September 5, 2007

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

RE: SSNs in the Private Sector – Comment, Project No. P075414

Dear Sir or Madam,

The Mortgage Bankers Association (MBA)[1] appreciates the opportunity to respond the Federal Trade Commission's (FTC) request for comments regarding the private sector use of Social Security Numbers (SSNs in the Private Sector – Comment, Project No. P075414). Balancing the needs of obtaining accurate information and preserving consumer privacy is an issue of constant concern in the mortgage industry. In addition to specific questions posed in the request for comment, MBA would like to give a general overview of what role the SSN and regulations regarding its use have played in the mortgage industry.

The SSN plays a critical role in the mortgage lending process as it is the only unique and permanent identifier that crosses over from business to business and across industries as well. In the financial services sector, the SSN helps connect an individual to accounts, credit reports, public records, tax reports and other documents. This functionality is crucial to the real estate finance industry. Being able to associate a single person with these records and accounts not only allows the lender to authenticate that a potential borrower is who he represents to be, but permits the lender to make informed underwriting decisions. The distinctive nature of the SSN allows lenders to effectively and efficiently connect information from such industries and sectors as financial services, health care, education and government to a specific customer. The SSN also aids lenders in correctly reporting information they collect to borrowers, credit repositories and government agencies.

As our economy moves towards electronic and other remote forms of commerce, consumers enjoy the option of increased competition, greater efficiency and lower costs. It will also significantly increase the flow of information across business and industry lines. This trend emphasizes how critical the private sector's ability to successfully correlate consumer

[1] MBA is the national association representing the real estate finance industry, an industry that employs more than 500,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets; to expand homeownership and extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 3,000 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, Wall Street conduits, life insurance companies and others in the mortgage lending field.

information with the right consumer is to an efficient economy. To ensure that transactions are performed with limited risk to either the business or the consumer, it is increasingly important that lenders have the ability to authenticate not only the identity of consumer, but to validate that consumer's financial profile. Due to its ubiquity, the SSN remains the primary facilitator for identification and authentication. The SSN's uniqueness, permanence and acceptance by government, business and the public for these and other functions remains a key impediment to eliminating its use by the private sector.

The rapid expansion of electronic commerce has, unfortunately, been accompanied by increased fraud and abuse. Public concern with the protection of sensitive personal information, such as the SSN, has grown considerably in recent years, and state and federal regulators have responded to that concern by enacting a number of rules regarding not only the protection of such data but the notification of any affected individuals if that information is compromised. In addition to these regulations, the mortgage industry has taken a number of steps to reduce the potential exposure of personal information to unauthorized individuals. These steps have included limiting employee access, increasing encryption methods and developing alternative methods of validation, where possible, to limit the possibility of sensitive information falling into the hands of unauthorized third parties.

A mortgage lender, depending on how it is organized, faces a variety of regulations regarding sensitive personal information. Legislation, including the Bank Secrecy Act, FACT Act, Sarbanes-Oxley, USA PATRIOT Act and Gramm-Leach-Bliley Act (GLBA), as well as state laws, has created a number of mandates that affect the transmission, maintenance and protection of personal information. Mortgage lenders, depending on what products are offered, face additional requirements from such institutions as Fannie Mae, Freddie Mac and the Federal Housing Administration (FHA), which all have their own policies regarding quality controls that commonly involve personal information. Any consideration of further limiting or regulating the use of SSNs should be made in the context of these existing requirements.

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?

The mortgage lending industry collects and uses SSN for a variety of purposes, including:

- Identify and authenticate customers;
- Validate information collected from customers;
- Access customers' credit reports to establish creditworthiness;
- Comply with existing legal requirements, such as "Know Your Customer" Bank Secrecy Act and Anti-Money Laundering compliance, including Suspicious Activity Report (SAR) requirements;
- Conduct quality control programs after a loan is funded;
- Prevent mortgage fraud;
- Report information to the Internal Revenue Services (IRS) for tax purposes, such as borrower interest paid, mortgage insurance paid, loan officer and broker compensation, and the forgiveness or abandonment of debt;
- Report loan payment activity to credit repositories;
- Obtain veterans' eligibility for loan guarantees based on military records through the Department of Veterans Affairs;

- Process FHA-insured loans through FHA Connection;
- Transmit loan information to secondary market loan investors for potential bulk purchase or securitization and fulfill investor reporting requirements; and
- Conduct non-industry specific business activities (administer employee payroll and benefits, conduct background checks on potential employees and perform due diligence on potential business partners, such as mortgage brokers).

