September 18, 2006

SENT VIA EMAIL TO: regs.comments@federalreserve.gov

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

RE: Docket No. R – 1255
"Red Flags Rule"

Dear Ms. Johnson:

Countrywide Home Loans, Inc. ("Countrywide") is pleased to submit comments on behalf of the companies in the Countrywide Financial Corporation family in connection with the Agencies' Joint Notice of Proposed Rule Making ("NPRM") implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"). Through its family of companies, Countrywide provides mortgage banking and diversified financial services in domestic and international markets. As a financial service provider, Countrywide is well aware of the threat posed by identity theft and other forms of fraud, and fully supports the efforts of the federal government to require financial institutions to take reasonable steps to mitigate this risk.

On July 18, 2006, the Agencies released their NPRM and requested comment from interested parties on proposed "Red Flag Guidelines" for identifying patterns, practices and specific forms of activity that indicate the possibility of identity theft and requiring reasonable policies and procedures for implementing such guidelines, including validating change of address requests for credit and debit card users. In addition, the Agencies sought comment on proposed rules regarding reasonable policies and procedures for financial institutions that receive notice of address discrepancies from a consumer reporting agency. Countrywide applauds the efforts of the Agencies to provide reasonable and meaningful guidance to financial institutions in meeting the obligations imposed by FACTA. As a member of the Financial Services Roundtable ("FSR"), Countrywide supports the comments in the FSR response. Countrywide appreciates the opportunity to also highlight a few areas, where it believes greater clarity and flexibility could be achieved.

The "Red Flag Guidelines" Under FACTA Section 114

Countrywide supports the Agencies efforts to identify indicators of potential identity theft and the proposed guidance regarding appropriate financial institution policies and procedures. Countrywide believes that the proposed rule could be strengthened in the following ways.

1. The "Red Flags" identified in Appendix J Must Not Each be Required

Countrywide applauds the risk-based nature of the proposed rule. Countrywide believes that this approach can be strengthened by including language in the final rule that makes it clear that the "Red Flags" listed in Appendix J are not required, but rather should be considered by financial institutions when developing their own program for detecting fraud. Countrywide believes that the risk-based nature of each financial institution's program is best developed and preserved where the final rule is clear that the "Red Flags" listed in Appendix J are not each necessary, but are examples that the Agencies believe financial institutions should consider along with the other "Red Flags" that the proposed rule describes. As written, the proposed rule may lead to confusion among both examiners and financial institutions as to the purpose of "Appendix J." Financial institutions may feel compelled to include each Red Flag from Appendix J in their Identity Theft Prevention Program ("Program") regardless of whether a particular Red Flag is relevant to its business model or a cost-effective means of combating identity theft. In the alternative, financial institutions may be forced to develop elaborate justifications for failing to include a particular Red Flag in its Program. Countrywide believes that this would result in wasted time and inefficient allocation of identity theft and fraud prevention resources. The Agencies should clearly state in the final rule that each red flag should be considered in developing a reasonable, risk-based program to detect, prevent and mitigate identity theft and that a financial institution may determine which red flags are appropriate to apply to particular types of transactions or particular types of identity theft risks.

2. Separate Lines of Business or Affiliates Within a Bank Holding Company Must Have the Flexibility to Design Their Own Identity Theft Prevention Programs

Countrywide is a large, diversified, financial services organization, delivering its products and services through multiple, distinct lines of business and affiliated companies. It would be appropriate to make clear in the final rule that organizations, like Countrywide, have the flexibility to design individual Identity Theft Prevention Programs that meet the unique needs of different business lines. A one-size-fits-all approach to a diversified financial services organization, like Countrywide, will not serve the purposes of the proposed rule, nor the interests of consumers. A Program that makes perfect sense for a home mortgage lending affiliate may not be appropriate for an insurance company affiliate or a bank offering deposit accounts within a financial services enterprise like Countrywide. It is consistent with the Agencies' stated desire to have a risk-based, flexible Identity Theft Prevention Program regulation to allow organizations to develop unique, individual Programs tailored to the needs and requirements of each line of business. This consideration would apply equally to the required training component of Programs. Individual lines of business or affiliates must have the flexibility to design independent training to implement its unique Programs.

3. *Frequency of Required Updates to Detection Program Must be Better Defined*

The language of the NPRM indicates that financial institutions must develop Programs that "address changing identity theft risks *as they arise* in connection with the experiences of the financial institution…" [see proposed Section 222.90(c)(2)] and "reflect changing identity theft risks to consumers and to the financial institution…*as they arise.* [see proposed Section 222.90(d)]. Financial institutions, like Countrywide, obviously are keenly aware of and interested in the changing nature of the threats posed by identity thieves and other fraudsters. Nevertheless, the use of the phrase "as they arise" within the context of a regulatory rule, is too vague and potentially too stringent a requirement. Financial institutions will adjust as rapidly as is reasonably possible to the changing nature of the identity theft risk environment. It does not necessarily follow that their written, formal Identity Theft Prevention Programs will be, or should be, updated as rapidly. As written, the Proposed Rule seems to imply that changes in the identity theft risk environment must be reflected immediately or "as they arise" in the written Program. Countrywide believes that the final rule should make it clear that financial institutions have some reasonable period of time to make any necessary changes to their written Program(s) as new or different threats emerge or as technology changes.

