The National Council of Social Security Management Associations, Inc.

THE WASHINGTON REPORT
LEGISLATIVE REPORT 12-2000

May 22, 2000

HOUSE SUBCOMMITTEE ON SOCIAL SECURITY HEARING ON USE AND MISUSE OF SOCIAL SECURITY NUMBERS Part I

On May 9th and 11th the Social Security Subcommittee of the Committee on Ways and Means held a two-part hearing on "Use and Misuse of Social Security Numbers." The first day of the hearing provided an overview of the issue and discussion of current laws and proposals to protect SSNs from misuse. The second day focused on the advantages and disadvantages of restricting the use of SSNs.

Rachel Emmons attended both days of the hearing and the following is a summary of the proceedings.

May 9, 2000 Hearing

The following members of the Subcommittee were present: Clay Shaw (R-FL); Sam Johnson (R-TX); Mac Collins (R-GA); Rob Portman (R-OH); Jerry Weller (R-IL); Kenny Hulshof (R-MO); Jim McCrery (R-LA); Robert Matsui (D-CA); John Tanner (D-TN); and Benjamin Cardin (D-MD).

Witnesses presenting oral testimony:

First Witnesses:
John T. Stevens, Jr., Retired Lieutenant Colonel, Upper Marlboro, Maryland;
and
Mrs. Mary Elizabeth H. Stevens, Upper Marlboro, Maryland

Second Witness:
U.S. General Accounting Office:
Barbara D. Bovbjerg, Associate Director, Education, Workforce and Income Security Issues; Health, Education and Human Services Division

Third Witness:
Social Security Administration:
The Honorable James G. Huse, Jr., Inspector General, Office of the Inspector General

The following are items of importance from the testimony of Lieutenant Colonel and Mrs. Stevens:

John T. Stevens, Jr., Retired Lieutenant Colonel, and Mary Elizabeth H. Stevens, Upper Marlboro, Maryland;

The testimony presented by these witnesses was a narrative describing the difficulties the couple has encountered during the past three years. Their SSNs and names have been used to open 33 fraud accounts with a total value of $113,000. The purpose of their testimony was to alert others to the danger of this crime.

The following questions were put forward by the members of the Subcommittee:

Rep. Johnson: Do you think there is a connection between the military and your problems?

Lt. Colonel Stevens: The fraud did seem to start in 1996 when my wife had to use her own SSN on her Air Force dependents ID card.

Rep. Johnson: This (social security number) is the only form of military ID. I remember when they were different numbers, but this was much harder to collate. It is my experience that you don't have to write your SSN on checks at military bases. Is there any other reason, other than your SSN, that could have affected your credit?

Lt. Colonel Stevens: Our SSNs are the only consistent piece of information being used.

Rep. Johnson: Have you had any trouble obtaining your credit reports?

Lt. Colonel Stevens: No.

Rep. Johnson: Didn't they (the credit reporting agencies) clear the records when you pursued it?

Lt. Colonel Stevens: No, often a third party became involved.

Rep. Johnson: Should we investigate the military process – using the SSN?

Lt. Colonel Stevens: I'm not really sure.

Rep. Matsui: Was there more than one person involved?

Lt. Colonel Stevens: We don't have any proof.

Rep. Matsui: What about the purchase of the 1997 Jeep Cherokee?

Lt. Colonel Stevens: They don't go after those people, they go after us.

Rep. Matsui: Did you contact law enforcement officials?

Lt. Colonel Stevens: We don't know how the transaction was actually made. They used our first and last names and our SSNs.

Rep. Matsui: Have the people been apprehended?

Lt. Colonel Stevens: It is up to the businesses that have suffered the losses to pursue them.

Rep. Matsui: Have the collection agencies stopped contacting you?

Lt. Colonel Stevens: No, an account has just shown up recently for the fourth time.

Rep. Portman: Aren't there rules and regulations for reporting agencies? Some liability for incorrect spelling, addresses, etc.

Lt. Colonel: We did contact them. They said it was inconvenient to update addresses, they told us that 15% of the people in the United States move every year. We responded that 85% don't.

Rep. Portman: What about incorrect spelling of names?

