

STATEMENT
OF
ERIK STEIN
EXECUTIVE VICE PRESIDENT & DIRECTOR,
FRAUD RISK MANAGEMENT
COUNTRYWIDE FINANCIAL CORPORATION
ON BEHALF OF BITS
BEFORE THE
UNITED STATES CONGRESS
HOUSE COMMITTEE ON WAYS & MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
HEARING ON
THE ROLE OF SOCIAL SECURITY NUMBERS (SSNs)
IN IDENTITY THEFT AND
ISSUES RELATED TO ENHANCING PRIVACY

MARCH 30, 2006

**TESTIMONY OF ERIK STEIN
MEMBER, BITS FRAUD REDUCTION STEERING COMMITTEE**

Introduction

Good afternoon Chairman McCrery and members of the Subcommittee. My name is Erik Stein. I am Executive Vice President and Director of Fraud Risk Management at Countrywide Financial Corporation, America's largest residential mortgage lender and servicer. I have over 25 years of banking, credit card, mortgage lending and dot com experience and am currently responsible for preventing, detecting, investigating, mitigating and reporting on criminal conduct by, through or within Countrywide and its family of companies.

I am pleased to appear before you today on behalf of BITS and its Fraud Reduction Steering Committee (FRSC) to discuss the role of Social Security Numbers (SSNs) in identity theft and enhancing SSN privacy.

BITS is a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS' member companies provide fuel for America's economic engine, accounting directly for \$40.7 trillion in managed assets, \$960 billion in revenue, and 2.3 million jobs. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS focuses on key issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses.

Especially relevant to today's testimony, the mission of the BITS Fraud Reduction Steering Committee (FRSC) is to identify fraudulent trend activity, reduce fraud losses, and foster new opportunities to reduce the impact of fraud on the financial services industry and our customers. Participants in the BITS Fraud Reduction Steering Committee include representatives from financial institutions, industry associations and the Federal Reserve.

BITS works with government organizations including the U.S. Department of Homeland Security, U.S. Department of the Treasury, federal financial regulators, Federal Reserve, technology associations, and major third-party service providers to achieve its mission.

BITS is also a founding and active member of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). The mission of the FSSCC is to:

- Foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security
- Identify voluntary efforts where improvements in coordination can foster sector preparedness
- Identify barriers and recommend initiatives to improve sector-wide knowledge sharing and timely dissemination of critical information among all sector constituents
- Promote public trust and confidence in the financial services sector's ability to withstand and recover from terrorist attacks, cybercrime, and natural disasters.

The financial services industry has been aggressive in its efforts to strengthen cyber security, reduce fraud, and mitigate identity theft. Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and ID theft. As just one example of these efforts, the Identity Theft Assistance Center (ITAC), which BITS and the Financial Services Roundtable established in 2004, recently announced that it had helped over 5,000 individuals in restoring their financial identity.

SSNs: A Unique Identifier

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 financial accounts, credit reports, public records, medical records and a host of other critical relationships and services to a consumer.

Critical Role of SSNs for Financial Institutions

The use of SSNs by financial institutions is essential to satisfy a variety of statutory obligations such as to report earned interest income and deductible interest payments on mortgages for millions of American consumers. In addition, SSNs facilitate practical realities such as accessing credit reports to determine creditworthiness, performing due diligence on business partners and correspondent banks and, as required by the USA Patriot Act, performing enhanced due diligence on politically-exposed persons (PEP)¹.

¹ The Federal Financial Institutions Examination Council's (FFIEC) Bank Secrecy Act Anti-Money Laundering Examination Manual defines a PEP as "a person identified in the course of normal account opening, maintenance or compliance procedures to be a 'senior foreign

Under the USA Patriot Act, financial institutions are obligated to “know their customer,” and to take steps to verify the identity of account holders. In addition, financial institutions perform due diligence on business partners and vendors. One of the integral parts of compliance with these obligations often involves the use of public records which are searched by use of the SSN, or, in the case of business, EIN, to ensure that the results returned are unique to the subject of the due diligence.

After the customer’s identity has been verified and the relationship has been established, many financial institutions utilize the SSN internally to track the customer’s relationship with the financial institution across multiple accounts and for a variety of legitimate internal business reasons. This legitimate, internal business use should remain exempt from additional limitations.

