AMERICAN BANKERS ASSOCIATION

1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

World-Class Solutions, Leadership & Advocacy Since 1875

Doug Johnson
Senior Policy Advisor
Government Relations
Phone: 202-663-5059
Fax: 202-828-4548
djohnson@aba.com

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:

The American Bankers Association (ABA) appreciates the opportunity to provide the Federal Trade Commission (FTC), and the other federal agencies involved in the Identity Theft Task Force (Task Force) the following comments on the private sector's use of social security numbers (SSNs). ABA, on behalf of the more than two million men and women who work in the nation's banks, brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks – makes ABA the largest banking trade association in the country.

In its strategic plan for combating identity theft, the Task Force recommended that a comprehensive record on SSN uses be developed, and that these uses be evaluated for their necessity. According to the plan, it is the intention of the Task Force to make recommendations to the President in the first quarter of 2008 as to whether additional specific steps should be taken.

Many current uses of SSNs are of great benefit to consumers. The use of SSNs to deter identity theft is well established, as are the benefits of its use to facilitate commerce. As the FTC has noted in the agency's own testimony, "Ultimately, the objective of any SSN restrictions should be to reduce unnecessary transfer or use of SSNs, without inadvertently burdening necessary transfers or uses."[1]

ABA believes that the FTC's approach to SSN restrictions, and any recommendations made to the President for additional legislative or regulatory steps, should be guided by the desire to maintain this balance between reducing unnecessary SSN transfers or uses and inadvertently burdening necessary and appropriate ones. Any recommendations should also take into account the substantial safeguards that financial institutions have in place to protect SSNs and other sensitive customer information. Limiting the ability of financial institutions to use SSNs for many necessary measures to deter fraud and for legitimate business purposes would raise significant regulatory and operational problems for banks and for their customers.

[1] Prepared Statement of Joel Winston on behalf of the FTC before the Subcommittee on Social Security of the House Committee on Ways and Means, June 21, 2007.

If legislation, regulations, or guidance relating to the banking industry are a result of the recommendations, these should be developed in coordination with and administered through the federal bank regulatory agencies. These agencies should also have exclusive rulemaking and enforcement authority with regard to banking institutions so that these institutions' unique role in facilitating transactions and fighting identity theft is properly addressed.

Current Private Sector Collection and Uses of the SSN

FTC testimony has also noted that "…identity theft must be attacked on other fronts, as well, from improving data security to keep sensitive information out of the hands of criminals, to educating consumers to better protect their information, to developing more effective means of authenticating consumers so that criminals who do obtain sensitive information cannot use it to open new accounts or access existing ones."[2]

Any evaluation of private sector collection and use of the SSN must take into account the substantial safeguards that financial institutions have in place to protect SSNs and other sensitive customer information. The banking industry has a long history of taking a multi-front approach to the problem of identity theft. It is in the industry's best interest, on behalf of its customers and to limit its losses due to fraud, to combat identity theft.

Banks have significant regulatory requirements to safeguard SSNs. The Gramm-Leach-Bliley Act, Section 501(b) (GLBA) requires banks to safeguard customer information properly and have information security programs approved by their boards. The federal financial institution regulatory agencies (the agencies), through the Federal Financial Institutions Examination Council, have issued guidance implementing these requirements, and the agencies regularly examine financial institutions to insure compliance. The requirement to safeguard customer information and have an information security program in place covers all personally identifiable information, including SSNs. Financial institutions are also responsible for evaluating safeguarding practices of their vendors and other third parties.

In addition to implementing the general requirement to safeguard customer information, the agencies have also issued additional guidance regarding implementing stronger authentication measures, vendor management, transport of sensitive information, and the reporting of information security breaches. GLBA and the extensive regulatory guidance as a result of GLBA, the Fair Credit Reporting Act (FCRA), and the amendments to FCRA under the Fair and Accurate Credit Transaction Act all serve to protect the security of customer information in banks, other financial institutions, and credit reporting agencies (CRAs).