4. *Flexibility in Reporting to the Full Board and Senior Management Oversight Responsibility*

Countrywide appreciates and supports the NPRM's requirement that there be senior level involvement in the development, implementation and maintenance of Identity Theft Prevention Programs. The language used in proposed Section 222.90(d)(5), however, would benefit from revisions that make it clear that the full Board of Directors need not be directly involved. At a minimum, the Agencies should clarify in the final rule that any reporting to the board of material information relating to the Program(s) may be combined with reporting obligations required under the Interagency Guidelines Establishing Information Security Standards. The NPRM would also benefit from revisions that make it clear that senior management, or a designated individual within a diverse financial services provider like Countrywide, can fulfill the requirements of proposed Sections 222.90(d)(5)(ii) and (iii). These proposed revisions would facilitate and enhance the Agencies stated desire for flexibility in the development, implementation and maintenance of Identity Theft Prevention Programs.

5. *Application of Identity Theft Prevention Program to Acquisition of Closed Loans on the Secondary Market*

Countrywide believes that is important for the final rule to clarify that the application of a financial institution's Program does not need to operate retroactively with regard to closed loan assets acquired after origination. Countrywide, like many other lenders, acquires closed

loans from correspondent lenders. These lenders accept applications from consumers, process their loan applications, fund and close the loans. Only after the lending process has been fully completed, do they sell the loan to financial institutions like Countrywide. Countrywide is not typically involved in the origination process with respect to these loans. Consistent with the "Customer Identity Program" requirements under the USA PATRIOT Act, the final rule should make it clear that the obligation to implement an effective Program only applies to an acquiring lender on a go-forward basis after acquisition of the loan, servicing rights, or account.

6. Implementation Time Frame Must be Sufficient to Allow Financial Intuitions to Prepare

The NPRM does not address the time frame between promulgation of the final rule and mandatory compliance. Because of the extensive nature of the proposed rule, Countrywide strongly suggests that the Agencies allow financial institutions ample time to bring systems, policies and procedures into compliance with the requirements of any final rule. Countrywide suggests at least 18 months between publication of the final rule and the effective date for mandatory compliance. This would allow many of the provisions of FACTA aimed at reducing the incidents of identity theft to further take hold and allow financial institutions to concentrate on filling any gaps that exist in the array of fraud and identity theft detection and prevention controls already in place.

7. *Comments on Red Flag 13 From Appendix J; "failure to provide required application information.*

Mortgage applications vary by type of loan, despite the fact that many lenders use a standard form of application to collect much of the information. In addition, for customer service reasons, creditors often help applicants complete the application. Finally, the mortgage application process is complex from a consumer perspective, frequently resulting in consumers submitting incomplete information. Within this context, it is not appropriate to consider "failure to provide required application information" as a "red flag" for potential fraud and Countrywide requests that it be removed from Appendix J.

Section 315: Reconciling Consumer Addresses

As with the "Red Flag Guidelines" proposed rule discussed above, Countrywide supports the Agencies efforts in providing effective regulatory guidance with regard to the requirements of FACTA Section 315. Many financial institutions have already taken steps toward full compliance with the requirements of Section 315. As with the proposed rule under Section 114, Countrywide takes this opportunity to suggest changes to the proposed rule.

1. Liability for Good Faith Verification

The proposed rule requires users of consumer credit reports to verify consumer addresses when a discrepancy is reported between the address provided to the consumer reporting agency and the address that the consumer reporting agency has on file. When a "continuing relationship" is established that results in regular reporting to the consumer reporting agency with regard to the consumer, users are required to report an address for that consumer that they have "reasonably confirmed." Countrywide suggests that the Agencies make it clear that users that report "reasonably confirmed" consumer addresses to consumer reporting agencies are not subject to liability for doing so, even if the "reasonably confirmed" address turns out to be incorrect. Users of consumer reports, like Countrywide, should not be financially responsible for false information provided by consumers, or other circumstances that may result in incorrect addresses being "confirmed" despite good faith efforts by those users to prevent that from occurring.

2. Verbal verification with customer acceptable

It is unclear from the text of the proposed rule whether a written document of some kind is required in order for a user of a consumer report to "reasonably confirm" a consumer's address. Countrywide suggests that it would be appropriate to make it clear that, in certain circumstances, it would be appropriate for such confirmation to occur verbally.

Conclusion

Countrywide remains committed to protecting our customer's financial information and identity from the evolving threats posed by fraud and identity theft. Countrywide believes that the proposed rule is a valuable step forward towards regulation consistent with the intentions of the FACTA. Countrywide appreciates the opportunity to comment on this very important matter and would welcome the opportunity to discuss these comments further or answer any questions that you may have regarding our views on this issue. Feel free to contact me at 818-871-5231 with any questions about these comments.

Sincerely,

Christopher Weinstock