National Retail Federation
The Voice of Retail Worldwide

September 5, 2007

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

RE: SSN in the Private Sector – Comments, Project No. PO75414

To Whom It May Concern:

On behalf of the National Retail Federation (NRF), we would like to take the opportunity presented by the Federal Trade Commission ("The Commission") as part of the ongoing Identity Theft Task Force to submit comments on the importance of the private sector's use of Social Security Numbers ("SSNs"). As you may know, NRF is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet, independent stores, chain restaurants, drug stores and grocery stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.6 million U.S. retail establishments, more than 24 million employees - about one in five American workers - and 2006 sales of $4.7 trillion.

Among our membership the use of SSNs is a very important part of day to day operations. SSNs are used in hiring associates, doing business with contractors, and the administration of benefits for current employees and retirees. SSNs are used extensively in credit granting operations to help authenticate the identity of a customer and to appropriately score that customer's credit application. SSNs are also used in ways that one might not expect, such as to submit tax information to the IRS on behalf of a customer who has won a sweepstakes or for those customers who have to submit Medicare or Medicaid claims for prosthetics or other medical equipment sold in retail stores. In many circumstances SSNs are collected to comply with current laws such as U.S. immigration laws, the USA PATRIOT Act, or any activity that triggers 1099 reporting to the Internal Revenue Sevice ("IRS"). While there are many legitimate uses of SSNs, retailers also recognize the importance of protecting this information from misuse by securing documents and data that might contain this sensitive information.

Liberty Place
325 7th Street NW, Suite 1100
Washington, DC 20004
800.NRF.HOW2 (800.673.4692)
202.783.7971 fax 202.737.2849
www.nrf.com

Among the many uses of the SSN, the use as the authenticator is particularly important in the context of both hiring and credit granting. As you may be aware, the Department of Homeland Security ("DHS") has recently highlighted the utility and importance of using SSNs to authenticate the identity of employees in its new "SSN No Match" rule. This rule, originally intended to be implemented on September 4, 2007, would require employers to further investigate and even terminate employees whose name and SSN do not match. While the purpose of this new regulation is to discourage the hiring of illegal aliens and to ferret out those individuals who are posing as legal members of the workforce, the practical effect is that DHS will be relying on the SSN as the primary authentication tool for the entire workforce.

In matters of credit granting the SSN is also a very important authentication tool. Many retailers offer "instant" credit at point of sale and this type of transaction relies on the ability to both authenticate and approve a credit application in a matter of minutes. At point of sale, only a consumer's personal identifiers such as name, SSN, address and telephone number can differentiate them from all other candidates for credit. Out of each of these elements, it is the SSN that is the most widely available element that is unique to the individual (short of biometrics which are not readily available or widely accepted by consumers). Individuals can have the same name, address and phone number, but, if the system is working correctly, only one person can have any particular SSN. Once this type of authentication is achieved it then becomes possible for those same individuals to be reliably scored for credit worthiness and ultimately extended credit. This is clearly a huge consumer benefit.

Fraud prevention is a key benefit of the ability to accurately authenticate the identity of customers, employees and contractors. To the extent that SSNs are a critical part of determining the actual identity of an individual, they are equally important in fraud prevention as well. Accurate authentication can prevent a whole host of fraudulent behavior, from the opening of new credit accounts in someone else's name (identity theft) to preventing payroll or employee benefits fraud. SSNs are also important in retail loss prevention efforts because perpetrators are required to give their SSN on police reports and other court documents. SNNs are also regularly used by businesses to keep track of liens and judgments, as well as ensuring proper administration of garnishment orders, or the withholding of child support obligations from the correct employees. Again, since there is no other universally recognized and accepted "unique identifier," SSNs remain critical in preventing fraud and carrying out many socially beneficial activities.

The SSN is also used extensively as an internal identifier for the administration of employee payroll and benefits. DHS, the IRS, and state departments of taxation all require the use of SSN on documents such as the W2 and I-9 forms filled out by new hires and on forms used in the administration of

tax benefits such as flexible spending accounts, child care, health savings accounts, and pre-tax commuter programs. The SSN is also important in the administration of health benefits (again to prevent fraud and comply with other government mandates) and the tracking of retirees. As you know, birth and death events are recorded by the Social Security Administration and employers rely on that same data in administering to their employees and their employees' families for purposes of worker's compensation, life insurance benefits, and pension plans (for example, by positively identifying beneficiaries).

While it is true that a clever identity thief can do significant damage to a consumer's credit standing if they obtain an SSN, they generally can only do that damage if they are also able to mimic the consumer in other ways as well -- such as learning the victim's name, date of birth, address, telephone number, and mother's maiden name. Having established the numbers and encouraged their widespread adoption and use, government should be careful not now to "throw the baby out with the bathwater" in an attempt to protect against the relatively less frequent incidence of identity crimes. As we have described above, there are many important processes that rely on a universally accepted unique identifier. Today that identifier is the SSN. And while some privacy advocates may be happy to eliminate the common use of the SSN, it will surely be replaced by some other tool or identifier (biometric or otherwise) because it will ***have to be***. Those same advocates will be just as unhappy with the use of a replacement "SSN" as they are with today's practices. Unfortunately, we no longer live in a small town society and individuals in today's more mobile world can only be accurately identified by their personally identifiable information ("PII). The most unique and most universally accepted of all PII is the SSN. The challenge then is to protect sensitive PII and put practices into effect that will help cut down on data misuse and fraud. Ironically, one of the best ways to protect consumers is to authenticate their identity using data -- and again we come back to the basic utility of the SSN. It is simply a lynchpin in the information economy.

Respectfully Submitted,

Mallory Duncan
Senior Vice President and General Counsel
The National Retail Federation

Elizabeth Oesterle
Vice President, Government Relations Counsel
The National Retail Federation