According to the Government Accountability Office, "[w]hile privacy concerns should not be discounted, it is important to note that the use of SSNs to link individuals to information about them enhances the administration of federal and state programs, makes credit more accessible to consumers, and allows medical care to be integrated across providers and insurers."[3]

---

[2] Prepared Statement of Joel Winston, June 21, 2007.
[3] Letter from Barbara Bovbjerg on behalf of the GAO to the Honorable E. Clay Shaw, Jr., July 7, 2000.

SSNs are collected and used by all segments of the financial services industry – by banks, licensed lenders, mortgage companies, insurance companies and broker-dealers. Such financial entities can be affiliated with each other under a holding company structure or have entered into third-party service and other agreements with each other in order to provide the full range of financial services their customers demand. The ability to link these accounts together, in diversified large financial institutions as well as community banks, is vital, as customers have an expectation that their full account relationship will be available to any representative of the financial institution they are communicating with. Moreover, without this means of linking the accounts of the same customer, the risk of confused identities and confused account records would be increased, with the attendant hardships for customers and the banks who serve them.

Banks collect SSNs of customers and of other persons related to a customer account, such as account beneficiaries, custodians, guardians, trustees, guarantors, grantees, cosigners and any insured. In many instances the initial collection is driven by some form of government obligation or mandate, most notably for tax reporting, employment purposes, or customer identification under the USA PATRIOT Act. The collection of the SSN at account opening allows the bank to evaluate the consumer for credit, insurance or other services, to record the consumer's transactions properly, and to fulfill the financial institution's legal obligations.

Banks often employ service providers to maintain and service their customer's accounts, including, for example, providing call-center customer service and payment processing. In order to allow service providers to perform these important back-office functions banks must provide such entities with access to customer information, including the use of SSNs to avoid misidentification or confusion of customer accounts and records, particularly records emanating from a variety of sources. Without SSNs, these back-office functions cannot normally be performed within the low tolerance for errors that customers and financial regulators would allow and that banks as businesses would find acceptable.

Banks also often act as custodians for these accounts and are required to make reports to federal and state government authorities regarding activity in these accounts, in much the same way an employer would provide administration for employee benefit plans. For example, banks must be able to transfer an account to a new provider if the account holder decides to transact business elsewhere, or if the bank needs to use a third-party locator service to track down a lost account owner.

In the employment context, SSNs are collected for full-time employees, agents, temporary workers, consultants, and family members who participate in employee benefit programs. SSNs are also collected from third parties, such as agents representing a financial institution or its customers. Banks receive SSNs from CRAs in conjunction with account monitoring, collections, and offers of credit. In addition, they receive SSNs in their capacity as a service provider for other companies and government entities – for example, when managing a retirement plan program, servicing a mortgage portfolio of another company or conducting brokerage clearing services for a third party.

The difficulties in devising legislation that protects SSNs while not adversely impacting the many legitimate SSN uses is evident in pending federal legislation, such as the "Social Security Number Privacy and Identity Theft Prevention Act of 2007" (H.R. 3046). This act would substantially limit the ability of financial institutions to use SSNs for many necessary and legitimate business purposes. H.R. 3046 would prohibit all sales and purchases of SSNs, except where an exception applies. Moreover, terms such as "sell" and "purchase" are

broadly defined. As a result, H.R. 3046 can be read to prohibit the sale or purchase of any product or service if the transaction involves a SSN and an exchange of value between the parties. That would cut a wide swath through the legitimate and important uses of SSNs today.

The legislative model presented by H.R. 3046, whereby legitimate uses of SSNs are presented as exceptions, is unworkable for the banking industry and its customers. There is simply no effective means to devise a comprehensive set of exceptions, a futile exercise that paves the way for legitimate and even necessary SSN uses to be called into question when they are not specified in the legislation and frustrating innovation that may rely upon the use of SSNs to provide valuable new services to customers.

Just as pending federal legislation would pose significant problems for banks and bank customers, if enacted, there are a variety of existing state laws that create unnecessary roadblocks to legitimate uses of the SSN. New York, for instance, prohibits the disclosure of SSNs or any number "derived from such number," which can be construed to include truncated SSNs. At the same time, other states *recommend* that truncated SSNs be used, especially in the context of public records, creating inconsistencies between the states.