Criminal investigations initiated by financial institutions are facilitated by the availability of SSNs both in the financial institution’s database and in public records. Public records are frequently used by financial institutions’ staff during the investigation of potential criminal conduct. During the investigation, the SSN is the single most reliable method of identification, correlation and association of the perpetrators to their public records, which often provide critical details imperative to solving the crime and locating the suspect(s). The loss of this valuable tool would jeopardize the effective investigation of financial crimes.

Financial institutions and other businesses routinely screen prospective employees to verify identity, validate applicant employment and education history, and check for criminal conduct prior to extending job offers. These background checks, particularly in high-risk occupations or vulnerable industries, can reduce the incidence of criminal infiltration, potential workplace violence and security risks, including customer data security and privacy risks. The SSN is critical in verifying a potential employee’s background and allows for the ongoing monitoring of employees in high-risk positions. Without the use of a SSN, financial institutions would find it very difficult to adhere to a “know your employee” standard.

SSN Verification: A Key Tool for Successful Identity Determination of Customers

SSNs play a pivotal role in identity determination: the establishment and verification of the identity of unique persons with whom financial institutions, and others, conduct business. With millions of John Smiths in America, the identity determinate of which John Smith with whom a financial institution is dealing is made by the single unique identifier common to all Americans, his SSN.

political figure,’ any member of a senior foreign political figure’s ‘immediate family,’ and any ‘close associate’ of a senior foreign political figure.”

Importantly, financial institutions realize that the ability to successfully verify John's SSN is not the same as successfully determining his identity. A financial institution must do this through the use of identification documents such as driver's license, passport and other, typically government-issued, identity documents containing a picture, signature, expiration date, security features, a physical description, etc. It should be noted that SSNs have not been used for identity verification due to the lack of a highly secure SSN card, tamper-proof signature, picture and expiration. The SSN card contains few security features making it easy to counterfeit and reducing or eliminating any value in its use for identity verification. The SSN is thus only a tool, albeit an invaluable one, in the process of determining the identity of an individual. It is clear, however, that verification is a key tool for achieving positive identity determination.

Value of the SSN to Criminals

The critical role of SSNs is the fundamental reason for their intrinsic value to criminals' intent on committing crimes. Criminals utilize SSNs in the commission of identity theft. Identity Theft may be divided into "true name" fraud where the perpetrator uses the "true" identity of a consumer, or identity fraud where combinations of consumer's identities are pieced together or even fabricated to create a synthetic identity, a new person.

It is important to recognize that criminals committing identity fraud don't need to steal or purchase SSNs to commit their crime. The structure of the SSN is common knowledge to anyone who has ever had, or seen, one or checked the Social Security Administration's (SSA) website (i.e. <http://policy.ssa.gov/poms.nsf/lnx/0100201030?opendocument>.) Valid SSNs can be determined by checking the SSA's website for the highest group issuance <http://www.socialsecurity.gov/employer/highgroup.txt>. By selecting a recently issued SSN, and applying for credit, a criminal creates an identity with the Credit Reporting Bureaus (for which there will be no conflicting SSN information since the valid SSN holder is an infant).

Since financial institutions and lenders don't have the ability to verify the SSN, name and date of birth combinations (other than the current Enumeration Verification System pilot in the mortgage industry which is not a robust, enterprise-strength, low cost, timely verification process and therefore narrowly used), the identity thief is unlikely to be caught. Restrictions on the sale and purchase of SSNs would do little to prevent this type of fraud. The fraud also doesn't rely on the theft of SSNs from their legitimate owner.

BITS members would encourage the Subcommittee to remove the highest group issuance list from the public domain and make it available to financial institutions and others with a legitimate business need on a subscription basis as is currently done with SSA's Death Master File. While this list is an essential tool today to

validate SSNs provided to financial institutions, its potential use by criminals is inconsistent with its availability to the general public.

Another area of risk is that criminals in search of identities for committing true name fraud can readily obtain name, address, SSN and account number combinations by mail theft during January each year when millions of account holders and borrowers receive their 1099's or 1098. By statute, these tax forms are required to display the account holder's SSN, and, for mailing purposes, must have the recipient's name and address along with the account number to identify the account for which the form has been filed. These forms are mailed *en masse* by financial institutions at the beginning of the year for use in requisite income tax filing by the consumer thereby making for a target-rich environment for obtaining identities through mail theft.

