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 on behalf of the Consumer Bankers Association ("CBA") in response to the Federal Trade Commission's ("FTC") request for comment regarding the private sector use of social security numbers ("SSNs"). CBA is the recognized voice on retail banking issues in the nation's capital. CBA's member institutions are the leaders in consumer, auto, home equity and education finance, electronic retail delivery systems, privacy, fair lending, bank sales of investment products, small business services and community development. CBA was founded in 1919 to provide a progressive voice in the retail banking industry. CBA represents over 750 federally insured financial institutions that collectively hold more than 70% of all consumer credit held by federally insured depository institutions in the United States. Although CBA's members are generally regulated by one of the four federal banking agencies, CBA appreciates the opportunity to provide its comments to the FTC on this important issue.

Summary

Financial institutions collect and use SSNs for a variety of reasons. For example, in many cases, such collection and use is required by the federal government. Financial institutions also collect and use SSNs for identification and authentication purposes. Specifically, they use SSNs to assist in authenticating a consumer's identity, but also to ensure that they are able to request (or match) the correct information about the correct consumer (*e.g.*, in connection with requesting a consumer report). The reason the SSN plays such a critical role in customer identification and authentication is that the SSN is the only readily available unique, constant, and universal identification information for individuals.

In order for the SSN to retain its current usefulness in preventing fraud, it is critically important that all public and private sector entities possessing consumers' SSNs take reasonable measures to protect them. We note that financial institutions have significant obligations to implement comprehensive information security programs designed to protect all of their nonpublic personal information, including customers' SSNs. CBA's members are examined for compliance with this requirement, and we

believe the financial services industry as a whole has undertaken significant initiatives to protect SSNs as a prudent business practice and in a manner that complies with federal regulatory requirements. It is our hope that other industries would take similar precautions to protect the confidentiality of individuals' SSNs.

Although there has been criticism regarding the SSN and how it allegedly enables identity theft, we believe the opposite is generally true. An identity thief may in fact need the SSN to commit identity theft, just as the thief would need the victim's name and perhaps other identifying information. This does not necessarily mean that the SSN *causes* or *contributes to* identity theft. Rather, the SSN is but one of many tools that prevent identity theft because the SSN is one more piece of information, among many pieces of information, that a consumer must produce for identification and authentication purposes. Financial institutions' reliance on such an approach helps to ensure against fraud and identity theft even if an identity thief has one or more, but not all, of the necessary pieces of information to transact in another's name. In short, the SSN is no more a key to identity theft than the consumer's name, and neither by themselves are generally sufficient to commit identity theft. On the other hand, the inability to produce a valid SSN in connection with a request for identification strongly suggests that the individual is not who he or she purports to be.

1. Current Private Sector Collection and Uses of the SSN

- What businesses and organizations collect and use the SSN? For what specific purposes are they used?

We believe it would not be possible to provide an exhaustive list of the types of institutions that collect SSNs and the purposes for which they are used. However, CBA's member financial institutions collect and use the SSN for a variety of reasons, including to comply with federal law and to protect themselves and their customers from fraud. By collecting the SSN, a financial institution is given an additional piece of information it can use to authenticate potential or current customers. For example, if an applicant does not provide a name and SSN that matches a file at a consumer reporting agency, the financial institution may have reason to suspect potential fraud. It may also be that the SSN on an application does not appear to fall in a range of SSNs assigned to persons with the birth date provided, which could be another sign of potential fraud.

Aside from its value as an authenticator, the SSN is useful as an identification tool for financial institutions. In fact, the SSN may be the feature that is most critical in attempting to identify the correct file in an internal or external database as belonging to a specific individual. For example, a financial institution may have information about "Steve Robinson" that must be placed in the correct file. If the financial institution has several "Steve Robinsons," the financial institution can ensure that it places the information in the correct "Steve Robinson" file if both the information and the file have the SSN associated with them.

Like any other employer, financial institutions also collect SSNs in the employment context for purposes of complying with federal employment requirements, such as those relating to tax and immigration. The SSN may be used to assist in locating information for background investigations on employees as well.