Additionally, Minnesota has enacted a law that broadly restricts the "sale" of SSNs. This law, just like H.R. 3046, could restrict the ability of banks to use important anti-fraud tools. For example, when a financial institution uses a third-party, anti-fraud tool to confirm a consumer's identity or to determine the fraud risk associated with entering into a transaction, the financial institution's transaction with the third party will involve the consumer's SSN and an exchange of value between the financial institution and the third party (which could be construed as a "sale"). If construed as a sale, the transaction could violate such a state or federal standard.

In addition, financial institutions frequently sell consumer loans and other assets on the secondary market. As part of a loan sale, the seller will provide the buyer with the underlying loan documentation, which normally will include the consumer's SSN for tax and related purposes, such as to facilitate credit checks. While it is possible to create exceptions for these kinds of sales, it is difficult to envision every instance where such an exception would be necessary.

ABA strongly recommends that the FTC, and the other agencies involved in making legislative recommendations as a part of the Task Force, acknowledge the substantial efforts underway at financial institutions to protect all sensitive customer information, including SSNs. It is in the best interest of banks not to depend on SSNs when viable alternatives are available. It is not in the best interest of our industry, or its customers, to place restrictions on SSN use that preclude its use where necessary or where valuable to the customer.

The Role of the SSN as an Authenticator

The SSN, at this point and into the foreseeable future, is a pertinent piece of the customer authentication process. Eliminating the use of the SSN as an authenticator could have a significant, adverse impact on financial institution customers.

Banks cannot rely solely upon name, address and phone number combinations for authentication, as our nation's population is highly mobile and may use alternative last names, addresses and phone numbers. Names are not unique, and addresses and phone

numbers change too frequently to be reliable authenticators. Even these *combinations* are not unique and often bring together unrelated individuals, such as in large apartment buildings or where mail is sent to business addresses. They may also bring together different generations within a household.

The FTC, in its request for comment, states that 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. While there are certainly instances where this is true, it is also true that there are circumstances where customers need access to their accounts or to provide the bank with information regarding their accounts (for example, a stolen wallet) and only have their SSN as their initial means to identify themselves. A key is a reliable but imperfect means of frustrating auto theft. When the key is stolen, the car can be easily stolen, but statistics clearly show that locked cars are far less likely to be stolen than unlocked cars. Keys are still valuable tools to frustrate thieves, and the same is true for SSNs.

When a SSN needs to be used for authentication purposes, compensating controls can be instituted including asking for additional factors such as passwords, PINs (personal identification numbers), challenge questions, identification of the originating device, and personal picture selections. Even in these instances, the SSN is often a vital component of the full authentication process.

Indeed, additional authentication methods and controls, in conjunction with the use of the SSN as a universal identifier, are increasingly being used to identify bank customers. Other universal identifiers, such as finger prints, facial scans or other biometrics, cannot be used in many settings, such as during telephone communications, and many have not achieved a level of customer acceptance whereby they can be broadly deployed.

Additional authentication mechanisms and compensating controls will ultimately become more mature and more universally accepted by the bank customer over time. Yet one constant will remain. A unique universal identifier will be needed, and nothing has been devised or is anticipated that is so universally accepted—by financial institution and customer alike—making it indispensable as one of a series of tools to ensure that customers gain swift and sure access to their financial accounts, particularly in times of stress or theft.

The SSN as an Internal Identifier

As stated in recent Government Accountability Office testimony, SSNs play an important role in our economy. With 300 million American consumers, many of whom share the same name, the SSN is a key identification tool for businesses, government, and educational institutions, and others.[4]

Tens of thousands of Americans share the same name. Many people who share the same name also share other identifying information, such as the city and state of residence or the month and year of birth. Unlike other identifying information, such as name, address and marital status, an individual's SSN does not change over that individual's life, and no other living person shares that number. As a result, the SSN is the most cost-effective, accurate, and efficient piece of information available for businesses to identify and to link various information to consumers.

