1133 Connecticut Avenue NW
Suite 675
Washington, DC 20036

Jeffrey A. Tassey
Executive Director
Phone: 202-464-8815

COALITION TO IMPLEMENT THE FACT ACT

September 5, 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

To whom it may concern:

This comment letter is submitted by the Coalition for the Implementation of the FACT A the Federal Trade Commission's request for comment on the private sector use of social security lition represents a diverse group of industries and companies involved in all stages of the consun The Coalition is pleased that the FTC has requested such information, and we appreciate the opp ments.

Overall

The private sector use of SSNs arises as a result of governmental mandates as well as a d protect itself and consumers from the harms associated with misidentification of individuals. Th curacies in records, fraud, and even identity theft. Reliance on SSNs (usually with other informa sector entities to identify and authenticate individuals with more accuracy than such entities wou were denied to them. The importance of the SSN in this regard stems from the fact that it is the unchanging identifier used by individuals today. Although members of the Coalition strive to de cation and authentication tools, it is unlikely that reliance on SSNs could be eliminated without c vate sector significant costs and inconveniences.

Current Private Sector Collection and Uses of the SSN

Virtually all private sector entities collect and use SSNs if for no other reason that the go so for employment and tax purposes. There are a variety of additional governmental mandates a companies (such as many types of financial institutions) requiring the collection and use of SSNs terrorism, or even abandoned property law purposes.

Although there are many governmental mandates requiring the collection and use of SSN necessarily believe that such mandates drive the private sector's use of the SSN in every respect. stances in which a company would not collect or use an SSN but for governmental requirements rely on SSNs for a variety of purposes independent of any legal requirement.

A company may use the SSN generally for two purposes: identification and authenticatio tion, a company may use an SSN to assist in identifying a consumer for purposes of recordkeepi record. For example, it may not be sufficient to request the consumer report of "Don Smith" fro agency due to the plethora of "Don Smiths" on file. However, the likelihood of correctly identif creases significantly if the request also includes Don Smith's SSN. The SSN may also be used i individual's identity in a variety of ways. For example, an individual who cannot provide a valid cords with a particular name is likely to be considered a potential impostor. The same can be sai

from a consumer reporting agency due to the plethora of "Don Smiths" on file. However, the likelihood of correctly identifying the individual's file increases significantly if the request also includes Don Smith's SSN. The SSN may also be used in an effort to authenticate an individual's identity in a variety of ways. For example, an individual who cannot provide a valid SSN that matches other records with a particular name is likely to be considered a potential impostor. The same can be said of an individual who provides a facially invalid SSN, such as one with more or less than 9 digits or one that is on a deceased persons file. The SSN can be used to locate a variety of records as well, and the information obtained from those records (and the fact that use of the SSN appears to return the correct records) can be used to conclude whether the consumer is who he or she purports to be. More sophisticated companies can use software or services that use the SSN to detect potentially fraudulent patterns of use of a particular SSN. These are only a few representative examples of how SSNs can be used for identification and authentication, but they should provide a general understanding to the FTC.

The Coalition is unaware of alternatives to the SSN that are widely available. Indeed, it appears that Congress and administrative agencies agree with our conclusion given the number of federal and regulatory requirements pertaining to the collection and use of SSNs. The value of the SSN arises from the fact that no other universal and widely used identifier is unique or constant. It may be possible in the future that technology is developed that allows the private sector to rely on other information for purposes of identification and authentication, but such technology is not currently in wide use. It may also be that reliance on biometrics in the future alleviates the need for the collection and use of SSNs, but there are a variety of other issues that must be resolved before consumers would be comfortable with such a solution.

The FTC has specifically requested comment on state law restrictions on SSNs. In general, those laws that attempt to limit or eliminate the "public display" of SSNs have not had a significant impact on legitimate private sector uses of SSNs. On the other hand, at least one state has passed a law attempting to limit the "sale" of SSNs, and there are similar proposals perpetually floating around Congress. Unless implemented with extreme care, such prohibitions have the potential to disrupt the private sector's use of SSNs for identification and authentication purposes. The net result would be less accurate information about consumers in corporate files and increased fraud and identity theft. A prohibition on the "sale" of SSNs could destroy consumer reporting databases, anti-fraud databases, and the ability of financial institutions or others to integrate information from disparate sources into a single record. Given the number of identity theft laws on the books today, it is also not clear to us that there is a gap in existing law that needs to be addressed by these proposals.

