PROTECTING SOCIAL SECURITY NUMBERS FROM IDENTITY THEFT

Background

The Social Security Administration estimates that approximately 227 million individuals currently have Social Security numbers (SSNs).1 Because both government agencies and private businesses use SSNs for a wide range of non-Social Security purposes, the SSN has become a de facto national identifier.2 For this reason, SSNs are much sought after by identity thieves, who use these numbers to assume the identity of another individual and commit fraud. With an estimated 10 million individuals being victimized by identity theft each year, preventing identity thieves from obtaining SSNs is increasingly essential to helping protect individuals from fraud.3

A recent Government Accountability Office (GAO) report examining how SSNs are used in the public sector found that federal, state, and local government agencies use them for a variety of non-Social Security purposes, including identity verification, data sharing, research, and the administration of programs that deliver services and benefits to the public.4 This creates numerous documents and records that contain SSNs, many of which are available to the public for inspection.5 In addition, some government agencies print SSNs on individual eligibility and identification cards, making it easier for identity thieves to gain access to this key number.

The private sector also uses SSNs extensively as a means to identify an individual’s records in a database and as an authenticator to confirm the identity of an individual.6 SSNs are often used by financial service companies to link individuals to their accounts and, as a result, they are highly valuable to would-be identity thieves.7

---

2 Testimony of Patrick P. O’Carroll, Jr. (inspector general for the Social Security Administration) before the U.S. House of Representatives Committee on Ways and Means, Subcommittee on Social Security (June 15, 2004).
3 Testimony of J. Howard Beales, III (director of the Bureau of Consumer Protection, Federal Trade Commission) before the U.S. House of Representatives Committee on Ways and Means, Subcommittee on Social Security (June 15, 2004); testimony of Barbara D. Bovbjerg, op. cit.; testimony of Patrick P. O’Carroll, Jr. (June 15, 2004), op. cit.; testimony of James X. Dempsey (executive director, Center for Democracy & Technology) before the U.S. Senate Committee on the Judiciary (April 13, 2005).
5 These public records are a major source of SSNs for information resellers; see Testimony of Barbara D. Bovbjerg (June 15, 2004), op. cit.
6 Testimony of James X. Dempsey (April 13, 2005), op. cit.; see also Smith, R. E. “Identity Theft Happens Mainly in America.” Privacy Journal 31 (5) (March 2005). Because the SSN is exclusive to each individual, it is considered to be a more accurate identifier than an individual’s name or address, which may be shared with other individuals or change over time. Similarly, credit reporting agencies use the SSN as the primary identifier to sort and retrieve credit file information. However, many experts consider the use of SSNs as “authenticators” in the same way one would use a personal identification number (PIN) to be a poor security practice because of widespread and easy access to these numbers.
7 Almost half of large financial institutions use SSNs for verification purposes, according to a recent study by Unisys Corp.; see Krim, J. “Net Aids Access to Sensitive ID Data.” Washington Post (April 4, 2005).
Widespread Access to SSNs

The widespread use of SSNs in both the public and private sectors, combined with their key role in identity theft, has raised important concerns about the ability of identity thieves to gain access to the SSNs of others.

SSNs are relatively easy to access by inspecting paper records such as court and property documents held by various state and local government agencies. According to the GAO report, up to 28 percent of counties make records containing SSNs available over the Internet, greatly enhancing access to them. SSNs are most often collected by state and local governments for verification purposes rather than as a requirement of law or regulation.

Eligibility and identity cards issued by federal agencies to individual employees, program beneficiaries, and military personnel often display SSNs. Because individuals must carry such cards routinely, the cardholder is at risk for identity theft through accidental loss, theft, or visual exposure of the card. For example, some 42 million Medicare cards display SSNs. Currently, the federal government does not have a uniform policy concerning the display of SSNs on these types of cards.

A major issue is the availability of SSNs through information brokers who sell sensitive personal information, including SSNs, over the Internet for modest fees. One investigation used a simple Web search to reveal over a dozen Internet sites offering a variety of personal information for sale. While information brokers maintain that they only sell this information to those who have a legal right to obtain it, the investigation found that safeguards were easily evaded.

Another concern is the use of SSNs on eligibility and identification cards by universities and insurance companies. As discussed above, this puts cardholders at risk for identity theft through accidental loss, theft, or visual exposure of these cards. Further, a number of university databases have been breached recently, potentially providing identity thieves with the SSNs of large numbers of students and alumni.

Policy Options to Protect SSNs

A number of policy options have been proposed at both the state and federal levels to strengthen SSN protections.

8 U.S. Government Accountability Office (November 2004), op. cit. On the other hand, SSNs generally are not available to the public in records held by the federal government, as disclosure of this information is restricted under the Privacy Act of 1974.
9 Ibid. In addition, eight million Department of Defense identification cards and seven million Department of Veterans Affairs identification cards display SSN information. Further, an estimated 830,000 federal employees carry health insurance cards that display their SSN. Many government agencies, such as the Department of Defense, Veterans Affairs, and Office of Personnel Management are taking steps to remove SSNs from these cards.

