

THE FINANCIAL SERVICES ROUNDTABLE



BITS

FINANCIAL SERVICES
R O U N D T A B L E

ITAC

IDENTITY THEFT ASSISTANCE CENTER

1001 PENNSYLVANIA AVE., NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
TEL 202-289-4322
FAX 202-628-2507

E-Mail info@fsround.org
www.fsround.org

September 5, 2007

To: Federal Trade Commission/Office of the Secretary
Via Web site: <https://secure.commentworks.com/ftc-SSNPrivateSector>
Room H-135 (Annex K)
600 Pennsylvania Ave., NW
Washington, DC 20580

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

Dear Sir/Madam:

The Financial Services Roundtable (“Roundtable”), including BITS and the Identity Theft Assistance Center (“ITAC”), appreciate the opportunity to comment on the Federal Trade Commission’s (“FTC”) request for public input on private sector uses of Social Security numbers (“SSNs”).¹ The following are general comments and specific responses to each of the questions in the FTC’s public comment request.

We expect that any FTC initiative relating to the financial services industry will be undertaken in conjunction with our primary banking regulators. Consequently, we are simultaneously sending copies of our comment letter to the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, and the Office of Thrift Supervision, respectively.

General Comments

Federal, state and local governments have taken steps to protect the unauthorized use of SSNs.

Public concern over the protection of sensitive information has increased in recent years in response to media reports, mandatory security breach notification, and the availability of information that could be used to perpetrate fraud and identity theft. Many states have enacted laws in recent years to address concerns over data security, breach notification requirements, privacy protection, and use of sensitive information such as SSNs. Additionally, the Administration’s Identity Theft Task Force released a report

¹ The Roundtable is a national association that represents 100 of the largest integrated financial services companies providing banking, insurance, investment products, and other financial services to American consumers. Roundtable member companies provide fuel for America's economic engine, accounting directly for \$65.8 trillion in managed assets, \$1 trillion in revenue, and 2.4 million jobs. BITS is a division of the Roundtable, leveraging intellectual capital to address issues at the intersection of financial services, operations and technology. BITS focuses on strategic issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. ITAC is an affiliate of the Roundtable dedicated to fighting identity theft through victim assistance, research and law enforcement partnerships. ITAC has helped more than 20,000 consumers restore their financial identities and is the leading source of verified data on identity theft crime.

in April 2007 that includes a number of helpful recommendations, including support for a uniform national standard for breach notification, endorsement of risk-based approaches and strategies to render lost or stolen data useless by identity thieves, and greater involvement by law enforcement in investigating and prosecuting identity theft crimes. The report also appropriately acknowledges the need for financial institutions and law enforcement to use SSNs for identification and verification.

Financial institutions are regulated and actively supervised by federal and state regulators.

Financial institutions must adhere to specific federal and state requirements to identify customers using SSNs and protect sensitive information, such as SSNs. For example, the USA PATRIOT Act requires financial institutions to establish customer identification programs. In addition, the Interagency Guidelines Establishing Information Security Standards, which implements Title V of the Gramm-Leach-Bliley Act (“GLBA”), require financial institutions to establish appropriate safeguards for the use, disclosure, privacy, and security of personal information, including SSNs. Federal and state financial regulators regularly examine institutions for compliance and take enforcement action against institutions that do not comply.

GLBA safeguard requirements should be extended to other industries.

Given that many other industries use, store, and process personal information such as SSNs, we *recommend* that risk-based safeguard requirements similar to those contained in the GLBA information safeguards requirements extend to other industries so that a uniform, national standard exists across all industries. It would be appropriate for federal legislation to allow the financial services industry to remain under the regulatory framework in place today.

Financial institutions continually enhance their processes and procedures on SSN use.

In addition to these regulatory requirements, financial institutions continually enhance their processes or procedures to protect customers’ information. Financial institutions have a strong history of protecting customer information, deploying broadly accepted authentication methods, applying other security controls to detect and prevent fraudulent activities, and educating customers on how to protect their information and prevent identity theft.

In addition to eliminating SSN use where possible, financial institutions have:

1. limited access to stored and processed SSNs to only a small subset of necessary employees;
2. created higher levels of background checks and ongoing activity monitoring for selected employees and third party vendors or servicers;
3. redacted or masked full SSNs in applications and displays (e.g., only displaying the last 4 digits for call center representatives to use as an authentication factor);
4. transformed or "scrambled" data in test environments so that genuine data may not be associated with individuals; and
5. encrypted databases containing SSN information, where appropriate.

