September 18, 2006

Via electronic delivery

John C. Dugan
Comptroller of the Currency
250 E Street, S.W.
Public Information Room
Mail Stop 1-5
Washington, D.C. 20219
Docket No. 06-07, Red Flags Rule

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552
Attention: No. 2006-19
Red Flags Rule

Jennifer J. Johnson
Secretary
Board of Governors of the Federal
Reserve System
20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551
Docket No. R-1255, Red Flags Rule

Mary F. Rupp
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428
RIN 3084-AA94
Rule 717, Red Flags Rule

Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, D.C. 20429
Re: RIN 3064-AD00, Red Flags Rule

Federal Trade Commission
Office of the Secretary
Room 135-H (Annex M)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
Red Flags Rule
Project No. R611019

Re: Interagency Proposal on Identity Theft Red Flags

Dear Sirs and Madams:

The Mortgage Bankers Association (MBA)[1] is pleased to comment on the proposed interagency regulations on identity theft red flags under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The proposal is designed

---

1 The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 500,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets; to expand homeownership and extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 3,000 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, Wall Street conduits, life insurance companies and others in the mortgage lending field. For additional information, visit MBA's Web site: www.mortgagebankers.org.

to prevent identity thieves from opening an account at a financial institution purportedly in the name of another. This is an important area of regulatory focus because identity theft has been a problem to consumers and to consumer lenders.

I. BACKGROUND

Six Federal agencies (the Agencies) propose to implement a requirement in § 114 of the FACT Act[2] that requires financial institutions to establish programs regarding identity theft. This § 114 requires the Agencies to establish guidelines regarding identity theft, and mandates regulations requiring financial institutions to implement the guidelines. The required regulations and guidelines are the subject of the current proposal.

Identity theft often occurs with breaches of privacy, and the two are often blurred together. It is important to note the distinction, however. An identity thief often will breach a consumer's privacy, such as by gaining unauthorized access to the consumer's identifying information at a financial institution. This is a breach of privacy. The thief may then go to a different financial institution and use the consumer's information to get a loan in the consumer's name without the consumer's knowledge. Using the information to try to obtain this loan is identity theft. The current proposal focuses on identity theft rather than breaches of privacy.

The proposed regulations would require financial institutions and creditors to have written identity theft prevention programs that include reasonable policies and procedures, and, more particularly, that identify "red flags" warning of identity theft risk. The identity theft prevention programs must require preventive steps in the case of an identity theft risk, commensurate with the degree of risk.

The proposal specifies internal board oversight and reporting requirements, would require staff training, and would require actions to help ensure that service providers are in compliance with the proposed red flag regulation.

While the proposal would apply to financial institutions and creditors broadly defined, MBA comments on the provisions of interest to mortgage market participants. Identity theft affects single family lenders but we know of no instances of identity theft affecting commercial or multifamily mortgage lenders, so we first cover the issues applicable to commercial and multifamily lending, then we separately discuss other issues.

[2] Fair and Accurate Credit Transactions Act (FACT Act) § 114, codified at 15 U.S.C. § 1681(m)(e)(1).

II. IDENTITY THEFT IS A PROBLEM FOR CONSUMERS AND CONSUMER LENDERS, BUT NOT FOR COMMERCIAL AND MULTIFAMILY MORTGAGE BORROWERS OR LENDERS. COMMERCIAL AND MULTIFAMILY MORTGAGE LENDERS SHOULD NOT BE SUBJECT TO THE PROPOSED RULE.

A. Identity Theft Is Not a Problem in Commercial and Multifamily Mortgage Lending.

Certainly identity theft problems exist in consumer lending. Identity thieves have many methods by which they can and do obtain loans by using another's personal information, without that person's knowledge or consent. By stealing a person's name, address, and Social Security number, identity thieves can go to a financial institution and apply for a loan using the stolen information. Unless the lender has sufficient safeguards in place, the identity thief can often fraudulently get the loan proceeds.

Commercial and multifamily mortgage lending is so fundamentally different from consumer lending that identity theft is not an issue in the commercial and multifamily mortgage markets.