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

SSNs are generally provided by the consumer to a lender during the loan application process. Once collected, SSNs are used to authenticate a customer's identity and to validate the information a customer provides, such as employment status, income and asset profile. It, or a truncated version, is commonly also used as an identifier and authenticator to access information once an account is established. When a loan or its servicing rights are sold, the purchasing entity will receive all relevant loan information, including SSN. The SSN is used by the purchasing entity as part of its due diligence practices, in many cases revalidating the information received by the loan originator. Throughout the life of the loan, regardless of who holds it, the SSN is used in conjunction with payment history reporting to the credit repositories, tax reporting to the IRS and compliance with any applicable regulation.

Typically, mortgage lenders retain loan files, which include SSNs, from the time of origination in accordance with all applicable state and federal record retention requirements. The records of those loans paid in full are generally retained for a period of the later of five years from the date of closing or two years past the date the loan is paid in full, though some states require that loan records be retained for a period of up to five years past the date the loan is paid in full. Records relating to loan applications that are either rejected or declined must also be retained for a period of time varying from 25 months past the date of decision to five years, again depending on applicable state law.

Most records are retained in paper form. Some documentation is also retained electronically and can be reproduced in the event that a paper copy of a specific document cannot be located in the file. Typically, a company employs a third party to hold all archived documents until the retention cycle is completed. At that time documents are destroyed in accordance with that company's approved guidelines.

Are governmental mandates driving these uses of the SSN?

There are a number of governmental mandates governing the use of SSNs. For example, lending institutions with Suspicious Activity Report (SAR) obligations must include the SSN connected with a suspicious transaction. Section 326 of the USA PATRIOT ACT establishes consumer identification requirements for individuals establishing new accounts. Specifically, covered institutions are, with limited exceptions, prohibited from opening accounts for customers who do not have a SSN or taxpayer identification number. Additionally, IRS regulations require including the taxpayer's full SSN on relevant IRS forms to the Service and related Payee Statements to the taxpayer. Mortgage servicers are required to file Forms 1098 and 1099 with the IRS, advising the Service of such things as interest paid by the borrower on a mortgage and interest paid by the servicer to the borrower on escrow accounts maintained by the servicer.

There are also governmental mandates governing the storage and protection of sensitive personal information, including the SSN. The Interagency Guidelines Establishing Information Security Standards, issued under Title V of GLBA, prescribes information security system standards for financial institutions regarding the access, collection, storage, use, transmission or protection of customer information, including SSNs.

Are there alternatives to these uses of the SSN?

The universal use of SSNs across industries and all levels of government make developing alternatives to the SSN a challenge, particularly in those instances when the SSN is a unifying element connecting relevant information from disparate sources. Furthermore, the SSN's status as a permanent, unique identifying characteristic makes it even more valuable when relocation, marriage and remarriage, and additional life events alter other identifying characteristics. The SSN also allows confusion arising from inconsistent recording (such as the use of initials or suffixes) to be resolved simply and efficiently.

One alternative is curtailing the use of the SSN for transactions or inquiries that pose decreased risk to both the consumer and institution. Many institutions, either through automated interactive voice responses systems or live operators, only require consumers to provide a truncated version of the SSN to access such information as loan balance or payment due date. It is also common practice in these instances that data systems will only display the truncated SSN to customer service representatives, further limiting the risk of exposure. Similarly, institutions have begun displaying truncated SSNs on physical or electronic documents delivered to consumers or other parties, except where full numbers are required, such as IRS forms. One alternative the Commission may wish to consider is permitting the use of truncated SSNs on Payee Statements and other government-mandated documents.

SSN truncation may be unsuitable for more complex transactions that, if fraudulent, could do material harm to both the consumer and institution. Other alternatives include implementing unique personal identification numbers in lieu of SSNs or the development of biometric security standards. However, the challenges are considerable. Feasibility can be affected by such factors as cost, available technology and the ability of those alternative systems to interface across business and industry lines. Most important, however, is consumer acceptance of these alternatives. If the public views an alternative as overly complicated or insufficiently secure, it will weaken consumer trust in the financial system.

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

Many states have followed the lead of California, which enacted a law restricting the display of SSNs in 2002. Under that law, companies are no longer allowed to:

- Post or publicly display SSNs;
- Print SSNs on identification cards or badges;
- Require people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted;
- Require people to log onto a Web site using an SSN without a password; or
- Print SSNs on anything mailed to a customer unless required by law or the document is a form or application.

California provided sufficient lead time and guidance to companies to prevent a burdensome compliance process. However, as other states began to pass legislation with similar aims, new problems arose. These laws lack standard definitions, making compliance difficult for those companies that operate in different states and, thus, under different regulatory standards. Some state laws impose new rules, procedures or restrictions for accessing public records that contain SSN and other sensitive information. These laws may require institutions to undertake a more manual review process than was previously required for hiring decisions and underwriting decisions.