Federal, state and local governments should work with legitimate businesses to balance the use of the SSN for legitimate business purposes with consumer protection.

Notwithstanding these important efforts to limit use of SSNs and their exposure, SSNs continue to serve a vital business, consumer, compliance, and governmental function because they have special status as the

only unique, permanent, universal individual identifier. Although there are some alternatives to using an SSN as a primary authenticator and identifier, the elimination of the SSN, particularly as an identifier, would adversely impact financial institutions and customers. Alternatives to SSNs may actually produce the same risks currently associated with SSNs. Therefore, we *urge* federal, state, and local governments to educate individuals on how to protect their SSNs, work with legitimate businesses to develop workable solutions to protect SSNs and avoid unintended consequences associated with unreasonably restricting the use of SSNs, particularly in the customer identification and verification.

Responses to FTC Questions

1. Current Private Sector Collection and Uses of the SSN

Why do businesses and organizations collect and use the SSN?

SSNs have a special status as the only unique, permanent, universal individual identifier. For this reason, SSNs are collected and used by almost all segments of the financial services industry, including banks, licensed lenders, mortgage companies, insurance companies, and broker-dealers. SSNs are collected for both customer and employment purposes.

For what specific purposes are they used?

Financial institutions collect and use SSNs for the following purposes:

- a. Legal Requirements - To comply with various federal and state laws and regulations, including the USA PATRIOT Act, tax reporting requirements, the Federal Reserve Board's Regulation O relating to verification of loans to executive officers, directors, and principle shareholders of member banks, and GLBA requirements.
- b. Fraud Prevention and Detection - For internal and industry-wide fraud prevention programs and coordination with law enforcement. (More information is included below in our response to the questions on use of SSNs for fraud prevention.)
- c. Identification, Authorization, and Verification in the context of:
 - i. Customer Service: Customers may identify themselves with their SSN and/or ask financial institutions to locate accounts using their SSN.
 - ii. Account Verification: Even when a financial institution has established an alternative to an SSN for customer access, there are instances where SSNs are necessary to resolve problems that cross legal entities or to ensure that access is restricted to only those accounts the customer has a right to view. SSNs are crucial to ensure that the client is linked to the correct accounts; failure to accurately link accounts with the right customer has the potential to become an information security breach incident, which may trigger mandatory notification.
 - iii. Marketing and Marketing Analysis: SSNs may be used to match records and avoid duplication when compiling information from various sources or to perform marketing analyses of customers with multiple accounts. A redacted SSN may be used in connection with marketing materials to distinguish the person to whom the offer is directed from other family members who may have

similar names. SSNs also can be used to recognize customer opt-in/opt-out requests when the customer provides an SSN and no other account information.

iv. Account Processing/Servicing/Collections to:

- Obtain information from credit reporting agencies and financial background checks of applicants/customers;
- Interpret the behavior of customers with multiple relationships with the financial institution;
- Respond to communications received by the Internal Revenue Service (“IRS”) or other government agencies (e.g., state abandoned property administrations, in response to garnishment orders, subpoenas, court orders and discovery requests);
- Refund premiums to Military Allotment Accounts;
- Protect a financial institution (e.g., when filing a proof of claim in bankruptcy court, facilitating collections activities);
- Administer abandoned property, which only can be done with an SSN (this applies to all business sectors, including, but not limited to, financial institutions, securities firms, mortgage companies, insurance companies, retail industry, hospitals, hotels, utilities, oil/gas, court and government agencies);
- Effectuate a customer transaction (e.g., payment to a college in connection with a student loan, payment to an appraiser in connection with a mortgage loan);
- Provide a service to or obtain a service from a third party or a government entity (e.g., administer a retirement plan program, service a mortgage portfolio of another company, conduct brokerage clearing services for a third party);
- Communicate with the Medical Information Bureau and other insurance support and service organizations;
- Synthesize information relating to a particular customer that has been collected from various third party sources (such as government agencies); and
- Maintain and test information technology systems.

d. Human Resources: Employers use SSNs to obtain background and credit checks on employees, consultants, or agents; to match information relating to a particular employee that has been collected from various third party sources such as government agencies; to administer retirement and health benefits; and to provide information to functional regulators such as the SEC, the Financial Industry Regulatory Authority (“FINRA”), and state insurance agencies relating to agent/broker registrations, satisfaction of educational requirements, disciplinary actions and terminations.

e. Audit and Examination: Regulators, when performing exams, request financial institutions provide SSNs in order to effectively select or access customer records for an audit. Similarly, internal and external compliance and audit staff may need SSNs to select or access customer records.