Lt. Colonel Stevens: They (the reporting agencies) didn't give us an answer.

Rep. Portman: Have you contacted the SSA?

Lt. Colonel Stevens: No, we haven't.

Rep. Weller: When you discovered what was going on did you contact law enforcement?

Lt. Colonel Stevens: It wasn't against the law.

Rep. Weller: How long has it taken you to clean this up?

Lt. Colonel Stevens: It is still going on.

Rep. Weller: What has been the biggest obstacle?

Lt. Colonel Stevens: Getting people to believe you didn't open the account.

Rep. Weller: Who has been your biggest source of assistance?

Lt. Colonel Stevens: The FTC.

Rep. Weller: Do you have any suggestions for prevention?

Lt. Colonel: Don't use the SSN for primary identification number, and then don't give it out to anyone.

Rep. Shaw: I believe the military commissaries are privately owned. Other stores don't require your SSN – why should they? I doubt it's a military regulation or statute.

Rep. Tanner: Is this still ongoing? Have there been new charges?

Lt. Colonel Stevens: We haven't seen any new accounts.

Rep. Tanner: You attorney has notified people (credit reporting agencies) that this information is incorrect. What about a defamation of character lawsuit against these organizations?

] Lt. Colonel Stevens: We haven't explored that.

Rep. Tanner: There has to be some responsibility on their part not to publish incorrect information. I hope you will explore that.

Rep. Shaw (looking at a newspaper article provided by Lt. Colonel and Mrs. Stevens): This article states that the SSN requirement at the commissaries is founded in law. I think that is false and we will get an answer to that question.

Rep. Collins: In some states you have option regarding the SSN on your driver's license.

Rep. Shaw: I think we also need to look into why the statement "not be used a form of identification" was taken off the Social Security card.

<u>The following are items of importance from Associate Director Bovbjerg's testimony:</u>

<u>Barbara D. Bovbjerg, Associate Director, Education, Workforce and Income Security Issues, Health, Education and Human Services Division, United States General Accounting Office</u>

- Overview
  - Over 277 million individuals have a unique SSN
  - Perceived widespread sharing of personal information and occurrences of identity theft have raise public concern.

- Testimony will provide information about how the SSN is currently used. This information is based on findings from a study we conducted for this Subcommittee during 1998 *(Social Security: Government and Commercial Use of the Social Security Number Is Widespread, GAO/HEHS-99-28, February 16, 1999)* and recent work conducted to update our information.

- Federal laws and regulations require and restrict certain SSN uses
  - A number of federal laws and regulations now require the use of the SSN to track participation in a variety of federal programs
    - Internal Revenue Code and other regulations require that individuals' SSN serve as taxpayer identification numbers
    - Social Security Act requires individuals to provide their SSNs in order to receive benefits under the SSI, food stamp, TANF, and Medicaid programs
    - States are required to use SSNs to maintain records of individuals who owe state-ordered child support or are owed child support and to collect from employers reports of new hires identified by SSN
  - Use of the SSN generally limit its use to the statutory purposes described in each of the laws
  - In addition, the Privacy Act of 1974 also restricts federal agencies in collecting and disclosing personal information, which includes SSNs
    - Act requires federal agencies that collect information from individuals to inform the individuals of the agencies' authority for requesting the information, whether the information is optional or mandatory, and how the agencies plan to use the information
    - The act also prohibits federal agencies from disclosing information without individuals' consent, but does not apply to other levels of government or to private business
- Governments and businesses use SSNs extensively
  - State agencies
    - States use SSNs to support state government operations and offer services to residents
      - All states that have personal income tax use SSNs to administer their programs (according to an official at an organization representing state tax administrators)
      - State driver licensing agencies are more likely to use SSNs to exchange data with other organizations than to support internal activities
        - The federal Drivers' Privacy Protection Act now prohibits states from disclosing personal information for purposes such as surveys, marketing, and solicitation without the express consent of the individual
  - Health care services organizations
    - Officials representing hospitals, an HMO, and a health insurance trade association told GAO that their organizations always ask for an SSN, but they do not deny services if a patient refuses to provide the number
      - Officials from a hospital and an HMO said they assign patients other identifying numbers, which they use internally as the primary identifiers – the SSN is used as a backup to identify records if a patient forgets or does not know the patient number