Combating Identity Theft through SSN Verification

For decades, financial institutions have required SSNs and identity documents to open accounts, make loans and accept transactions by their customers. However, the industry has been relegated to validation methods that do not, and cannot, validate the existence of, and their association with, a consumer's personal identifiers (such as name, date of birth and gender). For SSNs, financial institutions have relied on rules that determine if the SSN had been issued (the highest group issuance list referenced above available from SSA), that the SSN holder had not been reported deceased (SSA's Death Master File), and that the holder was not born after the issuance of the SSN by SSA (from historical highest group issuance lists). The single most important validation has been unavailable, that the consumer presenting the number is the holder of record in SSA's database.

The proposed Consent-Based SSN Verification (CBSV) program recently published for public comment by the SSA is an extension of the Enumeration Verification System pilot and is a critical effort to allow financial institutions to verify SSNs. It will allow financial institutions to verify the SSN holder's name and date of birth against SSA's database. Establishing a system capable of high volume, low cost, real time verification direct to financial institutions and lenders would significantly reduce the incidence of synthetic identities. "True name" identity theft would become more difficult with the validation of date of birth and the optional gender code by financial institutions utilizing a CBSV program.

BITS' members strongly encourage the Subcommittee to support the CBSV program². We also request that the SSA evaluate the removal of restrictions on the daily volume of submissions by participants, work towards improving the proposed response times, eliminate requirements for a standalone consumer

² Attached is the BITS/Financial Services Roundtable Comment Letter on the Social Security Administration's Consent-Based Social Security Verification Process (February 2006)

authorization allowing incorporation of the authorization into loan or account documents, and review the cost structure.

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

Further, the BITS members, due to the high perceived value of CBSV, would also encourage the consideration of federal legislation to mandate similar programs related to other governmental identity documents used in the financial industry to verify consumers including US passports, alien registration documents (e.g. Non-Resident Alien card) and state driver's licenses. Financial institutions, while under obligations to know their customer under the USA Patriot Act, have not been afforded the tools to ensure the validity of the documents presented for identity verification. We have had to rely exclusively on the appearance of legitimacy (e.g. verification of security features, visual inspections or tests that validate the structure of a driver's license number but, again, not the name of the true license holder).

Unintended Consequences for Limiting Use of SSNs

The critical roles of SSNs for use in financial institutions, investigations, public records, lending, account servicing, tax reporting and much more makes the availability and use of the SSN for legitimate business uses an imperative. It is important that additional proposed restrictions on the use, sale and purchase of SSNs be thoroughly evaluated to ensure that unintended consequences do not occur. This could include potential increases in fraud; economic impacts from increased lending costs; and decreased loan approval rates and other adverse implications to commerce.

Conclusion and Recommendations

In summary, the use of SSNs is critically important to the financial services industry. They allow financial institutions to meet various statutory obligations such as knowing who their customers, employees, and business associates are; reporting earned interest income and deductible interest payments on mortgages; and satisfying due diligence expectations as set forth by statutory obligations. All of these functions are performed to keep our customers and their financial assets safe, and to ensure the security and reliability of the economy.

On behalf of BITS and our member financial institutions, we encourage Congress to:

- Continue to allow financial institutions to use SSNs without additional restrictions and limitations;
- Exercise caution if changes are considered, to be especially alert to unintended consequences such as increased fraud;
- Support a verification program capable of high volume, low cost, real time verification in a manner consistent with customers' demands; and
- Review statutory obligations that require the printing of SSN's (e.g. 1098, 1099) to determine if the risk of compromise exceeds the value derived and, if so, enact changes to remove these obligations.

Thank you for the opportunity to testify before you today. I would be happy to answer any questions.



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

February 26, 2006

Office of Management and Budget (OMB)
Attn: Desk Officer for SSA
Fax: 202-395-6974

Social Security Administration, DCFAM,
Attn: Reports Clearance Officer
Fax: 410-965-6400
E-mail: OPLM.RCO@ssa.gov

Re: Comment to Consent Based Social Security Number Verification (CBSV) Process

Dear Sirs and Madams:

BITS and The Financial Services Roundtable appreciate the opportunity to participate in the Social Security Administration's (SSA) request for comment regarding the Consent Based Social Security Number Verification (CBSV) Process.

BITS and The Financial Services Roundtable share membership and represent 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. BITS works to leverage the intellectual capital of its members, fostering collaboration to address emerging issues where financial services, technology, and commerce intersect. The Roundtable promotes the interests of member companies in legislative, regulatory and judicial forums. Roundtable member companies provide fuel for America's economic engine, accounting directly for \$40.7 trillion in managed assets, \$960 billion in revenue, and 2.3 million jobs.