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

The following provides an overview of how financial institutions collect, access, disclose, protect, store, and destroy SSNs.

- a. SSN Collection – There are multiple ways in which an SSN may be collected, such as on applications (both paper and on-line), from credit reporting agencies for pre-screened offers, or from affiliates, where an account meets criteria for an offer from the receiving affiliate.

The industry continually evaluates the data it collects from job applicants, employees and consumers during account opening, loan origination, and other transactions to determine the need for and use of the data collected. Financial institutions have a vested interest in ensuring that they collect only necessary information and retain only information for which there is a continuing business need or statutory or regulatory obligation.

- b. SSN Access – The SSN is kept in active files while the relationship between the individual continues, as it is frequently needed in servicing or processing the relationship (as described above). Additionally, the financial services industry restricts employee access to the minimum necessary level of sensitive information required to perform their job functions. For example, if an account or loan is closed, employees who once required access to sensitive customer data while the relationship was open may no longer have a business need for such information. Thus, their access to this information may be restricted.
- c. Disclosure and Use of SSNs – Financial institutions routinely evaluate whether SSNs must be disclosed to accomplish any specific task. Financial institutions review the types of data that they provide both internally and externally to employees, consumers, and others. Additionally, the financial institutions administer changes to the disclosure as mandated by law or regulation or as required to meet a specific business purpose. Specific examples of this type of review include removal or truncation of SSNs when the entire number is not required and the removal or truncation of the account number or credit card number where the full number is not essential. It may be necessary to keep an SSN in an active file and continue to use it, even after the relationship between individual and business is over (e.g., tax reporting on employee pension payments, to regulators or auditors reviewing the period when the relationship did exist).
- d. Protection of SSNs – In addition to restricting access as described above, many financial institution applications create audit logs which record activities conducted through or within the application. These audit logs can provide the records of employees, contractors, and others who have accessed consumer information. The knowledge of the logs' existence serves as a deterrent to unauthorized access, and allows detection of access attempts and evidence of unauthorized activity. Audit logs also can facilitate anomalous behavior detection (e.g., activity that is inconsistent with expected behavior or outside the scope of anticipated norms), thereby providing an early indicator of potentially fraudulent activity.

Also, based on the specific facts and circumstances, financial institutions may encrypt sensitive consumer information. Various encryption technologies may be used based on such factors as the need and the sensitivity of the data and whether the data is in transit or at rest. Encryption can ensure that unauthorized access does not result in the compromise of the sensitive information. Financial institutions apply other measures such as intrusion detection, malicious software (“malware”) detection and cleaning, traffic monitoring, and firewall routing technology to protect their network infrastructure, consumer information, and proprietary information.

Some government agencies do not allow financial institutions to transmit sensitive data in encrypted formats. We *encourage* government agencies to permit the transmission of encrypted data when our member financial institutions share data with government agencies.

- e. Storage of SSNs – Storage of current and former employee and customer information is subject to information security requirements. Information retention periods are established by financial institutions in conformance with legal, regulatory, contractual, and operational obligations, which vary by line of business and between customer and employee records. These retention periods ensure that information, including consumer information, is destroyed once it is no longer required.
- f. Destruction of SSNs - When records containing SSNs are available for destruction, based on financial institutions' document retention schedules, destruction is accomplished securely, typically through third-party secure document destruction services, eliminating specific SSNs from all paper and computer systems. The documents, tapes, and other media are completely destroyed so as not to be retrievable. For some media, there exist other acceptable, non-destructive means of deleting the data, such as overwriting and erasure. BITS published a paper in March 2006 that outlines a framework for financial institutions to evaluate and mitigate the risks associated with the transport and storage of physical media and the destruction or erasure of data. This framework complements individual institutions' risk assessment and risk management policies and helps risk managers and information security professionals by outlining key questions, identifying risks that can (and cannot) be mitigated, educating key vendors about the needs of financial institutions, implementing appropriately secure storage and transport procedures, and developing effective audit procedures.²

