



September 5, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex K)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: SSNs IN THE PRIVATE SECTOR – COMMENT, PROJECT NO. P075414

To Whom It May Concern:

Consumers Union¹, the non-profit publisher of *Consumer Reports*[®] submits these comments in response to the Federal Trade Commission's inquiry regarding the use of social security account numbers (SSNs) by the private sector.²

Our comments provide an overview of the vulnerabilities created by the widespread use, sale, purchase, display and solicitation of social security numbers; the results of a Consumers Union (CU) August 2007 nationally representative poll on consumer attitudes regarding data protection, identity theft and use and solicitation of SSNs; and recommendations for policy improvements to mitigate the risks created by widespread use and trade in consumers' SSNs.

SUMMARY

The connection between SSNs and identity theft and the dangers and limitations of over-reliance on the number as an identifier and authenticator has been well-established. Consumers Union's survey results augment these prior research findings. The poll found that consumers are regularly asked for their SSN by businesses that don't have a clear need for it. Although consumers well understand the vulnerabilities associated with giving their SSN to others, most provide it when asked out of fear for the consequences of refusing. Many consumers believe their sensitive information held by others is not secure and support obligations to protect that data and to provide remedies to consumers when security is breached. The data also suggest that SSNs are widely used as identifiers and passwords, despite their inherent limitations for those purposes. In addition, the poll found that other ID theft vulnerabilities remain due to inclusion of the SSN on cards that consumers carry in their wallet and on postal mail they receive. Finally, federal and state policy makers should adopt new restrictions on the solicitation, use and sale of SSNs and strong requirements for breach notification. These measures not

Consumers Union
Headquarters Office
101 Truman Avenue
Yonkers, New York 10703-1057
(914) 378-2029
(914) 378-2992 (fax)

Washington Office
1666 Connecticut Avenue, NW
Washington, DC 20009-1039
(202) 462-6262 Suite 310
(202) 265-9548 (fax)

West Coast Regional Office
1535 Mission Street
San Francisco, CA 94103-2512
(415) 461-6747
(415) 431-0906 (fax)

South West Regional Office
1300 Guadalupe, Suite 100
Austin, TX 78701-1643
(512) 477-4431
(512) 477-8934 (fax)

only reduce ID theft vulnerabilities, they are policy measures consumers overwhelmingly support.

I. WIDESPREAD USE, SOLICITATION & AVAILABILITY OF SSNs INCREASE CONSUMER VULNERABILITY TO IDENTITY THEFT.

Social security account numbers are commonly used by businesses to both identify a person (determine the identity of a customer) and authenticate the identity of individuals (determine that the customer is the person he or she claims to be).³ Social security account numbers, either alone or in combination with portions of a consumer's name, phone number or other personal information, provide the key to a consumer's financial identity, allowing identity thieves possessing this information to open up new accounts in the consumer's name or perpetrate other fraud.⁴ The widespread commercial use and availability of SSNs as both authenticators and identifiers has been associated with increased vulnerability to ID theft.⁵

Consumers are frequently asked by businesses and government to provide their SSN, but not all businesses who ask for the SSN have a clear need for the number. Businesses providing credit or related financial services and healthcare providers serving Medicare or Medicaid beneficiaries may have a legitimate need for the SSNs to evaluate the credit worthiness of an applicant or the eligibility or status of a beneficiary, respectively. Healthcare providers serving Medicare beneficiaries must collect the SSN because it still appears on patients' Medicare cards. But even those with an initial legitimate need for the number are not restricted from using it for other purposes. In addition, many other types of businesses routinely ask consumer to provide their SSNs when its use may be convenient but unnecessary.⁶ Consumers may be asked for the SSN to join a health club, to donate blood, to purchase or activate a cell phone service, or simply to write a check. As the Inspector General of the Social Security Administration has testified, the increasing unnecessary use of SSNs increases the likelihood that the numbers will be inadequately protected and used by identity thieves.⁷