Commercial and multifamily lenders base their underwriting primarily on the collateral property. Single family mortgage lenders rely on the consumer's creditworthiness and, as a last resort, the collateral property.

This basic distinction explains why underwriting commercial and multifamily loans is vastly different from underwriting single family loans. Single family lenders rely primarily on consumers' credit histories and credit scores, as indicators of the consumers' ability to repay, and loan-to-home value ratios, as an indicator of the consumers' incentive to stay in the home. Commercial and multifamily lenders rely on expected future cash flows from the collateral property. Predicting these cash flows requires verifying every reasonable risk factor that could affect the cash flows, and there are quite a number of them.

Additionally, commercial and multifamily loans have larger principal balances than single family loans, commonly well into the tens of millions of dollars, so bad credit decisions are especially costly on commercial and multifamily loans. Single family lenders are more able to take the occasional bad loan in stride. The heightened need for careful credit decisions, due to potentially significantly larger losses, is part of the reason that commercial and multifamily mortgage lenders do much more extensive and detailed underwriting than do single family lenders.

Commercial and multifamily mortgage lenders look at a number of criteria that single family lenders do not. These include rents in the collateral property, of course, but lenders also look at factors that may affect rents over the life of the loan. These include vacancy rates, new construction of competing properties, the

population level, area income levels, inflation, and trends in all of these factors. Lenders also must consider all operating costs, including taxes, utility costs, and management and maintenance costs, both short term and long term. Commercial lenders look at commercial tenants' creditworthiness and ability to pay rent, and multifamily lenders have to consider rent control requirements. Because commercial and multifamily mortgage loans are all different, lenders also have to consider any significant contract provisions that may affect the risks in each individual loan.

Commercial and multifamily lenders physically inspect the property during loan underwriting, so it is not realistic for a borrower to deceive the lender about which property is the collateral.

Commercial and multifamily mortgage lenders also look at the principals involved in the ownership entity to which the loan will be made, even though the principals may not be personally liable on the loans. Lenders review the experience and track record of the ownership entity and its principals because they may impact the success of the property and thus of the loan.

Given the extensive underwriting, checking, verifying, and documenting that occurs for each and every commercial and multifamily mortgage loan in this country, it is unrealistic to believe anyone could, through identity theft, fraudulently obtain a commercial or multifamily mortgage loan. In these ways, commercial and multifamily lending is of a very different nature than single family lending.

MBA sees no reason to impose a new regulatory burden on commercial and multifamily mortgage lenders requiring them to prevent lending to identity thieves, when they already do so very effectively.

B. The FTC's Website Makes Clear That Identity Theft Is a Consumer Problem.

The Federal Trade Commission (FTC)'s website provides a wealth of information about identity theft, such as a description of the various forms it can take, how to prevent it, and what to do when it happens. Notably, the site map at ftc.gov lists this information under "For Consumers" and not under "For Businesses[.]" The FTC also describes methods of identity theft, stating that "Skilled identity thieves use a variety of methods to steal your *personal* information" (emphasis added).[3] Further, the FTC describes methods for deterring identity theft, explaining that "Identity theft is a serious crime. It occurs when your *personal* information is stolen and used without your knowledge to commit fraud or other crimes" (emphasis added).[4]

[3] Available at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm.
[4] *Id.*

Identity thieves steal personal information because some lenders make *consumer* loans based on fraudulent *consumer* loan applications.

None of the Agencies set forth any reason to believe identity theft is or will become a problem in the commercial and multifamily mortgage markets.

C. The FACT Act Provides Authority to Exempt Commercial and Multifamily Mortgage Lenders From the Red Flags Rule.

The statutory requirement for the red flags proposal is in § 114 of the FACT Act:

> The Federal banking agencies, the National Credit Union Administration, and the [Federal Trade] Commission shall jointly, with respect to the entities that are subject to their respective enforcement authority . . .
>
> (A) establish and maintain guidelines for use by each financial institution and creditor regarding identity theft with respect to account holders at, or customers of, such entities, and update such guidelines as often as necessary. . . .[5]

This FACT Act provision amends the Fair Credit Reporting Act (FCRA). The FCRA defines creditor to include:

> [A]ny person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.[6]

The term "person" in this definition is broadly defined to include corporations, partnerships, and other entities.[7]

1. The Agencies Have Statutory Authority to Construe the Term "Creditor" in § 114 to Exclude Commercial and Multifamily Mortgage Lenders.

