Missouri Credit Union Association

September 4, 2007

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

RE: SSNs In The Private Sector - Comment, Project No. P075414

Thank you for the opportunity to comment comments on the use of the social security number (SSN) in the private sector. The following comments are based upon the issues and concerns expressed by Missouri credit unions.

Preface
Limited use of SSN is good in theory. Any Personal Identification Number (PIN) or password developed in place of using the SSN inherits the same vulnerability to compromise. There are impediments to security including the inability to identify and penalize perpetrators, especially outside the United States. Therefore, the main focus should be to mitigate the risk of using the SSN.

Current Private Sector Collection and Uses of the SSN
Businesses and organizations collecting our social security numbers are extensive. Social security numbers are collected throughout most facets of our business and community infrastructures, including:

- Healthcare industries
- Financial institutions
- Private business endeavors
- Document storage companies – both paper and electronic
- Credit card issuing companies
- Credit reporting companies and services
- Libraries and schools
- Motor vehicle offices (which are not run by the state any longer and are an area where a consumer can register to vote, just like the public libraries).
- And governmental entities and public utilities.

The life cycle of social security numbers varies from industry to industry as a result of the various regulations imposed by the federal and state governmental agencies.

In the credit union industry, the social security number becomes a permanent record within the credit union on the membership/account card, as required by NCUA Rules and Regulations Part 749. NCUA is currently reviewing this regulation and hopefully will dramatically shorten this record keeping requirement. Perhaps the life of a SSN or any identifier is the length of time it continues to provide value, regardless of record retention issues. Retention for legitimate purposes, such as claims on dormant accounts, is warranted.

There is increased prominence in the use of our social security numbers as an identifier. The SSN is used in:

- Credit history and application scoring
- Employment
- Taxes
- Garnishments and levies
- Issuance of government ID and public utilities
- Pensions, SSA, Medicaid and other government benefits.
- Birth and death records in the US
- And every financial aspect of our American lives.

In the credit union industry, the SSN is required for all the above. Credit unions rely heavily upon the social security number as part of their Customer Identification Program required under the Bank Secrecy Act –Patriot Act and NCUA Rules and Regulation Part 748. Financial institutions have been using the SSN to report new account fraud to such companies as ChexSystems, using the SSN to pull credit reports in order to provide various credit services. Furthermore, credit unions use the social security number to report information back to the credit reporting agencies.

The Role of the SSN as an Authenticator

The SSN used as an authenticator must pass through our phone lines, the wireless world or some sort of computerized database. Regardless of what is used as an authenticator, the real issue does not lie in the "authentication item" whether it is the:

- SSN, although usually it is just the last four digits required.
- Assigned customer/member number, password, picture or combination thereof.
- Member/customer chosen number, password, picture or combination thereof.
- Biometrics and other items the consumer "has".
- Out of wallet questions.
- Or a combination of all of the above.

The only true authenticator is to use a combination of all of the above. The entity entrusted with this information must be held to the highest of standards by enforcement powers to mitigate stolen identity. The concern lies with the vast amount of data collected and stored data bases about each individual, and the potential breaches that may occur.

The protection of the SSN should lie in the security features used in retaining, storing, transferring, destroying, and sharing of this information, combined with punitive measures and enforcement powers.

The Role of the SSN in Fraud Prevention

The SSN was never intended to be used as a form of identification. Social security cards included statements to that affect. To rely on just one number to authenticate anything increases risk. A combination of identifiers, as suggested above, is more secure, but requires the individual to remember multiple pass codes, special words or numbers in order to prove their identity. This practice also causes consumers, in order to simplify the numbers necessary to remember, along with convenience, to write their PIN on the back of their ATM card. Regulation E has a section that protects the consumer who writes their personal identification number on the card, from any liability if it is used without their consent and they do not benefit from the transaction. This section certainly can parallel the effects of similar requirements for requiring multiple identifiers with the SSN as an identifier.

However, a combination of multiple identifiers is critical to consumer identity protection. Proper authentication is paramount to business to prevent financial loss as well as loss of reputation. The cost of multi-layer, multi-faceted authentication could be cost prohibitive to a small, limited services business, such as a smaller asset sized credit union. In assessing a solution careful consideration should be given to the cost of compliance and the burden it places on small businesses. The continued growth of micro-businesses should not be thwarted. Personal recognition of identity, supported by a long relationship, should also be a form of validation.

The Role of the SSN in Identity Theft

The problem is exacerbated when companies are permitted to know a variety of personal information about the consumer, such as their first car, mother's maiden name, best friend's name, first pet, etc. This information is transferred to more and more companies whose headquarters or service providers are on foreign soil, giving more opportunity to lose control over the use of this information. Consumer records and data are being shipped beyond our borders in a mere nanosecond. Globally, all countries must share in the responsibilities for the security of identification data.

As proper identification parameters are being determined, it would be appropriate to have the consumers' input in the authentication process, to minimize the invasion of privacy. When a consumer subscribes for a service or establishes an account, it would be appropriate for the consumer to determine the security questions they deem appropriate, not the merchant or financial institution. The level of authentication should be appropriate for the subjected risk.

Companies rely on those responsible for identifying the customer. Often times call center personnel are those assigned the task. These employees may be temporary, unskilled, or enticed to secure personal identification data. Data tracking and secondary systems must be in place to ensure data security.

Conclusion

Laws and regulations should be enacted to enforce penalties to agencies and businesses entrusted with responsibility for safeguarding identification data. However, the global community needs to be engaged and supportive. The substance of the information necessary to authenticate must be carefully considered to minimize consumer exposure, protect privacy, and mitigate the risk of misuse or identity theft.

Consumers worldwide deserve identities that are protected and that any business or agency responsible for negligence in data security be prosecuted to the full extent of the law.

Thank you for the opportunity to comment.

Sincerely,

Roshara J. Holub
President/CEO