        - Hospitals and HMOs use SSNs to track patients' medical care across multiple providers – helps establish a patient's medical history and avoids duplicate tests
        - Representative from a health insurance trade association said some health insurers use the SSN or a variation of the number as the customer's insurance number
            - Insurers and providers frequently match records among themselves, using SSNs to determine whether individuals have other insurance – allows insurers to coordinate payment of benefits
    - Health care providers may also use SSNs to gather information that is not directly relevant to a patient's health care
        - One hospital official said they plan to use SSNs during the admission process to obtain on-line verification of patients' addresses
- Financial services businesses
    - SSNs are one of the principal identifiers credit bureaus use to update individuals' credit records with the monthly reports of credit and payment activity creditors send them
    - Credit bureaus use SSNs that are provided by customers to retrieve credit reports on individuals
    - Credit bureau officials told GAO that customers are not required to provide SSNs when requesting reports, but requests without SSNs need to include enough information to identify the individual
    - Businesses such as insurance companies, collection agencies, and credit grantors use SSNs to request information about customers from credit bureaus
- Businesses that sell personal information
    - Continuing advances in computer technology and the ready availability of computerized data have spurred the growth of information brokers who amass and sell vast amounts of personal information, including SSNs, about members of the public
    - Federal law does not prohibit these businesses from disclosing SSNs
    - Examples of the information they buy include public records of bankruptcy, tax liens, civil judgments, real estate ownership, driving histories, voter registration, and professional licenses – the purchase may include SSNs
- Business and state officials believe federal laws restricting uses of SSNs would have a negative effect on their activities and programs
    - Officials from the businesses and agencies GAO contacted said that federal restrictions on using SSNs could hamper their ability to conduct routine internal activities and their ability to exchange date
    - Also told GAO that such action could impede state tax agencies' ability to identify those who file taxes, make it difficult to associate tax return information received from other tax agencies with tax information reported by residents, and make it more difficult for states to link driver license applicants to traffic violations they may have acquired under other state licenses
    - Because of privacy concerns raised by the disclosure of personal information, some businesses and sates have voluntarily restricted their disclosure of such information, including SSNs

- Some states are discontinuing practices that result in routine disclosure of SSNs
- SSA has stated that the expanded use and misuse of SSNs poses an administrative burden for the agency
    - According to agency officials, widespread use of SSNs as identifiers requires SSA to meet more requests for SSN verification from employers and government agencies
    - The disclosure of SSNs increases instances in which the agency must issue individuals new SSNs when theirs are being misused by another party
- Concluding observations
    - The widespread use of the SSN is permissible under existing laws and regulations, but because it provides a means to build and share databases of personal information, it creates privacy concerns and enables the growing problem of identity theft
    - Although restricting the use of SSNs may slow or reduce wide dissemination of personal information, such an action could also restrict commercial and public sector activities
        - Such effects could be temporary – until a new means of identifying unique personal records was devised
    - In an increasingly electronic world, protecting privacy will continue to be a public policy challenge

The following questions were put forward by the members of the Subcommittee:

Rep. Tanner: There was a case in Tennessee involving birth certificates and SSNs – what should they do?

Associate Director Bovbjerg: I must caution you that I am not a law enforcement officer. They should contact law enforcement, no single federal agency has authority in this area. The FTC has been given more authority.

Rep. Tanner: Is your answer the FTC?

Associate Director Bovbjerg: I believe that would be a good place to start.

Rep. Tanner: Do you have any suggestions on how Congress should approach this issue?

Associate Director Bovbjerg: I don't have an answer. It is an emerging problem that needs more federal attention and more policy attention.

Rep. Tanner: I think it is good to have this hearing. I think we can do some good work.

Rep. Portman: Thank you for your testimony. Regarding the option SSN on your driver's license – I have a letter from the Ohio Bureau of Motor Vehicles that I would like to submit for the Record. Do you have any feedback on how this is working?