[4] General Accounting Office, *Private Sector Entities Routinely Obtain and Use SSNs and Laws Limit the Disclosure of This Information* (GAO 04-11), January 2004.

Generations ago, when consumers lived, worked and shopped locally, their good name in the community enabled them to obtain credit, insurance, employment and other services. With today's more transient population and with the advent of national markets due to the Internet and other improvements in communication, the vast majority of financial businesses obtain and use SSNs to identify consumers for legitimate and necessary purposes frequently transacted in other than a face-to-face setting.

Many banks are moving toward internal identifiers, creating their own customer identification numbers. However, these are usually for the bank's own purposes, sometimes even limited to the use of only one affiliate or another of a bank; there remain many circumstances when only a SSN can be used to match diverse customer records. SSNs still must be maintained as part of the customer record for tax reporting and USA PARTRIOT Act customer identification program purposes. SSNs are also used to determine whether a customer of an acquired bank already has other relationships with the acquiring bank—very important for deposit insurance and other account integration purposes. SSNs are not only important for authentication purposes, they are also generally used in linking new product relationships to already existing products owned by the same customer, and in providing the service customers expect, especially when a customer request involves multiple accounts, either within the same bank or among its subsidiaries and affiliates.

The Role of the SSN in Fraud Prevention

ABA is concerned that counterproductive limitations on the use of SSNs, which today are employed effectively by banks to combat identity theft and fraud, could actually lead to increased identity theft by impeding our industry's preventive efforts. SSNs are invaluable in our fight against identity theft and fraud, and restrictions on its use could prohibit financial institutions from using a variety of existing anti-fraud tools. Much like consumer report databases, anti-fraud tools are based on the SSN as the only practical identifier that can be used to link consumers to information about them. These anti-fraud databases are much more extensive than those at credit reporting agencies and have proven to be particularly useful during the account-opening process, where a significant amount of identity theft is attempted. These systems have also been identified as an important means to keep terrorists and money launderers from gaining access to the payment system.

Verifying the SSN of a potential bank customer (such as verifying that the SSN holder has not been reported deceased via the Social Security Administration's (SSA's) Death Master File), is an important part of the account-opening process. Of increasing importance, as well, is the SSA's Consent Based Social Security Number Verification (CBSV) process. Under CBSV, the SSA has provided limited fee-based SSN verification to private businesses that obtain a valid, signed consent form from the SSN holder. The ABA applauds CBSV as the first phase of the SSA's long-term strategy to provide the business community with a high-volume/real-time verification process, and believes that general expansion of this program is needed to enhance the banking industry's ability to combat identity theft, fight fraud, and facilitate compliance with the USA PATRIOT Act.

The GAO recently testified before Congress that processing disaster assistance registrations over the Internet deterred the use of obviously false names and SSNs, and we would

envision similar positive results from an online CBSV process.[5] Developing CBSV as a user-friendly, Internet-based application could greatly enhance the efficiency and effectiveness of the process. ABA, in its CBSV comment letter, recommended that the SSA work quickly to develop a real-time, commercially-ready program that will meet the needs of the agency, participating organizations, and consumers.[6]

The SSN is also crucial in detecting and deterring insider fraud. Insider fraud compromises customer data and, according to the Federal Deposit Insurance Corporation, has in recent years made up more than half of all bank fraud and embezzlement cases closed by the Federal Bureau of Investigation.[7] To counter this threat, financial institutions are developing more sophisticated means to share internal fraud records in databases. These databases allow financial institutions to determine if potential employment candidates have compromised consumer information and/or knowingly caused financial losses at another institution and were fired for cause. The SSN is the only practical identifier for these databases, particularly for people who would prefer to obscure their past fraudulent actions.