The term "creditor" is defined in the FCRA broadly to include many creditors. The Red Flags Proposal, however, is narrow, and applies only to identity theft, the unauthorized use of a consumer's identifying information to obtain a loan.

It is important to distinguish identity theft from a breach of privacy.

- Identity theft is the unauthorized *use* of a consumer's identifying information, regardless of how the recipient accessed the

[5] FACT Act § 114, codified as § 603(r)(5) of the Fair Credit Reporting Act (FCRA) at 15 U.S.C. § 1681(m)(e)(1).
[6] FACT Act § 111, codified as § 603(r)(5) of the FCRA, 15 U.S.C. § 1681a, incorporating by reference the definition of creditor from 15 U.S.C. § 1691a(e).
[7] FCRA § 603(b), 15 U.S.C. § 1681a(b).

information. While the recipient may access the information improperly, a consumer may voluntarily give personal information to another, not expecting the recipient to use the information improperly. In either event, identity theft often occurs when the recipient *uses* the consumer's identifying information to obtain a loan in the consumer's name without the consumer's consent. It is this improper use of consumer information that FACT Act § 114 and the current red flags proposal intend to prevent.

- A breach of privacy is the improper *access* to a person's information, regardless of whether the recipient ever uses the information. Breaches of privacy often occur without resulting identity theft. Privacy is regulated by the Gramm-Leach-Bliley Act and its implementing regulations. [8]

As to commercial and multifamily lenders, this distinction is especially significant. Commercial and multifamily lenders can and do obtain information about individuals. In underwriting a loan, for example, commercial lenders may obtain credit histories and other personal information about the principals in the ownership entity. It is possible that an identity thief could hack into a commercial or multifamily lender's database and steal this personal identifying information. That would be a breach of privacy but not identity theft.

In other words, the current proposal is designed for one purpose – to require lenders to avoid making loans to identity thieves. Commercial and multifamily mortgage lenders have broad and extensive protections in place to prevent many types of faulty loans, including loans to identity thieves. It is therefore reasonable for the Agencies to construe the term "creditor," for § 114 purposes, to exclude commercial and multifamily mortgage lenders.

Any other construction would result in a waste of resources, requiring commercial and multifamily mortgage lenders to create, get board approval of, report annually on, and train staff to implement, a useless program that duplicates longstanding industry protections.

[8] The Gramm-Leach-Bliley Act requires financial institutions, whether or not they are creditors, to maintain information security standards to protect the privacy and security of information. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436 – 37 (1999) (codified at 15 U.S.C. § 6801(b)). The Agencies issued final standards to implement these requirements, at 66 Fed. Reg. 8152 (Jan. 30, 2001) (National Credit Union Administration); 66 Fed. Reg. 8616 (February 1, 2001) (Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision); 67 Fed. Reg. 36484 (May 23, 2002) (Federal Trade Commission).

2. The Agencies Have Statutory Authority to Construe the Terms "Account Holders" and "Customers" to Exclude Account Holders and Customers of Commercial and Multifamily Mortgage Lenders.

The § 114 provision quoted above requires red flag programs to prevent "identity theft with respect to account holders at, or customers of" financial institutions and creditors. This must mean that Congress requires identity theft red flag programs regarding account holders or customers that can or might reasonably be expected to result from identity theft. This must be true because preventing identity theft could be the only logical purpose to requiring identity theft prevention programs. As discussed above, commercial and multifamily mortgage loans are not at reasonable risk of identity theft.