Associate Director Bovbjerg: It is permissible to put SSNs on licenses, but states cannot sell that information without permission from individuals.

Rep. Portman: What are the current penalties at the federal level?

Associate Director Bovbjerg: I don't know, perhaps the IG will. I do know that they have expanded.

Rep. Portman: What if someone refuses to give their SSN, can a business decline service to you?

Associate Director Bovbjerg: I know that some do, banks for example.

Rep. Collins: In review of SSN misuse what did you find about EITC misuse?

Associate Director Bovbjerg: Our study didn't address misuse.

Rep. Collins: I think that is something that should be looked into.

The following are items of importance from the testimony of Inspector General Huse:

The Honorable James G. Huse, Jr., Inspector General, Office of the Inspector General, Social Security Administration

- Evolution of the SSN
  - SSN was never intended to be a "national identifier," but over the years, the SSN has become the "de facto" identifier for Federal and State Governments
  - The introduction of the SSN into the stream of electronic commerce has been accompanied by a dramatic rise in SSN misuse
    - The OIG is acutely aware of this problem due to the large number of SSN misuse allegations received by our Fraud Hotline and by the increasing number of requests for constituent assistance received from Congressional offices
      - In FY 1999, the Fraud Hotline processed over 75,000 allegations
      - Over 80 percent of the allegations and referrals made to our office involve the misuse of an SSN
        - Specifically, 32,000 had SSN misuse implications involving SSA programs and an additional 30,000 represented SSN misuse allegations with no direct program implication
- SSN misuse and SSA's programs and operations
  - Our work has revealed that certain misuse occurs because of vulnerabilities in SSA's processes
    - The OIG has investigated numerous cases where individuals apply for benefits under erroneous SSNs
    - Our office has also uncovered situations where individuals counterfeit SSN cards for sale
    - From time to time, we have even encountered SSA employees who sell legitimate SSNs for hundreds of dollars
    - Have seen examples where SSA's vulnerabilities in its enumeration business process adds to the pool of SSNs available for criminal fictitious identities
    - We have conducted numerous undercover operations regarding trafficking in SSA cards and numbers
    - Prioritized SSN misuse cases where there is a material impact on the SSA's Trust Funds, such as benefit application cases
    - Unyielding in our commitment to root out employee fraud and abuse in the SSN arena
      - Pleased that SSA employee fraud cases in this area have been few and far between
  - Preventing SSN misuse will provide the greatest cost benefit to the Agency
    - Once an improperly issued SSN enters the stream of commerce, there is scant hope for preventing subsequent damage
    - Share some of our suggested preventative measures

- May 1999 we issued a Management Advisory Report entitled *Using Social Security Numbers to Committee Fraud*
  - Report detailed cases in which the Agency issued SSNs based on fraudulent documentation
    - The improperly issued SSNs were used to commit identity crimes
  - We recommended that SSA incorporate preventative controls in its Modernized Enumeration System and as a result, SSA is developing automated edits within the system to identify transactions that have the greatest potential for fraud
    - This systems upgrade will alert employees to suspicious SSN applications, which they can then refer to the OIG for investigation
- This month, we released a follow-up report that further examined SSA's procedures for examining evidentiary documents
  - Draft audit report entitled, *Review of the Social Security Administration's Procedures for Verifying Evidentiary Documents Submitted with Original Social Security Number Applications*
  - Draft report concludes that SSA needs stronger procedures and better tools to verify evidentiary documents
    - Specifically, we will be recommending that SSA employees obtain independent verification of alien evidentiary documents, prior to issuing SSNs
    - Also recommending that SSA accelerate negotiations with INS and the State Department o implement an "Enumeration at Entry" program; that SSA not mail new SSNs to a post office box; and that SSA employees receive work credit and recognition for fraud detection and development
- Have also determined that there is a direct correlation between SSN misuse and SSA's responsibility to maintain accurate earnings records for individuals
  - When SSA cannot reconcile SSNs and identifying information provided by employers, SSA sends notices to wage earners requesting pertinent information to resolve the discrepancy
    - Most of the responses are returned "undeliverable – addressee unknown" to SSA
- SSN misuse and its impact on the public
  - SSN theft has a substantial impact on the lives of private citizens, as well as private industry
    - Theft of SSNs is becoming more prevalent as a result of today's electronic environment which has facilitated easy access to individuals' SSNs and other personal identifying information
  - Passage of the *Identity Theft Act*
    - Provided the OIG with additional tools to fight SSN theft
    - OIG has been in the forefront of the Federal Government's efforts to fight identity theft crimes
      - The OIG, in conjunction with the U.S. Attorneys' Office in Milwaukee, Wisconsin, was responsible for one of the first criminal prosecutions under this new law