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

Yes, there are numerous government mandates governing private sector use of SSNs in addition to requirements to ensure that sensitive information is adequately protected. For example, federal, state, and local laws that require financial institutions to collect SSNs include verifying the identity of potential or existing customers. The regulations implementing Section 326 of the USA PATRIOT Act require banks, savings associations, and credit unions to verify the identity of customers opening new accounts by obtaining a U.S. tax identification number for all customers who are "U.S. persons" which for most individuals will be their SSN.³ Those same rules require financial institutions to verify the identity of customers. Thus, financial institutions need to compare the given SSN to external data sources to ensure it really belongs to the customer using it. While that verification process often relies in part on information furnished by the traditional credit reporting agencies, it (a) is not covered by a "credit reporting" exemption, and (b) uses other data sources, such as the Social Security Administration ("SSA") "Death Master File" or "Death Index."

The US Department of Education uses an SSN as the account number for student loans and provides this account number (the SSN) to schools with disbursements to ensure the appropriate accounts are credited.

² See BITS Report: Key Considerations for Securing Data in Storage and Transport: Securing Physical Media in Storage, Transport, and for Data Erasure and Destruction, at: <http://www.bitsinfo.org/downloads/Publications%20Page/bitsdatatrans.pdf> (March 2006).

³ According to the Federal Financial Institutions Examination Council's Electronic Banking Booklet, "Verifying a customer's identity especially that of a new customer, is an integral part of all financial services. Consistent with the USA PATRIOT Act, federal regulations require that by October 1, 2003, each financial institution must develop and implement a CIP that is appropriate given the institution's size, location and type of business. The CIP must include risk-based procedures to verify the identity of customers (generally persons opening new accounts). See http://www.ffiec.gov/ffiecinfobase/html_pages/ebanking_book_frame.htm.

In this instance, the US Department of Education requires that financial institutions use an SSN as account number and identifier. Additionally, student lending departments are required by law to report to the National Student Loan Data System and must use the SSN, which is also the student's loan number.

There also are government requirements that financial institutions protect sensitive information, including SSNs. For example, the Interagency Guidelines Establishing Information Security Standards, which implements Title V of GLBA, require financial institutions to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family, or household purposes, and with whom the institution has a continuing relationship. In addition, the regulators issued guidance in October 2005 requiring financial institutions to review and strengthen their electronic banking authentication programs.⁴

Further, federal laws and regulations prohibit insurance companies from contracting or appointing agents and brokers convicted of a felony involving dishonesty or breach of trust unless written consent is obtained from the appropriate insurance regulator. In obtaining this consent, state insurance departments require insurers to conduct background investigations or attest to the worthiness of the agents and brokers it appoints. As a practical matter, the SSN is used to obtain the background report, but the use of an SSN for a background investigation is not required. Similar rules exist for screening bank employees, and in some cases, the employees of service providers of the bank.

Are there alternatives to these uses of the SSN?

As we mentioned, SSNs have a special status as the only unique, permanent, universal individual identifier. For example, name alone is inadequate because there are so many duplicates (and so much room for ambiguity with initials, diminutives, Jr., Sr., etc.), and even name plus date of birth ("DOB") or address often fails because of frequent address changes, multiple people with the same name at the same address, or common ethnic surnames. Without a universal identifier, it would be difficult for businesses to identify or verify identity, thus making it easier for fraudsters to perpetrate crimes.

If SSNs become unavailable to government and legitimate businesses as a unique identifier, either due to legal prohibitions or due to widespread compromise, potential consequences include increased verification errors, increased fraud, and ultimately increased lending and servicing costs. Additionally, substituting other measures for SSNs may actually face the same risks currently associated with SSNs. Eliminating the SSN could simply mean more errors and untangling errors, particularly tax reporting errors, which could be frustrating and costly for the consumer. That being said, there are some alternatives worth exploring, including restricting the use of the complete SSN, particularly when it is used for verification purposes (for which the last four or six digits are usually sufficient) and as account numbers for student loan purposes (as required by the US Department of Education) rather than identification purposes (for which any limitation on SSNs would be problematic).⁵ Additionally, we *encourage* the government to examine the use of other information for authentication purposes and, if other methods prove to be effective, gradually, move away from using SSNs as the primary authenticator.