It is true that the proposal is risk-based, requiring more preventive steps in circumstances when there is more risk of identity theft, and fewer preventive steps when there is less risk. The proposal does not, however, permit a covered lender to take no steps when there is no reason to believe there is a risk. Even for commercial and multifamily mortgage lenders, the proposal would impose requirements. These lenders would have to create written identity theft red flags programs, obtain approval of the programs from the boards of directors or from board committees, train staff to implement the programs, and submit annual reports on the programs. Because commercial and multifamily mortgage lenders already so thoroughly and extensively protect themselves from identity theft, there is no purpose to imposing these regulatory requirements on them. Congress could not have intended to apply the red flag requirements to commercial and multifamily mortgage lenders because it would impose costs with no benefit. Similarly, the Agencies have not stated a reason to apply these requirements to commercial and multifamily mortgage lenders.

3. The Agencies Have Statutory Authority to Tailor the Red Flags Requirements to Areas of Risk, and to Exclude Commercial and Multifamily Mortgage Lenders.

The Agencies, most appropriately, describe the current proposal as "a flexible, risk-based approach[.]"[9] Congress similarly directed the Agencies to "identify possible risks" of identity theft.[10] The reason Congress requires the Agencies to identify identity theft risks, and the reason the Agencies have proposed a flexible, risk-based approach to identity theft prevention, is to tie the regulatory costs of complying with the new rules with the risks of identity theft occurring. This is what both Congress and the Agencies intend, and it is certainly very sensible.

Using this approach, it is irrational to impose red flag regulatory requirements on commercial and multifamily lenders. To impose this regulatory burden on these

[9] 71 Fed. Reg. 40786, 40788 (July 18, 2006).
[10] FACT Act § 114, codified at 15 U.S.C. § 1681m(e)(1)(B).

lenders would run counter to the risk-based approach both Congress and the Agencies intend.

D. Conclusion – Commercial and Multifamily Mortgage Lenders Should Be Exempt.

For the reasons discussed above, the Agencies should not require commercial and multifamily mortgage lenders to create, implement, or maintain identity theft prevention programs. Even risk-based programs still impose regulatory burden. Because commercial and multifamily mortgage lenders, by the very nature of their businesses, already strongly and effectively protect themselves from identity thieves, there could be no rational basis for imposing identity theft prevention requirements on these lenders.

III. RED FLAG PROGRAM PROVISIONS

While commercial and multifamily lenders have a unique view of the red flags proposal as discussed above, some aspects of the proposal would affect all mortgage lenders. These are discussed in this section.

A. One Program Per Service Provider Is Most Effective.

While the risk of identity theft at a service provider is real, it is important that any preventive measures be designed to reduce these risks. The Agencies ask for comment on whether they should permit a service provider to use an identity theft prevention program that differs from that of the institution that retains the service provider. It is ***extremely important*** to permit this flexibility. It is common for one service provider to serve many financial institutions. Each financial institution will develop its own identity theft prevention program, and each program will be unique in its specifications. There is no reason to require one service provider to incorporate a separate program for each of its individual customers.

The goal is to minimize the risk of identity theft, and that should be the requirement. As long as a service provider uses a program that appropriately minimizes risk, it should not matter whether the form of that program matches the program of one or another financial institution. The goal should be substance rather than form.

Further, one financial institution commonly has multiple service providers. There is no reason to require a financial institution to train each of its many service providers on all the specific details of its identity theft prevention program, then regularly oversee every service provider to ensure continuing compliance with the financial institution's unique program. Again, as long as a service provider uses a program of adequate substance, the program's form should not matter.

Requiring one service provider to implement a different program for each of its customers and requiring each financial institution to impose a unique form of identity theft prevention program on each service provider would greatly increase the cost of, and the time required to implement, the several programs. As long as one program is as effective as another, concern about whose particular program a service provider uses would be unreasonable – it would add significantly to the compliance costs and to the time required to comply with the requirement, but would add no corresponding increase in protection.

MBA very strongly urges the Agencies to permit financial institutions to use identity theft protection programs that differ from the programs that their service providers use. We further urge the Agencies to so state in any final regulation because of the importance of this matter.