Financial institutions, data brokers and other businesses often assert the essential nature of the SSN in evaluating the creditworthiness of an applicant, ensuring the accuracy of credit reports, or providing or obtaining fraud prevention or detection services.⁸ Yet other information suggests that the numbers are used merely for administrative convenience. To the extent that the SSN is used for fraud-prevention or credit-related purposes, it is not necessarily effective in rooting out fraud or in ensuring accuracy of credit reports. Reported cases demonstrate that thieves can use another's SSN under a name that is *different* from that of the rightful account number holder and still obtain credit.⁹ In addition, frequent errors on consumer reports, such as even "innocent" attribution of another's credit history to the wrong consumer, strongly suggests that while existing use of the SSN for data-matching may be used to improve credit report accuracy, too often it falls short.¹⁰ Thus, the use of the SSN as an authenticator or for data matching is far from foolproof.

Ironically, it appears that the widespread reliance on the SSN for identity verification and fraud prevention is exactly why it is so valuable to identity thieves. Recognizing this risk, some entities are considering abandoning use of the SSN in favor of randomly assigned account numbers, demonstrating that not all uses of SSNs are essential. For example, beginning this fall, beneficiaries of the Federal Thrift Savings Plan will receive randomly assigned account numbers in place of their SSN, which had previously served as the account number, and is limiting further use of SSN.¹¹ In addition to the value of SSNs to thieves, they are easy for thieves to acquire. Because they are so widely used and available, SSNs are no longer secret—an essential element of an effective authenticator.

Section 7 of the Privacy Act requires federal agencies soliciting a consumer's SSN to disclose whether or not the individual must provide it, if it is required, under authority of what statute(s), and how it will be used. But the private sector faces no similar obligations. Thus, although the Social Security Administration advises consumers when asked for their social security number by a business to inquire why the number is needed; how it will be used; what happens if the consumer refuses to provide the number; and what law requires the consumer to provide the number,¹² federal law neither requires businesses to provide this information nor prohibits solicitation of the number or denial of the transaction if the customer refuses to provide it. Regardless, a disclosure-based approach is not an effective way to reduce the collection and circulation of sensitive data since, as our survey results will demonstrate, consumers fear the repercussions of refusing requests for their SSN. Moreover, for most businesses outside of the financial sector,¹³ no federal law requires the protection of this sensitive information once a business has collected it nor restricts how businesses may use or reuse the SSN or to whom they provide it, including even commercial resale of the SSN. The widespread and often unnecessary solicitation, use and commercial sale and purchase of SSNs, coupled with inadequate safeguards make consumers particularly vulnerable to identity theft.

Even businesses and government agencies that truncate SSNs leave consumers vulnerable to ID theft.¹⁴ First, because there is no uniform system of truncation—some entities truncate the first five digits, while others truncate the last four digits—thieves can reassemble the full SSN. Second, because only the last four digits of the SSN are unique to the individual, widespread use (as a password or authenticator, for example) and display (such as on pay stubs) of only the last four digits, also leaves consumers vulnerable to ID theft. Finally, because the Social Security Administration (SSA) has used date and location of issue to establish the first five digits, with access to just the last four in tandem with a little information about the individual and some guesswork, a thief can determine the full SSN. The SSA is currently proposing to randomize assignment of the first three digits to eliminate geographic significance, in part to reduce ID theft risks,¹⁵ but that will do little to protect individuals issued SSNs under the prior system of number assignment.