10 Krim (April 4, 2005), op. cit.
12 Non-public data from financial records cannot be sold or transferred without giving individuals a chance to opt out. There are several exceptions, however, including employment checks, for tax filing, or to process a financial transaction. Krim (April 4, 2005), op. cit.; Web browsers may also allow skilled computer users to access financial data, including SSNs, because many companies are engaged in “virtual hosting” of documents online. A virtual host provides Web services that include server functions and Internet connection services and is often used by companies that do not want to purchase and maintain their own Web servers and Internet connections. See Enterprise Security Today. “Social Security Numbers Easy to Find Online” (April 8, 2005); Jardin, X. “Your Identity, Open to All.” WWW.Wired.com (May 6, 2005).
Limiting the Display of SSNs

A recent AARP survey of adults age 50 and older indicates strong opposition to the display of SSNs on many types of identity and eligibility cards (see Table 1).

Table 1: Percent of Adults Age 50+ Who Want SSNs to Appear on Various Documents

<table>
<thead>
<tr>
<th>Document</th>
<th>Yes</th>
<th>No</th>
<th>No Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver’s License</td>
<td>10</td>
<td>87</td>
<td>3</td>
</tr>
<tr>
<td>Passport</td>
<td>15</td>
<td>79</td>
<td>6</td>
</tr>
<tr>
<td>Medicare Card</td>
<td>25</td>
<td>70</td>
<td>5</td>
</tr>
<tr>
<td>Medical Records</td>
<td>32</td>
<td>65</td>
<td>3</td>
</tr>
<tr>
<td>Health Insurance Card</td>
<td>21</td>
<td>77</td>
<td>2</td>
</tr>
<tr>
<td>Credit Report</td>
<td>15</td>
<td>81</td>
<td>4</td>
</tr>
<tr>
<td>Work/Student ID</td>
<td>6</td>
<td>91</td>
<td>3</td>
</tr>
<tr>
<td>Hunting/Fishing License</td>
<td>2</td>
<td>96</td>
<td>2</td>
</tr>
</tbody>
</table>


Removing SSNs from the myriad other publicly available documents is likely to be difficult and costly, however. A 2002 cost estimate by the Congressional Budget Office (CBO) found that the cost to state and local governments of complying with a ban on the display of SSNs on publicly available documents would likely be significant because of the pervasive use of SSNs. As a result, the proposed legislation cited previously would not mandate a complete ban of SSNs on all publicly available government documents without first considering the cost of doing so.17

Limiting the Sale and Purchase of SSNs

The Social Security Administration’s inspector general has noted that, “As long as criminals can buy a list of names and SSNs through an Internet auction, we will continue to be plagued by the consequences.” Proposed legislation would limit the sale and purchase of SSNs in the private sector by requiring an individual’s affirmative consent before his or her SSN could be sold. A related proposal includes banning the sale of SSNs by credit reporting agencies unless they are included as part of a full credit report. This would restrict the sale of SSNs by credit reporting agencies to instances where there is a permissible purpose, as defined under the Fair Credit Reporting Act (FCRA). The CBO estimates the cost to the private sector of limiting the sale and purchase of SSNs to be minimal.20

15 For example, S. 1332 and S. 29 were introduced in the 109th Congress.
17 The legislation would require an assessment of the costs of truncation, redacting, or removal of SSNs.
18 Testimony of Patrick P. O’Carroll, Jr. (June 15, 2004), op. cit.
19 Permissible purposes for obtaining a credit report from a credit reporting agency include establishing a consumer’s eligibility for credit, insurance, rental housing, and employment and for background checks in certain circumstances.
20 Congressional Budget Office (July 10, 2002), op. cit.
Preventing Businesses from Requiring SSNs as a Condition of Doing Business

Many experts cite the widespread misuse and overuse of SSNs.21 This policy option would restrict unnecessary or inappropriate collection of SSNs when consumers purchase goods or services. Such proposals generally make exceptions for cases where a SSN is required under federal law or is deemed necessary for the business process, such as to identify the individual or to prevent fraud.

Increasing Security for Legally Collected SSNs and Enhancing Penalties for Illegal SSN Disclosure

Recent data breaches indicate that databases containing legally collected SSNs are often inadequately protected against accidental or intentional disclosure.22 Security enhancements could include requiring SSNs transmitted via the Internet to be encrypted, preventing inmates from accessing SSNs, and requiring entities that maintain SSNs and other personal data to establish internal policies that ensure the security and confidentiality of such records.23 Enhanced criminal and civil penalties for SSN misuse have also been proposed to ensure that they reflect the increasingly serious nature of identity theft crimes and to deter violations by individuals and organizations.

Summary

The use of SSNs as an identifier and an authenticator makes these numbers highly desirable to identity thieves. Because many gaps exist in current protections, these valuable numbers are at risk of theft by criminals. Recent national surveys indicate that the public is increasingly concerned that personal information will be stolen, which has negatively affected purchasing decisions, especially on the Internet. Further, a significant majority believe stronger laws and business practices are necessary to ensure that SSNs are adequately protected.24

21 Testimony of James X. Dempsey (April 13, 2005), op. cit.; testimony of Patrick P. O’Carroll, Jr. (June 15, 2004), op. cit.
23 An example of such requirements is the Office of the Controller of the Currency’s Interagency Guidelines establishing standards for safeguarding customer information.
24 Privacy & American Business and Deloitte & Touche LLP. “New Survey Reports and Increase in ID Theft and Decrease in Consumer Confidence” (June 29, 2005); Sullivan, B. “Data Leaks Stunt E-Commerce, Survey Suggests.” MSNBC.com (June 15, 2005).