B. Institutions Cannot Oversee Their Service Providers' Service Providers.

The proposal would require financial institutions to take steps to ensure that their service providers are complying with an identity theft prevention program that meets the requirements of the proposed regulation. Section __.90(d)(4).[11] The proposal would define "service provider" to mean "a person that provides a service *directly* to the financial institution[.]" Section __.90(b)(6) (emphasis added).

The definition of service provider covers those providers that *directly* service a financial institution, while the operative provision does not make this clarification. MBA recommends that the final regulation add the word "directly" to § __.90(d)(4), to read that when "a financial institution or creditor *directly* engages a service provider to perform an activity on its behalf . . . ." This would make clearer that the regulation requires financial institutions only to oversee their direct service providers.

Financial institutions may not know of, do not have a contractual relationship with, and cannot therefore oversee, their service providers' service providers. Only a party with a direct connection to a service provider can oversee that service provider. Therefore, only the institution that directly retains a service provider should be required to oversee that service provider's identity theft prevention program.

C. Risk of Harm Affects Relevance of Red Flags.

The proposal would require institutions to have policies and procedures to identify red flags that are relevant to detecting a possible risk of identity theft. To identify which red flags are relevant, the proposal would require institutions to

[11] While the Agencies jointly propose substantially similar regulations, each Agency codifies its regulations separately, with differing citations. For ease of reference, citations to the proposal in this letter use the suffix shared by most of the Agencies, with a blank for the C.F.R. Part number.

consider a number of factors: the accounts subject to a risk of identity theft; the methods the institution used to open and provide access to those accounts; and the institution's size, location, and customer base.

While these listed factors are certainly important, the list should also include the risk of harm. Not every red flag indicates a realistic risk of identity theft. For example, an incorrect telephone number on a loan application may be an indicator of identity theft in some cases, but when all other information on a loan application is verified, a typographical error in a telephone number does not necessarily warrant significant action. This list needs to incorporate a reasonable amount of flexibility to require action when reasonable, but not when there is no reasonable risk of identity theft.

The proposal seems to indicate that a reasonableness test is appropriate, in that it provides that institutions "must have a reasonable basis for concluding that a red flag does not evidence a risk of identity theft[.]" Section __.90(d)(2)(iii). To make clear that institutions do not need to act on red flags when they do not pose a reasonable risk of identity theft, the concept should also be included in the list of factors for determining which red flags are relevant in § __.90(d)(1)(ii).

D. Addressing Risks of Identity Theft – Actions Should Be Commensurate With Risk.

After a financial institution has identified relevant red flags and has determined that those red flags evidence a risk of identity theft in a particular instance, some action is warranted. Appropriately, the proposal would not specify a one-size-fits-all action plan. Rather, and appropriately, the proposal would require policies and procedures to address the risk of identity theft "commensurate with the degree of risk posed." Section __.90(d)(2)(iv). It is very important that the actions required be commensurate with the degree of risk in any individual case because every case is unique. This flexibility in the proposal will permit institutions to focus their resources on cases where risks are actual rather than merely possible. MBA supports this flexibility.

E. Board Approval and Reports Should Be Determined Case By Case.

The proposal would require each financial institution's board of directors, or an appropriate board committee, to approve the identity theft protection program. The board, board committee, or "senior management" would be required to oversee the development, implementation, and maintenance of the program. The proposal would further require annual reports to the board, board committee, or to senior management, on the institution's compliance with its identity theft protection program. The proposal specifies a number of material matters that each annual report must discuss and evaluate.

While there is no question that effective oversight of identity theft protection programs is important for lenders at risk of making loans to identity thieves, MBA does not believe that detailed regulatory mandates are necessary or appropriate. Because financial institutions vary in size, business type, and management organization, it would be more appropriate for each institution to determine the form of oversight most effective under its circumstances. For institutions with a history of identity theft risks, annual board reports may be insufficient. Institutions with low levels of risk may not need detailed annual board reports. Further, the institutions themselves, rather than a regulation, should determine what a board report should cover.