In addition to these vulnerabilities, SSNs are also widely available on the Internet, both in online public records as well as for sale by data brokers who have purchased the SSNs or harvested them from public records.¹⁶ For example, at www.secret-info.com, the

service offers a social security number to buyers who provide a name and address, all for the low fee of \$45. Buyers who provide just an SSN are offered the name and address for an even lesser fee. For at least some sites, buyers need offer little justification for their need for the SSN and sellers infrequently verify the purported use.¹⁷ In addition, SSNs are still used on identification cards, such as student or employee ID cards, as well as on Medicare cards – all cards that consumers may reasonably feel they must keep in their wallets. Such a use is unnecessary as other unique identifiers can be assigned to the card or account holder. In the event a wallet containing a card with the SSN is stolen, the consumer is made doubly vulnerable to ID theft—not only will the thief likely have the drivers license and credit cards of the victim, they will also have a key piece of information needed to open new accounts and access new credit. Finally, SSNs still appear in mail that consumers receive – making them vulnerable to identity theft when their mail is stolen.

II. POLL RESULTS DEMONSTRATE FREQUENT SOLICITATION OF SSNS AND STRONG CONCERN ABOUT SSN USE, SOLICITATION AND SECURITY

Between August 16 -19, 2007, Consumers Union commissioned a nationally representative random survey of telephone households comprising more than 1,000 adult consumers regarding their attitudes and experiences about data protection, security breaches, identity theft and social security numbers. The full survey results are attached.

a. Consumers Demonstrate Strong and Growing Concern About the Security of Their Personal Financial Data, Including SSNs.

Consistent with other public poll findings, CU’s poll found significant concern regarding identity theft—defined as misuse of personal and financial information to make purchases or access credit in the consumer’s name. Nine out of ten consumers (91%) expressed concern about identity theft, with more than four in ten (42%) being “very concerned.” Not surprisingly, an even greater percentage of consumers who had already been victims of identity theft expressed greater concern than others: More than six in ten (62%) said they were very concerned.

Consumer experience with identity theft is likewise high: Nearly one-quarter (23%) of those surveyed had been victims of ID theft or had family members who had been victimized in the past five years, amounting to some 51 million American adults with personal experience with ID theft. Victims or those who had a family member victimized were disproportionately high income, female and under age 55.

The Consumers Union poll also found that consumer concern with the security of their personal financial information is strong and growing. Nearly three in ten (29%) viewed the current level of security of their sensitive information held by government or business as “unsafe.” Only one in nine believed the information was very safe. Understandably, those with personal experience with ID theft perceived the greatest security risk—with more than four out of ten (42%) classifying the level as “unsafe.”

Consumer concern regarding data security is growing. Four out of ten consumers said their confidence in the safety of their sensitive information had declined over the past several years. Only one in four said their confidence had grown.

b. Consumers are Frequently Asked for Their SSNs by Government and Businesses; SSNs Are Often Used for Identification and Authentication.

Consistent with government studies,¹⁸ the Consumers Union poll found that consumers are frequently asked for their SSNs by businesses and government entities. Nearly nine out of ten consumers (87%) were asked at least once for their full or partial SSN over the last year. Younger consumers (aged 18-34), those with incomes \$40,000 and over and those living in the West were more likely to be asked for the SSN than other consumers.

Companies providing credit or other financial services, including retailers issuing credit, were identified most frequently as requesting the SSN (60%). However, 82 percent of consumers reported requests from many other types of entities, some of which may not have a clear need for the SSN. Nearly half of consumers (49%) said a healthcare provider requested their SSN—far greater than the proportion of the population eligible for Medicare or Medicaid benefits where the SSN may be necessary to verify eligibility. Employers and potential employers asked 44 percent of consumers for their SSN. (Employers legitimately need the SSN to comply with federal tax and other laws.) In addition, consumers received requests for their SSNs from insurance companies (36%), government agencies other than the IRS and state tax bodies (32%), colleges and other schools (28%), service providers, such as cell phone or cable companies (26%), utilities (17%) and merchants or retailers (16%). Fifty-two percent of consumers, disproportionately women, were asked to provide a full or partial SSN for a child or other family member.