⁴ "Financial institutions should perform risk assessments of their environment and, where the risk assessments indicate the use of single-factor authentication is inadequate, the institutions should implement multi-factor authentication, layered security, or other controls reasonably calculated to mitigate risk." See FFIEC Information Security Booklet at: http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm.

⁵ "Verification" typically refers to supplemental use of SSNs in combination with other identifiers for account access while "identification" typically refers to the primary use of SSNs, potentially in combination with secondary identifiers.

It is important for government and business to work together to develop solutions and to continue educating individuals on how to protect their identity. For example, the financial services industry would like an enhanced ability to quickly verify SSNs used in new account opening procedures against the SSA databases. An expansion of the SSA's consumer consent-based social security verification ("CBSV") process (allowing for the economical, real time verification, of SSNs required as part of the account opening procedures) would be highly effective in reducing fraud and identity theft.⁶

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

A majority of states have enacted laws that restrict or govern the use of SSNs. California was the first state to enact laws requiring responses to data breaches and limiting display of SSNs. As such, the California law on limiting the use of SSNs has become the model for other states enacting similar laws. Most state laws have imposed additional requirements to safeguard sensitive personal information by financial institutions but continued to permit businesses to use SSNs for the purposes of identifying and verifying the identity of customers, potential customers (applicants), employees, and others as appropriate.⁷

Numerous state laws actually require the use of SSNs for verification purposes by insurance companies to check "dead-beat" parent lists before paying a claim, to ascertain if the deceased had additional policies with the carrier, or to check delinquent tax roles before making a claim payment.

Some states, however, enacted laws intended to safeguard SSNs with unintended negative impact on business practices. For example, New York enacted a law that prohibits the disclosure of SSNs in certain circumstances, among other new requirements. However, New York defines SSNs as the number provided by the SSA or any number "derived from such number."⁸ This could possibly include truncated SSNs even though that may not have been the intent of the legislation. New York also specifically states that an encrypted SSN is not an SSN without a definition of encryption. Prohibition on the use of a number redacted to only display the last four digits would be problematic for financial institutions since a redacted SSN is now commonly used for public records and in communications with customers to ensure the communication is with the appropriate person.

A recent Minnesota law also mandates that a "person or entity, not including a government entity, must restrict access to individual Social Security numbers it holds so that only employees who require [emphasis added] the numbers in order to perform their job duties have access to the numbers...."⁹ It may be difficult for a company to prove that the use of an SSN is "required" rather than "required or appropriate." The Minnesota state law was set to take effect in July 2007 but, recognizing that the law could greatly harm institutions, the compliance date was moved to July 1, 2008. Since it is difficult for a national institution to vary practices at the state level, especially where this was not the intent of the state, financial institutions would benefit from uniform national standards.

⁶ BITS and the Roundtable submitted a joint comment letter to the SSA in support of their CBSV process and provided comments on issues such as full name matching, real-time vs. batch submissions, daily limitation of records and expectation of volume, and document requirements. The comment letter is available at: <http://www.bitsinfo.org/downloads/Comment%20letters/SSACOMMENTBITSandRoundtableFINALccV2.pdf> (February 2006).

⁷ See GAO Report, "Social Security Numbers", at: <http://www.gao.gov/new.items/d051016t.pdf> (2005).

⁸ NY Social Security Number Protection Law, 2005 NY S.B. 6909 (2006).

⁹ MN Omnibus Data Practices Bill, 2006 S.F. No. 3132 (2006).

Additionally, the Minnesota law prohibits the sale of SSNs “obtained from consumers in the normal course of business.” Laws that contain broad prohibitions on the “sale” of SSNs are problematic because there are many situations in which SSNs are transferred by financial institutions and third parties as identifiers but may be deemed legally as part of the “sale.” In complying with the Minnesota law, credit reporting agencies interpreted "ban on sale" to mean that they could no longer provide the institution a full SSN. For example, when financial institutions send the SSN listed on credit applications to the credit reporting agencies, the consumer’s SSN on file at the credit reporting agency is returned as part of the standard information on consumer's credit report. The financial institutions then compare the SSN returned from the credit reporting agency with the one supplied by the consumer on the credit application. Because the credit reporting agencies consider this transfer of an SSN a "sell" transaction rather than a "matching or verification" transaction, they prepared to block the first five digits of the SSN on the credit report, thereby, rendering a highly effective method of verifying the identity of applicants and future customers obsolete. As a result, financial institutions would be required to change their fraud assessment systems to recognize a new error flag. Then, each error would have to be manually researched and resolved. This process also would include requesting a full SSN from the applicant in order to fulfill USA PATRIOT Act requirements, which could increase the likelihood of SSNs being compromised. We have similar concerns with provisions of H.R. 3046, which the House Ways and Means Committee of the U.S. House of Representatives is considering.¹⁰