Regulatory prescriptions of board and management oversight and of the specific requirements for periodic reports are not required by the FACT Act. Nor are such specific requirements appropriate in the absence of evidence of failure to implement regulatory requirements. Financial institutions often incur financial losses when identity theft occurs, and therefore they have strong incentives to fight identity theft. Finally, financial institutions are already subject to comprehensive oversight and reporting requirements imposed by their federal and state supervisors.

For these reasons, MBA recommends that the Agencies permit financial institutions to independently determine the most appropriate procedures for implementing and maintaining their identity theft prevention programs.

F. Training Relevant Staff.

The proposal would require financial institutions to “train staff to implement” their identity theft prevention programs. Again, this prescriptive mandate appears unnecessary and inappropriate. It would be impossible for an institution to comply with the proposed regulation and guideline without training its staff to do so. MBA believes this provision is unnecessary and should not be included in a final regulation. If the provision is finalized, it should be amended to say “training relevant staff to implement” the programs, because some staff may not be involved in identity theft prevention.

G. Inactive Accounts Are Not Necessarily a Red Flag.

The Appendix to the proposed regulation lists a number of red flags. One is “[a]n 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).”[12] The FACT Act directs the Agencies to consider including reasonable guidelines concerning accounts that have been inactive for longer than two years. The Agencies solicit comment on whether the red flag for dormant accounts should include a two year limit or whether a more flexible red flag, such as the one proposed, is more appropriate.

---

[12] Proposed Appendix to Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, Item 20.

Because there are a variety of types of accounts, MBA believes that a more flexible approach is most appropriate. This would permit financial institutions to concentrate their identity theft prevention efforts in areas of need.

It is common for Americans to put in place a line of credit secured by their homes before they need to draw on the credit. A family may choose this option to prepare for an anticipated future expense, such as the care of an elderly parent, a future medical expense, or a future home repair. The timing of the expense may be hard to predict. One family may put the line of credit in place, then draw on it immediately. Another family may put the line of credit in place then not need to use it for a longer period. It is unreasonable to assume that one case presents more risk of identity theft than the other. By using flexible red flags, the proposal most effectively implements Congress's intent that financial institutions address identity theft risks. MBA supports the red flag for inactive accounts as it is proposed.

H. Other Red Flags Cannot and Should Not Be Predetermined.

The Agencies solicit comment on whether the proposed red flags enumerated in the Appendix to the proposed rule are appropriate, or whether the list should include more or fewer red flags. MBA believes the list is appropriate because the red flags are designed to be flexible. It is not possible to identify every event that may indicate identity theft. Further, a long and rigid list containing a number of irrelevant red flags would bog down financial institutions in documenting why each enumerated red flag is not relevant in each case. This would drain resources away from the goal of preventing realistic risks of identity theft.

I. Identity Theft Prevention Programs.

The proposal, at § __.90(c), would, in broad terms, require financial institutions and creditors to implement a written identity theft prevention program. That program would need to have reasonable policies and procedures to address identity theft risks to customers, and to the safety and soundness of the institution, "in the manner discussed in paragraph (d) of this section." The referenced paragraph (d) contains the specific requirements for an identity theft prevention program. In other words, paragraph (c) would require institutions to have a written program, while paragraph (d) would specify what a program must contain and require.

This reference in paragraph (c) to the specific requirements of paragraph (d) is very important because it indicates that an institution that has a program meeting the specific requirements of paragraph (d) is in compliance with paragraph (c) as well. MBA recommends that the Agencies clarify this point explicitly in a final regulation to remove any possible doubt that compliance with paragraph (d) entails compliance with paragraph (c).