The Role of the SSN in Identity Theft

Identity theft is a serious problem, and the banking industry is committed to deterring such theft and assisting customers in its aftermath. There is some evidence that our efforts are working. Recent research reveals that the number of adult victims in our nation declined by a million between 2003 and 2006. This report, by Javelin Strategy and Research, also revealed that almost half of all identity fraud is perpetrated by friends, neighbors, in-home employees, family members or relatives.[8]

Many of the ways that identity thieves obtain SSNs are quite conventional, given that almost half of all perpetrators (in cases where the nature of the theft was known) were known by the victim. Others are more sophisticated, such as phishing or the use of malware, but occur as a result of the victims unknowingly giving their SSNs to the thief.

Some conventional means, such as mail theft, can compromise a SSN if the number is on an account statement (which is discouraged by the banking industry). Internal Revenue Service (IRS) regulations, however, penalize companies, including banks, for masking or truncating an individual's SSN or tax identification number in communication mailed to the taxpayer. Not permitting SSN masking or truncating on such documents creates an ideal opportunity for identity thieves to intercept mailings. ABA has requested that the IRS revise its regulations to allow masking and truncation in order to protect taxpayers from identity theft. In the letter, the ABA noted that the significant risk associated with the full display of a borrower's SSN on documents mailed to the borrower by a payor (as required by IRS regulations) clearly outweighs the benefit (if any) of such practice to the government. Therefore, we recommended that payors, trusts and partnerships continue to include full SSN and TIN on returns and forms filed with the IRS but be allowed to truncate the

[5] Testimony of Gregory D. Kutz before the Senate Committee on Homeland Security and Governmental Affairs, GAO-06-403-T, February 13, 2006.
[6] American Bankers Association comment letter, *Social Security Administration Consent Based Social Security Number Verification Process,* February 28, 2006.
[7] FDIC, *Risk Management Manual of Examination Policies,* April 2005.
[8] Javelin Strategy and Research, *Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses,* September 2006.

numbers in a manner that would protect taxpayers in the copies of such documents that are provided to the recipient taxpayer. [9]

More sophisticated means, such as electronic intrusions and hacking, are more common on personal, home computers than in a banking host environment. While every business must protect itself from such intrusions, the banking industry has been particularly vigilant. We have to be. Criminals are relentlessly seeking to break into bank data systems. A Financial Crimes Enforcement Network (FinCEN) study of Suspicious Activity Report (SAR) filings regarding computer intrusions found that, from 2003-2005, no hacking attempts on bank customer information file servers reported to FinCEN were successful, indicating the high level of bank-hosted server security. The phishing of customer computers was the most common manner of bank account compromise reported via a SAR during the period.[10]

Given the success of phishing and malware (particularly key loggers) in a home computing environment, identity theft risks would continue to be present even if an alternative were substituted for SSNs. Using an alternative to SSNs would decrease verification certainty, while increasing verification costs. The use of alternatives would also create cumbersome identification procedures for customers since they would have to recall numerous identifiers rather than a single number. It would not eliminate the criminal interest in discovering and exploiting the new identifier. Since the use of SSNs for the many necessary and legitimate purposes is not going be eliminated in the foreseeable future, any alternative would be used in addition to, as opposed to in lieu of, the SSN.

Conclusion

ABA welcomes the opportunity to continue to work with the FTC and the other agencies involved in the task force to craft recommendations that take into account the complex operations of financial institutions and the many and evolving needs of our customers.

Efforts to restrict the use of SSNs by the private sector are well-intended and make sense if carefully undertaken. As with antibiotics, unnecessary use can compromise the value of the instrument. But the need for caution should not be translated into a need for prohibition. Any effort to restrict SSN use must not interfere with identity verification, anti-fraud, anti-money laundering and anti-terrorist financing efforts, as well as normal business operations that allow financial institutions to meet the needs of customers and the financial markets.

Sincerely,

Doug Johnson
Senior Policy Advisor
American Bankers Association

---

[9] American Bankers Association, *Request for Guidance Regarding Masking of Social Security Numbers and Taxpayer Identification Numbers on Documents Mailed to Taxpayers*, February 12, 2007.
[10] FinCEN, *The SAR Activity Review, Trends, Tips, and Issues, Issue 9*, October 2005.