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?

An SSN is one of several necessary elements used for identification or verification of a customer. Financial institutions use the SSN with other information to initially ensure that the customer is truly who he/she claims to be when opening new accounts with financial institutions. Financial institutions also authenticate customers on an on-going basis before they access customer information or initiate transactions. Increasingly, SSNs are used only in combination with other information as an authenticator.

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

In recent years, financial institutions have enhanced authentication security and have reduced or eliminated the use of SSNs as the primary factor in the on-going authentication process for both customers and employees, as per guidance by financial regulators, and given the risks that some SSNs are publicly available. For example, financial institutions apply layered controls to protect consumers and financial institutions, including the monitoring of unusual account activity using sophisticated pattern detection tools to detect and prevent fraud.

While authentication is an important element in a robust information security program, there are practical challenges in deploying stronger authentication controls including customer acceptance, the maturity of the technology, cost, scalability, interoperability, and dependence on government-issued credentials. Authentication methods viewed by customers as overly complex or unwieldy will not be accepted and may result in even greater risk of misuse or fraud.

¹⁰ Social Security Number Privacy and Identity Theft Prevention Act of 2007, H.R. 3046 (2007).

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

The changes made by financial institutions to reduce the use of SSNs have been part of continuous efforts to improve information security programs in response to changing risks, customer concerns, and regulatory and supervisory requirements. This process is costly, but results in reduced fraud and addresses customer concerns and expectations. However, eliminating the use of the SSN in the broader process of identifying and verifying the customer in establishing accounts would be problematic. Eliminating the SSN would not only limit access to accurate credit history information and create significant infrastructure challenges, but would also restrict consumers from opening accounts, impose barriers to the USA PATRIOT Act CIP, and potentially create economic barriers to commerce. In cases in which identification other than an SSN is available, financial institutions must continually enhance their risk assessment processes and their verification procedures to guard against identity theft.¹¹

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?

Some financial institutions have substituted unique employee identification numbers for SSNs. A unique personnel number is used for employee identification so that SSNs are not easily accessible. However, these numbers continue to be tied to SSNs on employees' accounts in the back office for tax, legal, and regulatory reporting purposes. Even if financial institutions eliminate SSNs as an employee-facing number, the government still requires financial institutions to use SSNs to identify employees for tax and retirement reporting purposes.

In the case of customers, SSNs are still the best connector within the business, across all internal business and service lines. Third parties submit information, identifying individuals by their SSNs, since those parties would not have access to or knowledge of the internal number within the financial institution. The institution uses the SSN to match the information received to its internal identification number. Similarly, should the institution need to provide information to a third party about an individual, the institution sends the third party an individual's SSN since an internal number will not be recognized.

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

Elimination of SSNs as an internal identifier would create a loss of continuity across business lines and difficulty in accurately reporting to government (as required under the appropriate laws). Additionally, the elimination of SSNs would increase the chance of incorrect credit information and make it more

¹¹ The Roundtable and BITS filed a joint comment letter with the Department of Homeland Security regarding a proposal for minimum standards for state-issued driver's licenses and identification cards and recommended that the federal and state governments work closely with the industry to develop cost-effective mechanisms for verification purposes so that identity theft and fraud do not occur. The comment letter is available at: http://www.bitsinfo.org/downloads/Comment%20letters/RoundtableCommentLetterREALID_NPRMMay07.pdf (May 2007).

difficult to conduct required employee background checks. Prohibiting the use of SSNs on the whole can create more risks and customer dissatisfaction; however, by providing an opt-in alternative customer access number, financial institutions can take a positive step away from the use of an SSN as the sole identifier.

