



September 4, 2007

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

**RE: Social Security Numbers within the Private Sector
Project No. P075414**

To Whom It May Concern:

HSBC Finance Corporation ¹ ("HSBC") is pleased to submit this letter in response to the Federal Trade Commission's request for comment concerning our organization's use of social security numbers. HSBC is a part of one of the largest financial services organizations in the world, serving over 125 million customers on six continents. In the United States and Canada, HSBC's businesses provide financial products to nearly 60 million customers.

HSBC supports the President's Identity Theft Task Force effort to combat identity theft, as well as the FTC's role in overseeing such effort. HSBC recognizes that consumers who are victims of identity theft suffer direct harm, including delay or inability to receive credit, out-of-pocket financial losses, inconvenience, and related losses. Identity theft also has a large financial impact on the U.S. economy, which absorbs billions of dollars of fraud losses each year. This directly impacts lenders, such as HSBC, which incur significant losses in resolving identity theft events, and expend institutional resources to attempt to prevent identity fraud.

Similar to many other financial institutions, HSBC utilizes consumers' social security numbers in order to conduct its various financial service businesses. Social security numbers are an integral part of the origination and management of any credit extension underwritten by HSBC. The social security number has evolved into a common individual identifier used by the financial services and credit reporting industries as a means to ensure that customer relationships within an organization and credit experiences across the industry can be accurately tied to a particular consumer, in order to appropriately assess that consumer's credit capacity and to appropriately manage the institution's credit risk.

If new regulations were to prohibit or significantly restrict the use of social security numbers in this capacity, there would still remain a need for some kind of common identification system. Any replacement common identification number would soon become subject to the same risks and concerns that are associated with social security numbers today. Privacy regulation for financial institutions has appropriately focused on the safeguarding of social security numbers as sensitive customer data. Certainly HSBC and other financial institutions should continue to examine their uses of social security numbers in order to ensure that these uses continue to be appropriate and necessary, and in compliance with regulations with respect to the safeguarding of sensitive customer data. We believe that the focus of identity theft prevention regulation should continue to be based on the safeguarding and protection of sensitive information, not the attempted elimination of it.

A number of state legislatures have enacted, or attempted to enact, local regulations surrounding the use and protection of social security numbers. Where states have enacted such legislation, most have prohibited:

- (1) Public posting or display of a social security number;
- (2) Printing a social security number on any card required to access products or services;
- (3) Printing a social security number on a receipt;
- (4) Requiring an individual to transmit a social security number over the Internet, unless the connection is secure or social security number is encrypted;
- (5) Requiring a social security number to access a web site, unless a password or unique PIN or other authentication device is also required to access the web site; or
- (6) Printing a social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed.

These regulations are intended to reasonably limit access to social security number information. These prohibitions are reasonable and, coupled with Gramm Leach Bliley and current information security guidelines, they work to provide adequate protections to consumers with regard to the data that financial institutions use and manage. HSBC urges the FTC to consider appropriate and reasonable rules or guidelines governing access to social security numbers in a way that preserves the ability of financial institutions to wisely use social security numbers to conduct their business, manage credit risk, and continue to prevent identity theft.

Similar to other financial institutions, HSBC currently uses social security numbers in the following important ways:

I. Customer Identification and Account Origination, Management and Reporting

Social security numbers are an important data element used by HSBC to comply with federal legislation aimed at the vital objectives of fighting terrorism and detecting and preventing money laundering. HSBC uses social security numbers to comply with the requirements of the USA Patriot Act and the Bank Secrecy Act. The USA Patriot Act requires financial institutions to verify the identity of individuals seeking to conduct financial transactions with the institution. Although other data elements are also used to identify a consumer, the social security number is an important piece of identifying information. In particular, the consumer's social security number can be essential in order to distinguish among individuals with similar names or addresses, or to eliminate "false positive" matches.

To meet Currency Transaction Report (CTR) requirements under the Bank Secrecy Act, financial institutions must provide a customer's identification number on the CTR (Form 104, formerly Form 4789). Consumers typically provide their social security number as their "Taxpayer Identification Number" for federal reporting purposes (although a separate "Taxpayer Identification Number" may be used for CTR reporting). In addition, there are multiple mandatory IRS reporting provisions which require use of a social security number in order to comply.