IV. REGULATORY FLEXIBILITY ACT

The Regulatory Flexibility Act requires agencies, in their rulemakings, to consider the impact of rules on small businesses. Congress passed the Regulatory Flexibility Act because:

> [U]niform Federal regulatory and reporting requirements have in numerous instances imposed unnecessary and disproportionately burdensome demands including legal, accounting, and consulting costs upon small businesses, small organizations, and small governmental jurisdictions with limited resources; [T]he failure to recognize differences in the scale and resources of regulated entities has in numerous instances adversely affected competition in the marketplace, discouraged innovation and restricted improvements in productivity[.]
>
> [U]nnecessary regulations create entry barriers in many industries and discourage potential entrepreneurs from introducing beneficial products and processes; [and] alternative regulatory approaches which do not conflict with the stated objectives of applicable statutes may be available which minimize the significant economic impact of rules on small businesses . . . .[13]

Under this act, when a proposed regulation would have a significant economic impact on a substantial number of small entities, the agency must consider alternatives that would lessen the regulatory burden on small entities. In addition, the agency must publish compliance guides to assist small businesses in complying with the new regulation.[14]

In the present rulemaking, none of the Agencies has stated that the rule would have a significant economic impact on a substantial number of small businesses, but the agencies did request comment on regulatory alternatives that would minimize the regulatory burden on small entities. The Federal Trade Commission requests comment on the number of small businesses that its proposed rule would cover.

MBA represents most mortgage lenders in this country. We comment only on the number of small mortgage lenders that would be subject to the proposed rule. Some mortgage lenders are depository institutions. We find there are 10,314 depository institutions with assets of less than $100 million that would be subject to the rule, as it is proposed. We believe this is a substantial number of small businesses. In addition, there are a number of mortgage banks in this country

[13] Regulatory Flexibility Act, Pub. L. No. 96-354, § 2, 96 Stat. 1164 (1980) (codified at 5 U.S.C. § 601 note).
[14] Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, § 212, 110 Stat. 857, 858 (codified at 5 U.S.C. § 601 note).

that are not affiliated with a depository institution. The asset size of these lenders is difficult to pinpoint because some of them have parent companies that may own multiple mortgage banks. Nevertheless, we estimate that there are at least 500 and perhaps as many as 1000 mortgage banks that are independent of depository institutions that would be subject to the proposed rule. We therefore believe this proposed rule would affect a substantial number of small entities.

The Agencies seem to agree that the proposal would not have a significant economic impact on the small entities affected. As discussed above, the proposal would impose a regulatory burden on commercial and multifamily mortgage lenders with no purpose. Useless regulatory burdens are inconsistent with the purposes of the Regulatory Flexibility Act, and these lenders should therefore be exempt from the red flag program requirements.

As to single family mortgage lenders, MBA believes the proposal, as drafted, would not have a significant economic impact. Should a final rule differ from the proposal, our belief may also change.

In particular, we believe the proposal would not have a significant economic impact on mortgage lenders largely because the proposal would not require every service provider to implement an Identity Theft Prevention Program that is the same as that of each of the service provider's lender customers.

Mortgage lenders are quite heavily dependent on service providers, probably more dependent than other lenders. The treatment of service providers in this rulemaking therefore will greatly affect mortgage lenders.

MBA very strongly supports the proposal to permit each service provider to implement its own Identity Theft Prevention Program. We believe that any alternative treatment of service providers in the current rulemaking would trigger the requirements under the Regulatory Flexibility Act for regulations that have a significant economic impact on a substantial number of small entities.

MBA believes that, as to the treatment of service providers, the Agencies have selected the regulatory alternative that minimizes regulatory burdens on small entities. By also exempting commercial and multifamily lenders from the red flags program requirements, the Agencies would finalize the regulatory alternative that minimizes regulatory burden while simultaneously protecting consumers from identity theft.

V. CONCLUSION

MBA supports the efforts by all of the Agencies to deter, detect, and mitigate the harms of identity theft. MBA urges the Agencies to undertake these important efforts while minimizing regulatory burdens, commensurate with identity theft risks.

Because commercial and multifamily mortgage lenders, by the nature of their businesses, protect themselves from identity theft as discussed above, MBA strongly urges that the Agencies exempt commercial and multifamily mortgage lenders from any identity theft red flag requirements. MBA supports the proposal to permit service providers to implement one identity theft prevention program rather than multiple programs. MBA supports the Agencies' efforts to craft flexible and risk-based guidelines and regulations.

Sincerely,

Regina M. Lowrie, CMB
Chairman
Mortgage Bankers Association