Using another internal identification number, rather than an SSN, is not feasible in the financial industry due to the common interaction with other financial entities. Additionally, many more customers can recall their SSNs easier than a customer identification number assigned by a particular institution. Customer education and customer frustration create significant costs in implementing an internal identifier. As a result, for operational reasons and at customers' request, many financial institutions continue to use SSNs across businesses, when working with third party service providers, and according to governmental reporting requirements (e.g., tax reporting, USA PATRIOT Act CIP, anti-money laundering).

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?

SSNs have evolved, regardless of original intent, to become the *de facto* unique identifier for consumers. This number is the only unique identifier that today accompanies most consumers from cradle to grave. SSNs remain a constant in an ever-changing world of name change from marriage and divorce, shifting addresses, and driver's license re-issuance as consumers move from one state to another. SSNs are used in efforts to ensure the accurate association of historical information on financial accounts, credit reports, public records, medical records, and a host of other critical relationships and services to a specific consumer who stands before you. For example, the financial industry reviews each SSN to ensure that the SSN is valid using the SSA High Group List.¹² This review identifies the creation of fictitious SSNs from ranges not issued by the SSA and thereby preventing fraud or credit abuse. Additionally, institutions use the SSN to verify that the SSN holder had not been reported deceased in the SSA Death Master File. State law enforcement uses the SSN to protect against both business and individual fraud.

In the mortgage industry, SSNs are used to validate employment status, income, and assets, all of which have a significant impact on a lender's decision to extend credit. Lenders use third-party databases to verify employment status, income, and assets in light of the potential that this information is fraudulent or embellished. One check, for example, is to see if the borrower has previously been involved in a fraudulent transaction with another lender, which would raise a significant "red flag."

Consumers also benefit from industry's ability to verify SSN information by reducing the incidence of fraud and errors. Incorrect data entry of consumers' SSNs can be easily determined, reducing the incidence of erroneous tax reporting on interest earned and deductible interest expense and thereby reducing the number of consumers required to be subjected to annual solicitation for a corrected SSN due to mismatches submitted to the IRS and misrepresentation.

There are certain fraud mitigation processes that use SSN matching to detect patterns that are associated with fraud. Many financial institutions utilize software to identify patterns and common threads and analyze variations as a means of preventing and detecting fraudulent activity. Prohibiting the use of SSNs

¹² See SSA's High Group List at: <http://www.ssa.gov/employer/ssnvhighgroup.htm>.

will reduce the effectiveness of these activities in direct contrast to the purpose of any rule or law designed to prevent misuse and identity theft.

Identity Theft Assistance Center uses SSNs at the beginning of its victim assistance service as part of its identity verification process to ensure that ITAC is speaking to the right individual, the actual identity theft victim.

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

There are no alternatives that are as effective as an SSN. SSNs are the best means by which one can protect against fraud across all businesses and industries. Although few industries use SSNs as the sole means to protect against fraud, it is a vital component in all risk-management programs.

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

Limitations or restrictions on the use of SSNs by other sectors could make it more difficult for financial institutions to prevent or investigate fraud. In the mortgage industry, if SSNs were limited or restricted, the ability to identify “red flags” prior to granting a mortgage would be limited or restricted. Additionally, as previously discussed, limitations on the sale of SSNs or numbers derived from the SSN (as in the Minnesota state law) require financial institutions to create additional “red flags” within their fraud programs and restrict the uses of their fraud programs.

5. The Role of the SSN in Identity Theft

How do identity thieves obtain SSNs?

There are many ways in which SSNs might be obtained by identity thieves. Some of these methods include, subjectively ranked from the most prevalent to the least prevalent:

- a. Intrusion at home or office by friends, family, or in-home employees;¹³
- b. Malware/spyware/keystroke loggers;
- c. Pretexting via email and websites (often referred to as "phishing"), via telephone (often times referred to as "vishing") and in-person;¹⁴
- d. Sifting through refuse or other forms of improper disposal of personally identifiable information (e.g., “dumpster diving”);
- e. Mail theft;
- f. Internal fraud (employee sells information to an outside party);
- g. Electronic intrusions or hacking;
- h. Stolen or lost data (in electronic, paper or other media) or devices (laptops, PDAs);
- i. Loss of wallet/purse; or

¹³ ITAC interviewed 275 verified victims of identity theft at the conclusion of the ITAC victim assistance interview. Forty-two percent of victims knew how their information was compromised and of those, the cause most frequently cited was friends, relatives and in-home employees. See ITAC news release dated January 29, 2007 at: www.identitytheftassistance.org.

