

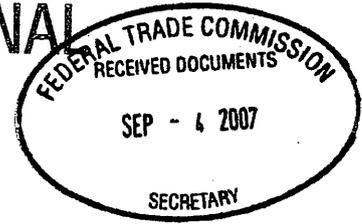


Credit Union National Association

cuna.org

601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | PHONE: 202-638-5777 | FAX: 202-638-7734

ORIGINAL



September 4, 2007

Federal Trade Commission/Office of the Secretary  
Room H-135 (Annex K)  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580.

Re: SSNs in the Private Sector – Comment, Project No. PO75414

Dear Sir or Madam:

The Credit Union National Association (CUNA) appreciates the opportunity to respond to the request from the Federal Trade Commission (FTC) for comments on the use of Social Security numbers (SSNs) in the private sector as it relates to identity theft. CUNA is the largest credit union trade association in this country and represents approximately 90 percent of our nation's 8,500 state and federal credit unions, which serve nearly 87 million members.

### Summary of CUNA's Comments

- Credit unions use SSNs to verify members' identity and to associate the member with the accounts they maintain at the credit union. Government requirements, such as those under the USA PATRIOT Act, also contribute to the need to collect this type of information.
- If any new regulatory requirements are needed to address the misuse of SSNs, they should exclude financial institutions, such as credit unions. Financial institutions are already required to safeguard this type of information under the Gramm-Leach-Bliley (GLB) Act.
- Credit unions have historically undertaken efforts to use SSNs only when needed and to protect this information when it is used. Prohibiting the use of SSNs at this time is not feasible, given their broad use as identifiers. Prohibiting the use of SSNs will only require the use of another method or numbering system for identifying individuals, which would also subject consumers to possible fraud should data security breaches occur.

### Discussion

The use of SSNs as a unique identifier has long facilitated information exchanges involving government agencies, including law enforcement, an



OFFICES: | WASHINGTON, D.C. | MADISON, WISCONSIN

has also proved beneficial to the private sector, which has adopted the use of SSNs for commercial transactions. For credit unions, SSNs have been used to verify the member's identity, which helps protect against fraud, and to associate the member with the various accounts that he or she maintains at the credit union.

Recent government mandates continue to perpetuate the need for financial institutions to use SSNs. These include the regulations implementing the USA PATRIOT Act, which require credit unions and other financial institutions to verify the identity of consumers who open new accounts. Additional rules administered by the Office of Foreign Assets Control and the Financial Crimes Enforcement Network also involve the use of SSNs, as well as rules administered by the Internal Revenue Service. SSNs are also necessary to access credit reports in order to determine creditworthiness.

Other government rules require financial institutions to protect sensitive information, such as SSNs. These include the guidelines for safeguarding consumer information that were required under the GLB Act. For these reasons, we do not support a prohibition on the use of SSNs to identify consumers. If, however, the FTC, based on its thorough analysis of empirical evidence, concludes that additional regulatory action is needed to safeguard the use of SSNs, we urge that the FTC and other government agencies provide an exemption for financial institutions as the rules under the GLB Act already address protection of SSNs in financial transactions.

We recognize that the use of SSNs has been an issue in the rapid growth of identity theft. In addition to searching through trash, stealing mail, and manipulating change of address procedures, identity thieves have been successful in using technology to perpetuate these crimes by breaching databases, phishing and other means. Identity thieves have been able to use SSNs and other information obtained in this manner to open accounts in the name of the victim and to commit other types of fraud.

For this reason, credit unions and the entire financial services industry have undertaken efforts to educate their members on how to protect themselves against identity theft. Credit unions caution their members to use SSNs only when necessary and to use current technologies and procedures to protect such information. This includes using sophisticated data protection measures, such as encryption, as well as additional means to verify the consumer's identity when he or she initiates a transaction.

Also, in October 2005, the financial institution regulators issued guidance requiring enhanced authentication for higher-risk transactions, which helped decrease reliance on SSNs as a sole means of authentication. To further limit or eliminate the use of SSNs as a means to identify consumers or authenticate

transactions may actually increase fraud, as SSNs have successfully been used to accurately identify and authenticate consumer transactions. The result could be increased lending costs, decreased loan approval rates, and increased instances of fraud and errors.

In addition to our other concerns, we believe that prohibiting the use of SSNs is simply not feasible at this time. SSNs serve a vital function with regard to identification due to their status as the only unique and nationwide individual identifier. There appears to be few alternatives at this time. For example, the consumer's name alone could never be used as an identifier since duplicate names are common, and names change due to marriage and divorce. Using both the consumer's name and address as an identifier would also be problematic due to address changes. A feasible alternative may be to require increased use of truncated SSNs, such as the last five or six digits, but any alternative must be thoroughly considered before it is required.

Also, prohibiting the use of SSNs will only require the use of another method or number for identifying individuals. This would impose a significant cost on businesses by requiring computer software changes and additional employee training. Unfortunately, there would be little, if any, corresponding benefit for consumers since any unique method or number system would render consumers vulnerable to fraud that would result from security breaches, whether it is based on SSNs or another numbering system.

We believe rather than prohibiting the use of SSNs, the government and the private sector should continue to work together to develop practical and reasonable approaches that will help shield SSNs from misuse while allowing the numbers to continue to be used to identify consumers in business and other transactions. For example, we would support efforts to explore the establishment of a verification program that will allow financial institutions to affirmatively verify a consumer's name, SSN, and date of birth.

Thank you for the opportunity to comment on these issues associated with the use of SSNs. If you or your staff have questions about our comments, please give Senior Vice President and Deputy General Counsel Mary Dunn or me a call at (202) 638-5777.

Sincerely,

Jeffrey Bloch  
Senior Assistant General Counsel