Our members have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology,

information sharing, and cooperative efforts with government and law enforcement agencies. While our members' foremost concern is to protect their customers and maintain their trust, they are also mindful of the need to comply with the regulations set forth by Section 326 of the Patriot Act. This section requires institutions to verify not only the identity of a customer, but also the accuracy of the information provided.

In the interest of reducing fraud and complying with Section 326 of the Patriot Act, BITS members supported the initial pilot, the Enumeration Verification System (EVS), to allow institutions to affirmatively verify consumer's name, social security number and date of birth (DOB). This pilot provided a means to ensure accounts were opened for the legitimate consumer and not a "fraudster" and we applaud the SSA's efforts to provide enhancements in the form of the CBSV that would benefit our customers and our industry.

After careful review of the information collection process outlined in the December 30, 2005 Federal Register, we respectfully offer the following comments:

"Valid Consent from Number Holders"

There is concern that, since the CBSV is designed to verify a person's Social Security Number (SSN) to their name (and potentially DOB), there may be instances where financial institutions are misled and the consent is not from the true applicant as may be the case in identity theft or identity manipulation. There should be acknowledgement that while financial institutions have established a process for verification, there is still an opportunity for applicants to provide false information. This verification process is fundamental to ensuring the name, SSN, and DOB (optionally) match the authorizing consumer. While we understand the use of "valid consent from number holders," we want to ensure that there are no consequential impacts to financial institutions from the fraudulent completion of consent authorizations.

Inclusion of Gender Code

The public comment details the submission as consisting of a name, SSN and DOB (if available) and the results provide a match to name, SSN, date of birth and gender code (which is not part of the submission). Clarity needs to be provided on whether gender code is intended to be a submitted/verified field.

Full Name Matching

While SSN, DOB (and possibly gender assuming it is used) are unique variables, one's name is subject to wide variation. It is suggested that the full first and full last be used for matching and that a secondary field be available for each that could include a nickname, shortened name (Jim vs. James) and last name. The use of a secondary field for name matching would reduce the incidence of re-running queries; improve match rates including where Soundex matching is utilized and the name variation is not conducive to such matching logic; and would accommodate name changes due to marriage, divorce, etc. which may not yet have been reported to SSA.

Real-time vs. Batch Submissions

SSA had indicated its intention to continue the practice of EVS in providing the results of inquiries by Requesting Parties within 48 hours while not guaranteeing such response time. Institutions believe there is strong value in having real-time capabilities and encourage the

SSA to evaluate methods to provide this verification service in real-time as soon as feasible. If batch submissions remain exclusively available, members strongly encourage SSA to provide a response, to inquiries submitted before midnight, by no later than 5am the following business morning consistent with other batch jobs run by financial institutions for fraud detection, verification and posting.

Daily Limitation of Records and Expectation of Volume

While strongly supportive of CBSV, we urge the SSA to reconsider the daily limitation of 5,000 records. One of the inherent values of an automated system of SSN verification is its scalability. With scalability in mind, we recommend the SSA remove the daily limitation. Should hardware limitations be reached by the overwhelming success and adoption of CBSV, the SSA should charge registered user businesses sufficient additional fees to allow the SSA to meet this demand. This linear scalability should also keep the cost per inquiry low. We believe that SSA's expectations of demand for CBSV are substantially below the industry's need for this verification solution. We encourage the SSA to revise its expectations and lower the cost of entry for business by reducing the initial fee of \$40,288.10. While the basis for SSA's expectation of only 150 business users for CBSV is not explained in the publicly available documents, we believe that, with nearly 9,000 FDIC-insured financial institutions alone in the U.S., 5,000 business users is both reasonable and sustainable. This would lower the initial cost of entry to \$1,208.64. However, to both encourage maximum participation and guarantee SSA's financial support of the program, we recommend the initial fee be set at \$10,000.

Document Requirements

SSA-89- Authorization for the Social Security Administration (SSA) To Release Social Security Number (SSN) Verification

Evidence of consumer authorization to verify their SSN is clearly both an obligation of the Requesting Party and a necessary privacy safeguard. However, the requirement for a standalone SSA-89 evidencing said authorization provides no additional safeguard over an obligation for equivalent language, approved by the SSA prior to usage, incorporated into account or loan documents. In addition, this document (SSA-89) cannot be incorporated into loan documents, account signature cards or any other documents. For efficiency and enhancement purposes, institutions must be able to incorporate the authorization language into existing documents that allows them to run the SSN which can then be retained for six years from the authorization date.

