Commentary, by expanding the definition of the term “customer” to include businesses and defining the term “account” to include extensions of credit for business purposes.

In addition to being inconsistent with the FCRA, the FCRA Commentary and the FACT Act’s legislative intent, AFSA believes that the additional burden associated with requiring financial institutions to implement the Rule in connection with businesses will not be justified by the resulting benefit. Although businesses can in some cases be subject to identity theft, the problem is much more significant and costly in connection with consumers. Furthermore, the Customer Identification Program requirements issued pursuant to the Patriot Act apply to businesses as well as consumers; thus, there already is a regulatory requirement in place that protects business entities from the most common type of identity theft risks – those associated with new account openings. See 31 C.F.R. § 103.121. For these reasons, we do not believe the Agencies should further burden the industry by extending the scope of the Rules beyond what is necessary to protect consumers and is supported by the FACT Act’s legislative history.

B. Duties of Users Regarding Address Discrepancies.

Section __.82 of the Red Flag Rule requires users of consumer reports (“users”) to “develop and implement reasonable policies and procedures” for verifying the identity

September 18, 2006

Page 5

of a consumer for whom it has obtained a consumer report and for whom it has received a notice of address discrepancy. Additionally, Section __.82 requires users to “develop and implement reasonable policies and procedures” for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency (“CRA”) from which the address discrepancy notice was received, if the user can verify the consumer’s identity, establishes or maintains a continuing relationship with the consumer, and regularly furnishes information to the CRA from which the notice was received.

AFSA requests that the Agencies limit the obligations imposed on users under Section __.82 to situations in which a user has obtained a consumer report in connection with establishing a new relationship with a consumer and actually establishes the relationship. Financial institutions often obtain consumer reports in connection with reviewing existing accounts. Address discrepancies in such situations – where the relationship with the consumer is already in place – present little or no risk of identity theft. Furthermore, institutions and creditors should not be required to comply with Section __.82 when they decline to proceed with a transaction (because, for example, the consumer’s credit score was too low to qualify for a loan). Given that the Red Flag Rule – including Section __.82 – will create a whole new set of costs and burdens for the industry, we urge the Agencies to limit the new obligations to those situations in which they will have a material impact on identity theft prevention. Given that the FACT Act directs the Agencies to provide guidance regarding “reasonable” policies and procedures that a user should employ when it receives an address discrepancy notice (see 15 U.S.C. § 1681c(h)(2)), we believe that the Agencies have the authority to limit the Section __.82 obligations to those circumstances that actually involve a real risk of identity theft.

AFSA also urges the Agencies to establish a safe harbor provision for users who establish and follow the policies and procedures required by Section __.82. The FCRA contains an express private right of action for willful and negligent noncompliance with the statute. 15 U.S.C. §§ 1681n and 1681o. Given the significant exposure created by these provisions, users need protection from private claims in cases where they in good faith establish and comply with the policies and procedures policies required by Rule Section __.82.

Finally, we request that the Agencies provide CRAs with guidance on what constitutes a “substantial difference” between an address provided by a user and an address on file with a CRA, and direct CRAs to provide a notice of discrepancy only when the difference is substantial. AFSA members have observed that CRAs tend to

September 18, 2006

Page 6

send discrepancy notices even when address differences are minor, and that in the vast majority of cases, the situation does not involve identity theft. Each time a user must go through the extra steps of verifying a consumer's identity and furnishing a confirmed address to a CRA, it will incur additional operational burdens and costs. These burdens and costs should be imposed only when the address discrepancy is material enough to present a real risk.

C. Board of Directors Involvement

Section ____90(d)(5)(i) of the Red Flags Rule would require "the board of directors or an appropriate committee of the board" to approve the written identity theft prevention program. Although AFSA agrees that identity theft prevention is critical to consumers, creditors and financial institutions, we believe that it is inappropriate to elevate the approval of the written program to the board or a board committee. Boards of directors typically are responsible for high level, strategic decision-making and oversight. While a board should be responsible for oversight over an institution's overall compliance function, we do not believe it is appropriate to require a board to expend its resources on reviewing and approving the details of an identity theft prevention program or the implementation of any other discrete regulatory requirement. Such a requirement would be an inefficient use of the board's time and resources. Furthermore, requiring board approval of some compliance programs but not others could be misconstrued to diminish the importance of compliance all regulatory requirements. Consistent with Rule Section ____90(d)(5)(ii), which allows senior management to oversee the development, implementation, and maintenance of the program, we believe that senior management approval also should be sufficient for the approval of the written identity theft prevention program.

D. Implementation Date

The Red Flags Rule will require financial institutions and creditors to expend a considerable amount of time and resources. At a minimum, each entity subject to the Rule will need to perform a comprehensive risk assessment, develop and document an identity theft prevention program, design a strategy to implement the program, train employees and establish third party service provider oversight procedures. This effort will involve participation by and coordination among many different divisions within each organization. Further, the new requirements will likely require significant changes to established procedures, software and technology enhancements, input from third parties (such as legal counsel, software providers, and consumer reporting agencies), as well as changes to third party service provider arrangements. AFSA urges the

September 18, 2006

Page 7

Agencies to carefully consider the extent of the burden the new requirements will place on the industry and provide financial institutions and creditors enough time for implementation. We note that the FTC provided financial institutions with a year to implement its Standards for Safeguarding Customer Information. See 67 Fed. Reg. 36484 (May 23, 2002). At a minimum, the Agencies should provide creditors and financial institutions with the same amount of time to implement the Red Flags Rule.