- What is the life cycle (collection, use, transfer, storage and disposal) of the SSN within the businesses and organizations that use it?

There is no specific "life cycle" for the SSN or any other customer information held by a financial institution. Having said this, we believe it is important to recognize that financial institutions have obligations under federal and state law to have comprehensive customer information security programs designed to protect information such as customers' SSNs. CBA members are examined for their compliance with these federal requirements and corrective action and/or enforcement is taken when necessary. Many state law requirements and federal guidance from the federal banking agencies which require CBA members to notify individuals if certain information is breached also serve as a strong incentive to protect information securely or to dispose of it properly when it is no longer needed.

- Are governmental mandates driving the private sector's use of the SSN?

There are various government mandates that required the collection and use of the SSN, such as for tax reporting, customer identification programs required by the USA PATRIOT act, and employment purposes. CBA does not believe that governmental mandates are necessarily driving financial institutions' use of the SSN, if by "driving" the FTC means that financial institutions would not collect and use SSNs but for those mandates. We believe financial institutions would still likely rely on SSNs for at least some purposes, especially those pertaining to fraud and identity theft prevention and customer services, regardless of these federal laws.

- Are there alternatives to these uses of the SSN?

CBA is not aware of readily accessible alternatives to the SSN for purposes of identifying and authenticating consumers or their information. The SSN is the only widely used information that is unique to an individual, unchanging, and relied upon by a wide variety of companies and government entities. For example, a consumer's name or address is neither necessarily unique nor unchanging. An account number assigned by a financial institution may be both unique and unchanging, but such an account number is likely of limited use outside of that financial institution.

This is not to say that there are no alternatives to SSNs for identification and authentication purposes. Biometrics are an example of an alternative, as they are unique, unchanging, and could be recognized across companies and industries. Any such alternative, however, presents significant cost, social, and/or political obstacles to widespread adoption. CBA doubts, for example, that a requirement to collect and

transmit biometric information to the federal government for tax purposes would be politically acceptable now or in the near future.

- What has been the impact of state laws restricting the use of the SSN on the private sector's use of the SSN?

CBA does not believe that state laws restricting the private sector display of SSNs to the "general public" have had a significant impact on the ability of the private sector to use SSNs for legitimate purposes. Legitimate businesses neither make SSNs available to the general public, nor do they collect SSNs from private sector sources available to the general public.

We note, however, that some state laws have raised concerns. In New York, for example, the law pertaining to SSNs defines the SSN as not only the SSN itself, but any number derived from the SSN. The law provides that an encrypted SSN is not covered, however, begging the question of the distinction between a "derivative" of the SSN and an encrypted SSN. Regardless, this could include significantly truncated forms of the SSN which do not necessarily have the same value to identity thieves as the SSN itself. Another state, Minnesota, has recently adopted a law that broadly prohibits the "sale" of SSNs.[1] Restrictions on the "sale" of SSNs could have significantly negative effects on financial institutions and their customers. For example, such restrictions could make it difficult to sell consumer report or fraud prevention information if it includes the SSN (a key fraud fighting tool). Such restrictions could also prohibit the inclusion of SSNs in loan portfolios that are sold, making it very difficult for the purchasing financial institution to integrate the purchased accounts into its existing portfolio. These and other legitimate and beneficial transfers of SSNs could be affected by these laws.[2]

2. The Role of the SSN as an Authenticator

- The use of the SSN as an authenticator—as proof that consumers are who they say they are—is widely viewed as exacerbating the risk of identity theft. What are the circumstances in which the SSN is used as an authenticator?

While some may believe that SSNs "exacerbate" the risk of identity theft, we suspect that most individuals understand that the SSN is one of many factors used to prevent fraud and identify individuals properly. SSNs prevent fraud by requiring individuals to provide an additional piece of information that can be used by a financial institution to verify the consumers identity. The value of the SSN lies not in the number itself, but relying on it as part of a comprehensive authentication process. Banks rely on such a process to ensure that there is no "silver bullet" available to defeat their anti-fraud systems. The federal banking agencies also expect banks to have sufficient

[1] Similar federal laws are pending in Congress.