The existing retention of these underlying documents already, in most cases, meets or exceeds the SSA minimum retention requirement. Where the existing document retention is shorter than SSA-89's retention requirement, Requesting Parties will voluntarily comply with modification of their retention schedules to achieve the efficiencies afforded by merging these documents with the CBSV authorization. The SSA should consider inclusion of specific authorization of the SSN owner for electronic signature in accordance with the Electronic Signatures in Global and National Commerce Act (ESIGN). SSA's existing allowance of storage of the SSA-89 electronically would be consistent with the use of ESIGN for electronic of the authorization process with inherent increased efficiency.

SSA-89 cannot be modified by the Requesting Party. The defined term can be modified by agreement as specified in the User Agreement, by agreement of the parties executing the Authorization and documented therein. These two statements are mutually exclusive. We recommend SSA clearly delineate the method by which Authorization term extension is to be documented so the Requesting Party can ensure compliance with SSA's requirements.

SSA-88- Pre-Approval Form for CBSV

The Requesting Party has a contractual obligation to protect the integrity of SSA's systems, utilize information requested only for authorized purposes, and to be authorized by the Requesting Party in accordance with their internal approval policies. The need for completion of form SSA-88 for each employee in a large company that has access to the results of the inquiry is overly burdensome and inefficient. We strongly encourage the SSA to make user administration for Requesting Parties an obligation of authorized employees of the Requesting Party and managed through a user interface in Business Services Online (BSO). All service providers to the financial services industry allow the participant to manage their employees' access. The BSO administrative user interface can be designed so as to require the data elements mandated by SSA (e.g. name, SSN, phone number, and email address of each employee) with appropriate electronic attestation by the authorized admin user during new user setup. Maintenance (e.g. changes to the existing information as a result of job status changes, phone or email changes) and deletion (e.g. termination of the employee or job status changes no longer requiring access) can likewise be accomplished through the BSO administrative user interface by the authorized employee of the Requesting Party. This process is much more conducive to large scale employers who may have thousands of employees authorized to access the information from SSA during the processing of accounts or loans.

SSA-1235- Agreement Covering Reimbursable Services

SSA-1235 is "effective upon signature of both parties and shall remain in effect until one or more of the following events occur . . ." While the Agreement is continuously in effect (barring one of the events listed), SSA requires an annual resubmission of the Agreement. The resubmission appears inconsistent with an Agreement with no defined term. We recommend the SSA eliminate the annual submission requirement for form SSA-1235. The provision of the annual fee as defined by SSA each year should be sufficient evidence of the Requesting Party's intent to continue the Agreement. The Conditions of Agreement, paragraph 6, stipulates that the Authorization "must be presented within 60 days after its execution," however the Authorization itself indicates it "is valid only for 90 days from the date signed. . . ." These statements are incongruous and we recommend the SSA reconcile these documents to a consistent period of 90 days. The Conditions of Agreement, paragraph 8, stipulates the Agreement may be terminated "by giving a 60 day advance written notice." However, Section XI. *Duration of Agreement, Suspension of Services, Annual SSA-1235* of the User Agreement specifies "the Agreement shall terminate 30 days after the date of the notice or at a later date specified in the notice." We recommend the SSA reconcile this discrepancy by establishing a consistent 30 day written notice requirement for termination.

Submission of Requests

The CBSV User Guide establishes the file format for submission of requests by the

Requesting Party to SSA. The file format contains a field for a “Multiple Request Sequence Number”; however, the SSA limits the number of file submissions by a Requesting Party to one. Since only one file can be submitted daily, there would never be a need for this field. If the field is anticipated for future use when Requesting Parties may be allowed multiple daily file submissions, we suggest “Future Use” indicated in the description for this field to remove ambiguity.

If you have any further questions or comments on this matter, please do not hesitate to contact us or Heather Wyson at (202) 289-4322.

Sincerely,

A handwritten signature in black ink that reads "Catherine A. Allen". The script is cursive and fluid.

Catherine A. Allen
CEO, BITS

A handwritten signature in black ink that reads "Richard M. Whiting". The script is cursive and fluid.

Richard M. Whiting
Executive Director and General Counsel