The Role of the SSN as Authenticator and in Fraud Prevention

For the reasons described above, among others, the SSN can be a critical tool in authenticating an individual's identity. It is important to understand that the SSN *reduces* identity theft as a result. We note that the use of a victim's SSN as part of a fraudulent

credit application, for example, may result in fraud or identity theft, but that is only because the identity thief was able to defeat the creditor's anti-fraud program that may have included the SSN as one of several authentication factors. This begs the question of whether the victim would have been better protected if the SSN was not used in the first place by the creditor as part of the authentication process. The answer is that the creditor simply would have had less information to consider when making its decision to authenticate the consumer's identity. Rarely is it the case that the identity thief is successful only because he or she possesses the victim's SSN.

To date, the integrity of the SSN is sufficiently protected to allow it to be used as one of many identification and authentication factors available to the private sector. We are unaware of any piece of information that is so confidential and secure that a company need not obtain any other information to be confident in knowing that it has authenticated an individual. Furthermore, it is not necessary for information to be confidential in order for it to be of value. Few would dispute the value of a consumer's name in authenticating his or her identity. Yet, that name is certainly more widely available than an SSN. Of course, the more widely available the information is, the less valuable it is, which is why the SSN provides significant benefits over having only a name and address when authenticating identities.

The Role of the SSN in Identity Theft

The role of the SSN in identity theft is similar to the role of a victim's name or other information that may be used to open an account. The SSN does not necessarily provide an identity thief the "keys to the kingdom" in terms of being able to commit identity theft. However, because the SSN is a factor in many identification authentication programs, if an identity thief has the victim's SSN, the thief is more likely to succeed in his or her efforts than if the SSN is not available to the thief. But this exception should help prove the rule that the SSN is an additional protection against identity theft and fraud, not the cause of it.

The FTC has asked for comment on how identity thieves obtain SSNs. We are unaware of any particular method that is overwhelmingly favored over others. However, in many instances fraudulent use of SSNs involves "family or friend fraud" in which the impostor takes advantage of the proximity of the victim's confidential information and steals the SSN. An SSN could be obtained in certain other ways, such as by pretexting a consumer or a financial institution, literally stealing the SSN from a database, or by purchasing them in the black market.

State Law Issues

The FTC has specifically requested comment on the impact of state laws pertaining to SSNs. Generally speaking, state laws purporting to limit the public display of SSNs had a relatively minor impact on legitimate private sector companies, although there were some costs involved to ensure compliance. A few state laws, however, have had a much broader scope and could have a significant impact on the private sector. For example, a New York law would prevent disclosure of the SSN in certain circumstances, but the law includes an unnecessarily broad definition of "SSN" possibly to include truncated SSNs or other similar derivations. Another law in Minnesota has the potential to have an even greater impact regarding limitations on the "sale" of SSNs. This law is not scheduled to become effective until next year, but has the potential to significantly affect the ability to obtain SSNs from consumer reporting agencies (unless litigation demonstrates that the Fair Credit Reporting Act preempts it in this regard), to include SSNs in asset sales, or to obtain SSNs in connection with identity verification efforts through the use of third parties. The Coalition notes that there is also legislation in Congress regarding the purchase and sale of SSNs that could have catastrophic consequences.

Conclusion

The private sector collects and uses SSNs for a variety of reasons, but most notably to protect consumers and themselves against fraud. For better or worse, the SSN is the only unique, universal, and constant identifier available to the private sector (and to the public sector, for that matter), making it useful for purposes of identification and authentication. Any attempt to restrict or reduce the availability of SSNs for these and other legitimate purposes would have a negative impact on consumers and the private sector.

Thank you again for the opportunity to provide our comments on this important matter. Please do not hesitate to contact me at (202) 464-8815 if I may provide further information.

Sincerely,

Jeffrey A. Tassey