HSBC also obtains social security numbers on its credit applications to confirm with a credit reporting agency (CRA) that the applicant meets (or continues to meet) credit underwriting requirements. During the term of a loan, HSBC uses a social security number in other interactions with CRAs, as well, including (1) to obtain updated consumer report information (where permitted) in order to determine whether a customer continues to meet underwriting standards, and (2) to report its own transactional experience with a consumer to CRAs. In both cases, the use of the consumer's social security number significantly improves the ability of the CRA to identify the correct consumer report to furnish or to update. The use of social security numbers, therefore, helps to guaranty the integrity and functionality of the credit reporting system.

In connection with the purchase and sale of portfolio loan accounts (including mortgages, auto loans, credit card accounts etc.), financial institutions provide account information, including the social security numbers of the underlying debtors, so that the purchaser can conduct its due diligence. After the portfolio sale is consummated, the purchaser will need to obtain and use the social security number, along with other pertinent account information, in order to continue to report the account to the CRAs accurately and for verification purposes.

II. Fraud Control

The consumer's social security number is a critical tool in the task of fraud prevention and fraud investigation. HSBC uses social security numbers, along with other consumer information, in order to detect fraud by comparing such information to the information maintained in CRA databases, public records information, and other databases, many of which are maintained specifically for fraud prevention and control. For example, investigators might be able to use a social security number in order to discover that a consumer never resided at the address listed on a consumer application. Significantly, fraud investigators may be able to use such databases, along with social security numbers, in order to locate contact information about the fraud perpetrator and/or the victim of fraud. If such database providers were required to eliminate social security numbers from their databases, many instances of fraud would never be detected, and many consumers who are victims of fraud would not learn about the fraud, possibly until a much later time. Early detection of financial fraud, including identity theft, is critical in order to avoid additional losses.

Consumers benefit from the use of social security numbers in fraud control in other ways. Financial institutions may provide information about identity theft (including the relevant social security numbers) to specialist third party firms in order to assist their customers who have been victims of identity theft, at the financial institutions' expense. These third parties will assist consumers to place fraud alerts, obtain credit reports for review, contact other financial institutions, and otherwise take steps to clear the identity theft.

III. Customer Verification and Account Look-up

Social security numbers or portions of social security numbers (such as the last four digits) are the primary form of verification for consumers calling in for live or automated customer service (which is voice- or touchtone-activated). HSBC's customer service units utilize social security numbers in the resolution and processing of consumer complaints, disputes, bankruptcy, and death notices, and to aid in credit collections.

Social security numbers are a secondary form of information used internally to locate accounts when an account number is not available. Numerous internal information technology systems which house customer data are built with special functionality to enable social security number "look up," which serves significant purposes. For example, one information technology system is used to look up accounts by social security number in order to distinguish between multiple accounts with the same name, perform account servicing or research, identify historical and purged accounts, identify accounts across business units, and conduct enhanced due diligence with respect to fraud and Bank Secrecy Act processes.

Conclusion

HSBC recognizes the problem of identity theft within the United States, and appreciates this opportunity to provide comment to assist in working toward solutions. The social security number is a key form of identifying information which financial institutions must obtain to verify its customers. Further, the social security number serves many legitimate purposes in the underwriting and management of financial accounts, including fraud prevention functions, which result in the protection of both financial institution and consumer interests. Efforts to prevent identity theft should continue to focus on data security measures. Restrictions on the appropriate and necessary uses of the social security number (as described in this letter) would adversely impact the ability of HSBC and other financial institutions to effectively and wisely conduct business, consistent with safe and sound financial institution management principles.

Again, HSBC appreciates this opportunity to comment on the FTC's request.

Sincerely,

Jéffrey B. Wood
General Counsel, Insurance Services

¹ Among other companies, HSBC Finance Corporation wholly owns HSBC Auto Finance Inc., HSBC Consumer Lending (USA) Inc., Beneficial Company LLC, HSBC Mortgage Services Inc., HSBC Card Services Inc., HSBC Bank Nevada, N.A., and HFC Company LLC.