[2] For these and other reasons, if federal proposals pertaining to SSNs and the private sector advance, it would be critically important to have the appropriate expert agencies functionally regulate their respective industries' use of the SSNs such that unintended consequences are minimized.

authentication programs in place, including use of multi-factor authentication systems when appropriate.[3]

CBA cannot stress enough that the SSN *is just one piece* of an overall identification authorization puzzle. Other information, such as the consumer's name, current address, previous address, telephone number, birth date, or place of employment is also important for purposes of authentication. None of these pieces of information, by themselves, would necessarily serve to authenticate an individual's identity. When this information is considered on the whole, in conjunction with information obtained from internal or external sources, a financial institution can determine whether it has enough information to authenticate the consumer's identification. Therefore, although there is obvious value with respect to the SSN for fraud prevention purposes, a compromised SSN will not necessarily provide an identity thief with the key to an individual's identity.

Having touted the benefits of relying on multiple pieces of information or multiple factors for authentication, the SSN itself may also provide useful information for purposes of "negative" authentication. For example, it may be possible to rely on the SSN provided by an individual to suggest strongly that the individual's identity cannot be authenticated. For example, if a consumer provides an SSN that is matched against a deceased person list or a known fraud list, the financial institution may determine that the identity cannot be authenticated regardless of any other information provided at the time of application. The SSN could be used with other information for such "negative" authentication as well, such as if the SSN does not coincide with the SSN range applicable to people in the birth year given on the application, or if the name and SSN do not match on the internal or external databases consulted by the financial institution.

- Are SSNs so widely available that they should never be used as an authenticator?

SSNs are generally not widely available. For example, one could not simply call a bank, consumer reporting agency, or any other legitimate business for that matter and obtain anyone's SSN on request, no questions asked. Furthermore, as described above, some of the entities most likely to make significant use of SSNs—financial institutions—have implemented information security programs that are reasonably designed to protect against the unauthorized acquisition of customer SSNs and other customer information. CBA believes these efforts have generally been effective in preserving the general integrity of the SSN.

CBA members believe that the integrity of SSNs, on the whole, is such that they may be relied upon as one piece of information to be used in authenticating a consumer's identity. It is important to note that information may still be useful in authenticating an individual's identity even if such information were widely available. An individual's name, for example, is generally available but that person's name is still

[3] *See, e.g.,* "Authentication in an Internet Banking Environment" issued by the Federal Financial Institutions Examination Council, http://www.ffiec.gov/pdf/authentication_guidance.pdf.

useful when attempting to authenticate his or her identity. However, because a consumer's name may be widely available, a financial institution may need less widely available information (such as the SSN) to assist in its authentication efforts. This is the reason that financial institutions and others may rely on multiple pieces of information or factors for authentication when necessary.

- What are the costs or other challenges associated with eliminating the use of the SSN as an authenticator?

As we discussed above, there are no other readily available forms of unique, constant, and universal identification similar to the SSN. Therefore, if a financial institution could not obtain the SSN for purposes of authentication, it would be deprived of an effective tool to prevent identity theft. This is not to say that a financial institution could not rely on other authentication techniques, but such techniques are likely to be less effective than they would otherwise be if the financial institution could request and validate one more piece of information about the consumer (*i.e.*, the SSN).

3. The SSN as an Internal Identifier

- Some members of the private sector use the SSN as an internal identifier (*e.g.*, employee or customer number), but others no longer use the SSN for that purpose. What have been the costs for private sector entities that have moved away from using the SSN as an internal identifier? What challenges have these entities faced in substituting another identifier for the SSN? How long have such transitions taken? Do those entities still use the SSN to communicate with other private sector entities and government about their customers or members?