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?

In the most direct sense, many lenders use the SSN, or a truncated version, as an authenticator when customers contact their lender with inquiries. The SSN is also a powerful tool in helping banks authenticate information borrowers provide about themselves that has a material impact on the decision to extend credit. Not only is the SSN used to authenticate that potential borrowers are who they say are – a SSN is routinely run against databases to ensure it is not associated with known frauds, deceased individuals or AML screening lists – it assists lenders in authenticating that potential borrowers' financial profiles support underwriting a mortgage. Using the SSN, lending institutions can search consumer reports, licensing databases of regulators and even contact prior employer or firms represented to gather more facts to be used in authenticating the identity of an applicant.

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

The universal use of the SSN makes completely eliminating its use as an authenticator extremely difficult. However, lending institutions recognize that the SSN's ubiquity, and the efforts of determined identity thieves, significantly weakens its use as a *sole* authenticator. Many institutions, in accordance with recent guidance published by the Federal Financial Institutions Examination Council (FFIEC), have begun implementing multi-factor authentication systems in an internet banking environment in response to pervasive criminal attempts to gain access to and conduct fraudulent transactions via consumer accounts. These systems rely not only on something the customer (or identity thief) knows, such as the SSN, but something the consumer has (a specific IP address or home phone, for example) or something the consumer is (biometric factors).

It is also important to note that existing government mandates drive the use of the SSN as authenticator, such as in Customer Identification Programs required under section 326 of the USA PATRIOT ACT. Whether institutions are attempting to authenticate the identity of, and information provided by, new customers or authenticate the identity of existing customers, the SSN, when used properly in conjunction with other authentication methods, continues to provide a critical tool in allowing lending institutions to establish that individuals are who the represent themselves to be.

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

The greatest challenge would be the development of alternatives that receive the necessary level of public acceptance to be viable. Many institutions report that though customers commonly have difficulty recalling a PIN or account number, there is not nearly as much difficulty remembering the SSN. Transferability is another challenge. A loan is commonly sold from one entity to another, often multiple times, over its life. If the SSN is completely eliminated as an authenticator, whatever replacement system is established by, say, the loan originator, may not be compatible with whatever authentication controls are employed by entities that hold the loan later in the life cycle. As a result, a customer may need three or four different PINs (or whatever form the authentication system takes) over the life of the loan. This could lead to considerable confusion and frustration among consumers.

Eliminating the SSN as an authenticator would pose significant challenges to lending institutions that have long-established systems predicated on the SSN's use. The cost could easily reach into the hundreds of thousands of dollars per company depending on how many systems are impacted. A company would need to develop a new way to authenticate users that has many of the same characteristics of the SSN – permanence and uniqueness – and develop systems to integrate not only this new system but that of other industry participants, as business practices necessitate. Other identifying technologies, including biometrics, have shown accurate results but are both costly to implements and potentially seen by consumers as overly intrusive.

3. The SSN as 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?

When large lending institutions migrated from using the SSN as the primary employee identifier, virtually all internal processing systems needed to be updated. Internal controls for each of these systems require identification of the person conducting the update and/or transaction, and thus had to be adjusted to the new identifier. One large member institution reported that the transition for employee numbers took more than four years to be fully completed, given the number of internal and external systems that were affected. A particular challenge has been employee and customer acceptance. Customers and employees may not know or may not remember the account or other internal number, resulting in frustration and aggravation at the individual level.

However, these transitions toward employee and account numbers not associated with SSNs do not eliminate the need to adequately capture, validate, and use the SSN for other legitimate purposes, such as back office operations related to employee records or additional identification and authentication methods for customers. Internal identifiers have little value when communicating with outside entities, whether other businesses or the government, who do not share identifier systems. The use of the SSN as an identifying characteristic continues to offer benefits to both the consumer and institution that could be compromised if it is completely eliminated. For example, relying solely on entity-generated identifiers may hamper credit reporting agencies' ability to correctly associate credit files with consumers. Not only would the lender be forced make underwriting decisions based on incomplete information, but a borrower

may not be able to qualify for the best product available because the credit score does reflect the borrower's complete credit history.

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

As previously noted, existing government mandates, including IRS reporting requirements, drive institutions to internally associate accounts with a particular SSN so that all necessary information can be efficiently associated with the proper account and reported to correct individual or entity.