- Waverly Burns, an SSI recipient, had commandeered another person's SSN
  - Used the stolen SSN to secure employment as a cleaning crew supervisor
  - While on the job, he stole over $80,000 in computer equipment from the offices of the Wisconsin Supreme Court
  - The stolen SSN was used to obtain a State of Wisconsin identity card, to open bank accounts in the victim's name, and to file fraudulent tax returns
  - Mr. Burns continued to falsely represent to SSA that he was disabled and unemployed – indeed there were no earnings appearing under his true SSN
  - On May 5, 1999, OIG special agents arrested Mr. Burns after tracking him to Chicago
  - He was sentenced to 21 months in prison and ordered to pay over $62,000 in restitution
- The OIG would like to pursue the thousands of potential identity theft cases received each month
  - With less than 300 investigators nationwide we lack the investigative capacity to handle the entire volume of identity theft referrals
    - Forced to focus on major cases that directly impact on SSA's operations such as the Wisconsin case
    - Also work collectively through task forces with other law enforcement agencies to make the most efficient use of resources
    - One of the toughest challenges is to find realistic strategies to fight this battle in an effective and efficient manner, while remaining focused on SSA's programs
  - Office of Investigations launched an SSN misuse pilot operation in five major American cities last summer
    - Partnered with Federal and State law enforcement agencies to target identity crimes and SSN misuse
    - In less than one year, we have opened 125 investigations which have resulted in 30 convictions to date
  - Developing for our FY 2002 budget submission, an integrated model that combines the talents of our auditors, investigators, and attorneys
    - If authorized, this group will focus its efforts on developing patterns and trends to better target our audit work, refer cases for investigation, and liaison with other relevant public and private sector entities
    - We need to focus audit and investigative attention where there is:
      - An apparent failure of SSA's business processes for issuing SSNs;
      - An apparent failure in SSA's wage and reporting systems;
      - A suspicion that SSN cards are being counterfeited;
      - Concealment of work activity using false identifications to obtain or maintain eligibility for Federal benefits
- Possible solutions
  - Several suggestions for SSA and Congress to consider, in addition to our formal audit recommendations discussed previously**:**
    - Regulating the sale of SSNs;

- Prohibiting businesses from refusing services for nondisclosure of an SSN when not relevant to the services being provided;
- Requiring photo identification when conducting business with SSA;
- Urging the implementation of new technologies and data bases to help employers, Government, and private industry verify that names and/or SSNs are correct to improve the identification process;
- Legislating statutory law enforcement authority for our investigators;
- Broadening civil monetary penalty authority for the sale or misuse of an SSN

- When SSN misuse compromises SSA business processes and the Social Security Trust Funds, involvement of the OIG is necessary and vigorous
  - To focus on our mission, we make tough choices to ensure that we bring the most benefit to SSA
    - Often we become the court of last resort for victims of identity theft
    - Would appreciate the Subcommittee's view on how to fulfill the role that the public seems to expect from SSA and this OIG

The following questions were put forward by the members of the Subcommittee:

Rep. Shaw: In your 6 point solutions, you recommended regulating the sale of SSNs. Should we even allow this? It seems like there's nothing but mischief involved in this.

Inspector General Huse: There are databases maintained by businesses.

Rep. Shaw: Is there any legitimate reason why this information is sold?

Inspector General Huse: No.

Rep. Johnson: Federal law requires the SSN for food stamps, Medicaid, etc.

Inspector General Huse: It is very difficult to keep track of beneficiaries. The SSN is really what sorts us out.