In addition, survey results suggest frequent use of the SSN for identification and authentication. Over the past year, more than four in ten (42%) consumers were asked over the telephone or via the Internet to provide their full or partial SSN. Thirty-eight percent reported a request for their SSN to identify themselves to a customer service representative over the telephone or Internet. And 20 percent reported being asked for their SSN to purchase goods or access services over the phone or the Internet. As noted in Section I, use of even a partial SSN may be an ineffective authenticator given the widespread availability of these numbers.

c. Consumers Understand the Sensitivity of their SSNs and are Reluctant to Share Them, but Most are Concerned About the Consequences of Refusing Requests.

Consumers understand the sensitivity of providing their SSN to others. More than nine in ten (91%) consumers agreed that they are more vulnerable to ID theft when a business has their SSN. Sixty-four percent strongly agreed. Among those who said they

were very concerned about identity theft, three in four (76%) believed business acquisition of their SSN increased their vulnerability.

Yet consumers reluctantly and only infrequently refuse to provide their SSN to a third party when asked. Nearly four in five consumers (78%) agreed that they'd prefer not to provide their SSN to other entities, but are concerned about the consequences of refusing. Over the past year, fewer than three in ten (28%) consumers refused to provide it. Concern about the consequences of refusal is understandable: Of those consumers who refused to provide the number, slightly more than one in three (35%) were denied the service or product they were seeking.

d. SSNs Frequently Appear on Cards that Consumers Carry with Them & Inclusion of SSNs in Mail Appears to be More Frequent Than Necessary.

In addition to frequent collection of SSNs, consumers' vulnerability to ID theft is exacerbated when the number is printed on cards that consumers carry in their wallets or purses. Our poll results show that elderly and low-income populations disproportionately carry SSN-bearing cards, increasing their vulnerability.

Among the overall population, more than half of all consumers (52%) report that they carry a card bearing their SSN. Nearly one in four (23%) report carrying a card, such as an employment or student ID card, a membership card or other card used to access goods or services, that bears the SSN. Consumers in the age cohort 18-34 are slightly more likely (26%) to carry such a card, which may reflect the use of SSNs on student ID cards. And one in three consumers (34%), disproportionately represented by those over age 65 or with incomes below \$40,000, report carrying their social security card. The frequency with which consumers' SSNs are solicited helps explain why consumers may carry their SSN cards. But even with greater consumer education about the risks of carrying their SSN card, a large number of consumers remain vulnerable to ID theft until other cards they need to routinely carry with them no longer bear their SSN.

The elderly, because they disproportionately carry cards bearing their SSNs are particularly vulnerable to ID theft if their wallets are stolen. Nine in ten elderly Americans (age 65 or older) carry something in their wallet with the SSN printed on it. Eighty-five percent of elderly Americans report that they carry their Medicare cards, which include the SSN and are necessary for receipt of medical services. Medicare cards are among one of the few government-issued cards that still bear the SSN. (Military ID and military-dependent cards also continue to bear the SSN.) And 46 percent of the elderly report that they carry their SSN cards.

Relative to the general population, lower income populations also appear at higher risk. Consumers with household incomes below \$40,000 annually were far more likely to carry their SSN card than higher income brackets—55% vs. 21% for households with incomes \$75,000 and greater. They were also more likely to carry another type of card bearing the SSN—28% vs. 22% for households with incomes \$75,000 and greater. And only one-fourth (26%) of consumers with incomes under \$40,000 report carrying *no*

SSN-bearing card, compared to more than half (56%) of consumers from \$75,000+ households who report carrying no such card.

Inclusion of the SSN in mail also increases consumers' vulnerability to ID theft since mail theft has been associated with ID theft. Over the past year, one in seven (14%) consumers received postal mail other than tax documents that include their SSN. The number is higher—one in five (21%)—for consumers in mid-range income households (\$40,000-\$74,999 annually).

e. Consumers Strongly Support Greater Restrictions on Solicitation & Use of, and Security of Their SSNs Held by Others.