Financial institutions have used "internal identifiers" in the form of account numbers for years when working with consumers. However, for the reasons discussed above, these do not replace SSNs in any meaningful sense. Among those financial institutions that have relied upon SSNs as internal identifiers for other purposes, such as employment or even as an internal customer tracker across multiple accounts, it is our understanding that efforts to "move away" from SSNs have not been cost free. Such changes require the reprogramming of software and the retraining of employees to use such software. One large financial institution has reported to us that its internal transition to employee numbers other than SSNs *took four years* given the number of external and internal systems affected. Furthermore, these changes have limited utility as consumers may not be able to provide customer service representatives with such assigned numbers or accounts, but they can provide their SSN. The net result of these efforts is that the SSN may not be relied upon as widely internally. However, because financial institutions must collect and use SSNs for purposes of regulatory compliance, government reporting, consumer reporting and loan underwriting, account integration (including with respect to historical files that may not have a newly assigned number), etc., it is not possible for a financial institution to eliminate its reliance on the SSN altogether.

- For entities that have not moved away from using the SSN as an internal identifier, what are the barriers to doing so?

In light of the fact that a financial institution cannot avoid collecting and using SSNs for a variety of legitimate and beneficial purposes, the financial institution may question the benefits of incurring significant costs and compliance burdens for relatively little change in its reliance on SSNs on the whole.

4. The Role of SSNs in Fraud Prevention

- Many segments of the private sector use the SSN for fraud prevention, or, in other words, to prevent identity theft. How is the SSN used in fraud prevention?

Please see our responses above for illustrative examples of how the SSN is used in fraud prevention.

- Are alternatives to the SSN available for this purpose? Are those alternatives as effective as using the SSN?

Please see our responses above for a discussion of whether there are readily available alternatives to the SSN for identity authentication purposes.

- If the use of the SSN by other sectors of the economy were limited or restricted, what would the ramifications be for fraud prevention?

The ability of a financial institution to depend on the SSN as one tool among many in fighting identity theft is dependent on the financial institution being able to access databases created by others, with information furnished by others, to assess the validity of the individual's identity. Therefore, if businesses other than financial services companies were unable to access or use SSNs, such databases would be less robust and therefore less effective at protecting consumers against identity theft. For example, if a landlord could not use SSNs, it obviously could not report SSNs to a consumer reporting agency. Consumers whose only financial or other interactions were with such types of entities may not have a file with a consumer reporting agency as a result, making it difficult for a financial institution to obtain the consumer's consumer report for authentication purposes.

5. The Role of the SSN in Identity Theft

- How do identity thieves obtain SSNs?

Identity thieves can obtain SSNs by reviewing records of family, roommates, or others with whom they have close contact or to whose records they have access. They can also obtain them through pretext calling, phishing, malware, spyware, or database

intrusions. It is our understanding that there is also a "black market" for SSNs via the Internet and other mechanisms.

- Which private sector uses of the SSN do thieves exploit to obtain SSNs, *i.e.*, SSN as identifier or SSN as an authenticator? Which of those uses are most vulnerable to identity thieves?

Thieves may exploit either or both types of uses of SSNs. It is not clear to us whether one use is more or less vulnerable than another.

- Once thieves obtain SSNs, how do they use them to commit identity theft? What types of identity theft are thieves able to commit with the SSN? Do thieves need other information in conjunction with the SSN to commit identity theft? If so, what other kinds of information must they have?

An impostor can use the SSN, with other information, to attempt to defeat a financial institution's fraud protection program. In other words, the thief may be able to provide enough information, such as a name with a valid address, SSN, and any other information requested on the application to satisfy the financial institution that the identity is valid and that there are no "red flags" suggesting possible fraud. Generally, this could occur in connection with the opening of a new account or "hijacking" an existing account.

- Where alternatives to the SSN are available, what kind of identity theft risks do they present, if any?

Please see our responses above regarding alternatives to the SSN.

Again, CBA appreciates the opportunity to provide these comments to the FTC. Please do not hesitate to contact me if we may be of further assistance.

Very truly yours,

Marcia Z. Sullivan
Vice President
Director, Government Relations