¹⁴ Phishing is the use of technology and social engineering to entice consumers to supply personal information such as account numbers, login IDs, passwords, and other verifiable information that can then be exploited for fraudulent purposes, including identity theft. Phishing is most often perpetrated through mass emails and spoofed websites. Vishing is the criminal practice of using social engineering and Voice over IP (“VoIP”) to gain access to private personal and financial information from the public for the purpose of financial reward.

- j. Submitting change of address on an existing account and asking for the SSN to be mailed.¹⁵

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? 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 typically use the SSN in order to gather other, additional information before approaching a business, as few businesses accept SSNs as the only means for either identification or authorization. Many institutions request different items for authentication, so the thief needs to obtain (or falsify documents) as much as possible. Once a thief acquires an SSN, he or she can use social engineering¹⁶ to round out the compromised identity and commit identity theft by:

- a. Opening or taking over an account;
- b. Changing one's address (to cover up accounts opened);
- c. Committing employment and tax fraud (e.g., illegal immigrants using SSNs for employment or someone trying to hide one's true identity to get hired);
- d. Obtaining utility services and/or renting apartments;
- e. Obtaining other government-issued identification/benefits; or
- f. Impersonating another individual.

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

If alternatives to SSNs were available, the same risks faced by SSNs, including identity theft risks would still be present. On the business side, alternatives to SSNs would decrease verification certainty while increasing the necessary costs to attributing these alternatives to a specific individual. Alternatives will lead to greater inaccuracy and create a need to match more common data elements. As a result, there will be an increased likelihood of inaccurate records and a greater opportunity for fraud. Additionally, the use of alternatives may create cumbersome identification procedures for customers because they would have to recall many identifiers rather than the single number that they remember across all accounts, the SSN. In cases in which identification other than a SSN is available, financial institutions must continually enhance their risk assessment processes and their verification procedures to guard against identity theft.

Conclusions

SSNs are critical to the processes within financial institutions for identification, authentication, and verification purposes. Using an SSN for identification is important to reduce fraud, facilitate various customer accounts, comply with regulations, and conduct tax and legal reporting requirements. Financial institutions continually take proactive steps to further enhance the protection of SSNs. As such, the use of an SSN as an authenticator, except in combination with other protections, is being curtailed by the

¹⁵ Studies have shown that data breaches are not the leading cause of identity theft; in fact, a Javelin Strategy and Research study found that less than one percent of those whose data was lost were actually victims of identity fraud. See *Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses*, Javelin Strategy and Research, September 2006.

¹⁶ "Social engineering" refers to the practice used to manipulate people into divulging confidential information. This information can include information about other accounts, personal and transactional information, a driver's license, credit card information, or mother's maiden name.

financial services industry. The financial services industry is continually evolving the use of SSNs for fraud prevention purposes.

We *urge* federal, state, and local governments to work closely with all industries before limiting operational uses of SSNs since there may be unintended consequences from these limitations. The creation of another identifier in place of an SSN may result in the same risks to consumers.

In compliance with existing laws and regulations, at the request of our customers, and to address changing risks, the financial services industry has taken extensive steps to improve its processes and procedures to protect sensitive information, including SSNs. We *recommend* that the current regulatory framework for financial institutions be extended to other industries so that a uniform, national standard exists across all industries.

If you have any questions or comments on this matter, please do not hesitate to contact us or John Carlson, Senior Vice President of BITS or Melissa Netram, Director of Regulatory and Securities Affairs for the Roundtable at 202.289.4322. Thank you for your consideration.

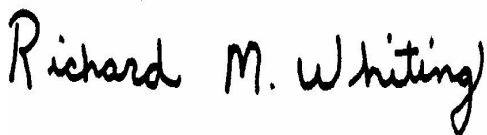
Sincerely,



Anne Wallace
Executive Director
Identity Theft Assistance Center



Leigh Williams
President
BITS



Richard M. Whiting
Executive Director and General Counsel
The Financial Services Roundtable

cc: Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency, Office of Thrift Supervision, Securities and Exchange Commission