4. The Role of the SSN 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?

Many of the processes lenders undertake to authenticate both the identity of a borrower and the information a borrower provides go hand in hand with lenders' efforts to prevent mortgage fraud. To that end, the SSN plays a critical role in protecting both lending institutions and innocent consumers from fraudulent transactions. Checking records associated with a particular SSN can raise inconsistencies during the application process that can uncover the possibility of an individual's SSN being used by someone else to access or open a line of credit. Once an account is established, the SSN, in conjunction with other authentication methods, can limit access to sensitive account information to only those with a right to that information.

The SSN also plays an important role in protecting institutions from funding loan applications that fraudsters have no intention of repaying. The SSN can be compared to Social Security Administration-published High Group and Death Master Lists to ensure that the SSN is in fact valid and held by a living individual. SSNs are regularly run against exiting fraud databases. Lenders use SSNs to validate employment status, income and existing assets, all of which have a significant impact on a lender's decision to extend credit, and all of which, unfortunately, lenders commonly see either fabricated or embellished. To illustrate the point, Fannie Mae's Mortgage Fraud Update published in July, 2007, noted that misrepresentations involving these three loan characteristics (income, employment and assets), constituted almost half of all misrepresentations uncovered on loans delivered to Fannie Mae in 2005 and 2006. The use of SSNs to authenticate third parties, such as mortgage brokers, can prevent a lender from acting on information fraudulently transmitted by an individual posing as a legitimate business partner.

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

In many of these instances, the SSN remains one of the most powerful tools to ensure the integrity of a loan transaction. As a unique, permanent identifier, used across industry lines in both the private and public sector, it is indispensable as lenders work to associate all necessary information in order to not only make a decision regarding the extension of credit, but to make such a decision based on reliable information. Mortgage fraud can be indicated by other loan characteristics, but work best when used in conjunction with the SSN.

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

Reducing the use of the SSN where it is not necessary for a transaction's security and integrity would limit the SSN's exposure to theft and misuse. Even restricting the use of the SSN to a truncated form in some instances would significantly mitigate the risk of identity theft, as the last four digits cannot be used to leverage existing accounts or establish new ones. However, limiting use of the SSN, either during initial collection or in subsequent transmissions between business partners, could significantly compromise efforts by all sectors of the financial services industry to limit and combat fraud. A key component of those efforts is the proper association of relevant information to the correct individual or transaction. The SSN's universal use across industries and sectors allows lenders to not only authenticate that a customer is how he says he is, but that other vital information, including employment, income and residence, is factual.

5. The Role of the SSN in Identity Theft

How do identity thieves obtain SSNs?

Lenders have encountered a number of techniques used by identity thieves, both online and offline. Offline, thieves can obtain SSN through "dumpster diving" – sorting through trash looking for valuable material on customers that have not been properly disposed. Thieves have also intercepted mail containing documents with sensitive information such as SSNs. SSNs can also be obtained and misused by persons known to the individual, such as family, friends or by persons with access to a consumer's personal account information. Online, thieves can simply purchase SSNs that are collected through data breaches of varying scales, "phishing" or spyware.

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

Physical transmission of the SSN, such as through the mail, either to or from the customer may be the easiest to exploit, In addition to the SSN, an identity thieve could use mail theft to gain access to additional identifying characteristics such as name and address, as well as additional information specific to the account. Due to state laws and companies' internal information security programs, the SSN has been removed on many documents delivered to consumers including pay statements, bank statements, and health care communications. Where the SSN must be included, it often appears in truncated (last four digit) form.

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?

Identity thieves commonly use a stolen SSN to steal the identity of an existing individual. For the mortgage industry, the problem most often presents itself in the form of an individual attempting to open and access credit using the identity and credit profile of another individual. Many lenders have instituted controls to limit the damage a stolen SSN can do to both the affected consumer and lender. These include the multi-factor authentication systems described

above. Lenders also commonly require some other form of identification that has also likely been verified, such as a utility bill or government issued photo identification.

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

Alternatives to the SSN exist, but present significant challenges to identity theft. Biometrics, for example, provides a stable and valid method of uniquely identifying an individual. However, significant concerns regarding privacy, such as who would maintain biometric information, and implementation cost have impeded the widespread adoption of biometrics as a replacement of the SSN. If biometric data is compromised, the risk of identity theft could potentially be greater than that posed by a compromised SSN. Other account numbers can replace the SSN as a unique custom identifier, but to the extent that such numbers become universally used across industry and sector lines, those new numbers will likely become equally at risk to theft and abuse as the existing SSN.

MBA greatly appreciates the opportunity to provide these comments. Please contact Kevin Finnerty, Senior Specialist of Government Affairs, at (202) 557-2815 if you have any additional questions.

Sincerely,

John Robbins, CMB
Chairman