E. Duties of Card Issuers Regarding Changes of Address

Red Flags Rule Section __.91 requires credit card issuers to establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account.

We request that the proposed language be amended to require card issuers to assess the validity of an address change if it receives direct notification of the change from the consumer, as opposed to an address change notification from the U.S. Postal Service. There is a higher risk of fraud with direct change of address notices and corresponding requests for a card as opposed to scenarios where the issuer receives a change of address notice from a third party, such as the U.S. Postal Service. Fraudsters will typically contact the issuer notifying of a change of address and then request a new card

F. Transactions Involving Multiple Parties

Section __.90(d)(4) of the Red Flags Rule addresses the use of service providers in complying with the Rule's requirements. The Rule does not, however, address situations – such as indirect lending - in which multiple financial institutions and creditors are involved in a transaction. AFSA believes that the Red Flags Rule should clarify how the Rules will apply in such transactions.

G. Appendix J

1. Clarify That Appendix J Red Flags Are Examples, Not Mandates

Section __.90(d) of the Red Flag Rule requires that a financial institution or creditor incorporate into its Identity Theft Prevention Program any relevant Red Flags from Appendix J. Throughout the Rule's preamble, the Agencies make it clear that financial institutions and creditors must adopt only those Red Flags that are relevant to their particular operations. See, e.g. 71 Fed. Reg. 40786, 40791 ("The Agencies are not proposing to prescribe which Red Flags will be relevant to a particular type of financial institution or creditor."); and 71 Fed. Reg. 40786, 40794 ("Recognizing that a wide range of financial institutions and creditors and a broad variety of accounts will be covered by the Red Flag Regulations, the proposed Regulations provide each financial institution and creditor with the flexibility to develop policies and procedures to identify which Red Flags in Appendix J are relevant to detecting the possible risk of identity theft.")

Even though it appears clear that the Agencies intend the Rule to provide flexibility, AFSA is concerned that certain provisions of the Rule could be viewed as requiring the adoption of specific procedures, regardless of whether they are reasonable given the size, operations and resources of a particular financial institution or creditor. In particular, we are concerned that the Red Flags enumerated in Appendix J could be viewed as a mandatory list, rather than a series of examples.² Accordingly, AFSA requests that the Agencies affirmatively state in the text of the Rule that the Red Flags set forth in Appendix J are examples of the types of Red Flags that financial institutions and creditors can consider incorporating into their programs, but that none of them are mandatory or required. We believe that the language used in the FTC's Safeguards Rule implementation guidance, "Facts for Business: Financial Institutions and Customer Information: Complying with the Safeguards Rule," provides a useful illustration. In particular, this publication uses the following language: "Depending on the nature of their business operations, firms should consider implementing the following practices."

AFSA also is concerned that when a financial institution or creditor detects a Red Flag in connection with a particular account, the Rule does not provide sufficient

² For example, Rule Section __.90(d)(1) requires institutions "[a]t a minimum" to incorporate any relevant Red Flags from Appendix J into their identity theft prevention programs.

flexibility in determining whether the Red Flag does or does not evidence identity theft. In particular, Rule Section __.90(d)(2)(iii) states that if a Red Flag is detected, the institution or creditor “must have a reasonable basis for concluding that [it] does not evidence a risk of identity theft.” (emphasis added.) We believe that the Rule should be revised to ensure that financial institutions and creditors have the flexibility and discretion to use their own judgment to determine whether or not a Red Flag presents a real risk of identity theft in connection with a particular transaction.

2. Risk Assessment Should Include Compliance Burden Assessment

Rule Section __.90(d)(1)(ii) directs financial institutions and creditors to perform a risk evaluation to determine which Red Flags are relevant to its operations. We believe it is critical for the Agencies to clarify that in performing such a risk evaluation, institutions and creditors can include an assessment of the practicalities – including time, costs and burdens -- associated with adopting any given Red Flag. Although some Red Flags may be effective in detecting potential instances of identity theft, implementing them could involve unjustified costs and inconveniences, and do little more than create delays and frustrate consumers. For example, Red Flag # 3 states as follows:

3. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries.
 - b. An unusual number of recently established credit relationships.
 - c. A material change in the use of credit, especially with respect to recently established credit relationships.
 - d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Although this Red Flag would likely be useful in detecting identity theft, if lenders were required to painstakingly review all loan applicants' consumer reports for evidence of inconsistent activity patterns, credit decisions that currently take minutes – because they are based on credit scores and few other factors - could literally take weeks or longer. The time delays, inconvenience and costs associated with this result are not

September 18, 2006

Page 10

justified by the likelihood that such reviews would help to detect identity theft in some cases. Financial institutions and creditors must be permitted to include the costs and operational burdens associated adopting Red Flags into their risk assessment process.

*

*

*

*

We appreciate the opportunity to comment on the Red Flags Rule. If you have any questions, please call 202-776-7300.

Sincerely,

Robert McKew
Senior Vice President and General Counsel
American Financial Services Association