Rep. Johnson: In Texas we use the driver's license number not the SSN for identification. Is this a problem?

Inspector General Huse: Not at all – but there are some business costs associated.

Rep. Johnson: With the advent of the Internet do you see more instances?

Inspector General Huse: The numbers are increasing significantly each year. Tens of thousands of each year – for the five years we've been in existence.

Rep. Johnson: How do we slow it down, without saying we can't use the SSN for I.D.?

Inspector General Huse: Everyone is very careful not to say that the SSN is the national identifier, but it is. We need to have aggressive deterrents, and see that the laws are enforced. We need to make it a priority. It is hard to get to the bottom of what is actually lost – "value of reputation." We often become the court of last resort when people are turned aside by other courts because the threshold of loss is not reached. Maybe not criminal prosecution but sanctions could be used.

Rep. Shaw: What about case law?

Inspector General Huse: I will submit an answer for the Record.

Rep. Shaw: Are SSNs recycled when people die?

Inspector General Huse: No, and there are still several hundred million SSNs left.

Rep. Tanner: How does your office interact with the FTC?

Inspector General Huse: We have a great relationship. The FTC acts as the clearinghouse. They refer cases that fall under our general jurisdiction. It is a close relationship, we both get a lot of victim reporting.

Rep. Tanner: How do you try to stop it?

Inspector General Huse: We investigate and bring cases to the Department of Justice. We focus on portions where SSA's and other government programs are being affected.

Rep. Tanner: Do you refer individual instances?

Inspector General Huse: Yes, and we also participate in task forces and pilot projects.

Rep. Tanner: What about the goal of processing 97% of SSN applications within 5 days? How can you do this? What about manpower and accuracy and the resources to do this?

Inspector General Huse: I suggested to SSA that this process is too fast. They need to slow down to verify, especially birth certificates.

Rep. Tanner: Most people getting SSNs are infants – it seems like a longer wait shouldn't matter to them.

Rep. Tanner: Do you have any suggestions regarding the testimony of Lt. Colonel and Mrs. Stevens? It seems like outrageous abuse by the system.

Inspector General Huse: The FTC has the ability to take in reports – civil authorities sanction. The same power should be applied to our investigative agencies – civil monetary penalties. I don't know if the FTC can. We are asking for our authority to be expanded.

Rep. Portman: Following up on your recommendations – broadening CMPs for misuse – can you give us your specifics? Do we need to legislative authority for your investigators regarding the SSN issue?

Inspector General Huse: It is at the front end of this process, we can't cross-task force under the current rules.

Rep. Portman: The idea of a photo identification when conducting business with SSA is a good one – but what if a person has no photo identification?

Inspector General Huse: It is not a common practice in field offices – someone became a rep payee without identification, it was done over the phone.

Rep. Portman: How do we cut down on fraud in other areas and reconcile this with the trend of more online services?

Inspector General Huse: Of necessity it will limit e-commerce.

Rep. Cardin: Thank you for your testimony. We will concentrate on your recommendations. What about H.R. 1450, Mr. Kleczka's legislation which prohibits the sale of SSNs?

Inspector General Huse: I have reviewed the legislation. It is effective and a good start.

Rep. Shaw: The misuse of SSNs – growing problem. What percentage of cases are brought to your attention?

Inspector General Huse: We are receiving more and more allegations on the Hotline.

Rep. Shaw: How do people know how to get in touch with you?

Inspector General Huse: That is also growing (awareness) – more people are aware of the Hotline.

Rep. Shaw: Would you submit for the Record figures (instances of misuse) for the first 4-5 months of this year?

Inspector General Huse: I also want to say that there were federal laws in effect in 1997. Lt. Colonel and Mrs. Stevens were told that there were not. I also want to add that the OIG only has 300 agents and that the principle mission of these agents is program fraud.

Copies of the witnesses' written statements are available. Please contact us if you have any questions or would like copies.

The Washington Report
418 C Street, NE
Washington, DC 20002
202-547-8530/FAX 202-547-8532
Contact: Sara Garland or Rachel Emmons
e-mail: sarag@mail.greystone-group.com or rachele@mail.greystone-group.com