Our poll results found that Americans overwhelmingly believe that their SSN is sensitive personal information that *they* should control, that others should safeguard, and the use and sale of which should be restricted. They also overwhelmingly support government action to better protect consumers from identity theft and inappropriate use of SSNs.

Consumers overwhelmingly wanted new restrictions on the use, sale and protections of their SSNs. Nearly all consumers agreed that:

- Companies should *not be allowed to sell* consumers' SSNs (96% total agreement, 95% strongly agreed)
- Companies that hold SSNs should be *required to protect* them (99% total agreement, 95% strongly agreed)
- *No one should be allowed to use* consumers' SSNs for any purpose without their permission (98% total agreement, 94% strongly agreed)
- Companies should *stop using SSNs to identify customers* (89% total agreement, 66% strongly agreed)

Consumers overwhelmingly want requirements for notification when a database containing their SSN has been breached and remedies when the security of their sensitive information is breached. Nearly all consumers agreed that:

- When the security of SSNs held by a business or government entity has been compromised, the agency or business should *always be required to notify affected consumers* (98% agree, 90% strongly agree)
- When a company or government agency fails to protect SSNs, consumers *should receive a remedy* to prevent ID theft (97% agree, 84% strongly agree)

Of those consumers who agreed that a remedy should be made available to SSN security breach victims, the most popular remedy identified was the *ability to freeze access to the consumers' credit files at no charge* (68% most preferred this remedy). Only 12 percent preferred free credit monitoring—the remedy that some businesses offer to their customers when they suffer a breach. This suggests that consumers want remedies that do not impose a burden on them to routinely monitor their credit files to prevent ID theft.

The freeze, unlike monitoring, allows a consumer to put in place a protection that requires no further activity to stop new account fraud. The freeze allows consumers to ensure that an identity thief can't open a new account that requires a credit check.

Consumers also overwhelmingly agree that lawmakers should adopt new protections to prevent ID theft. *Nearly all consumers agreed that:*

- Consumers should have the right to freeze access to their credit files to prevent new account fraud (97% total agreement, 85% strongly agreed)
- Federal and state lawmakers should pass laws restricting the use of SSNs. (89% total agreement, 65% strongly agreed).

III. POLICY RECOMMENDATIONS

Despite years of study and analysis¹⁹ and strong consumer concern, federal lawmakers have yet to enact privacy protections for social security numbers. With some limited exceptions that apply to government entities and some types of businesses, there are few restrictions on the solicitation, use, sale or purchase, or protection of social security account numbers. Though some states have taken steps to protect the privacy of SSNs, most measures are limited to addressing only some aspects of the SSN privacy problems.²⁰ Thus, federal and state law- and policy- makers should take the following steps to better protect consumers from identity theft by reducing the circulation of and over-reliance on the SSN and to get consumers' SSNs off the Internet, out of the wallet, out of the mail, out of the marketplace and to better protect consumers from identity theft:

a. Reduce ID Theft Vulnerabilities Through Improved SSN Privacy Protections

- Prohibit the solicitation and collection of SSNs with exceptions only where required by law or for the specific purposes of credit, tax compliance, employment or investment.
- Prohibit both public and private use of the SSN as a password to access goods or services and as a customer identifier. Use of the SSN as the sole means of identification should be prohibited.
- Where solicitation is permitted, prohibit use of the SSN for any purpose beyond the initial purpose for which the exemption was provided.
- Prohibit the transmission of SSNs over the Internet unless by secure connection.
- Prohibit the sale and purchase of SSNs subject to only limited national security, public health emergencies and other similarly narrow exceptions that clearly serve the public interest. Reducing SSNs as a commodity in trade will help reduce the overall circulation of SSNs and thieves access to them.
- Prohibit the public display of SSNs over the Internet; require governmental entities that display public records containing SSNs and located on the Internet to redact any SSNs. Going forward, public entities should redact SSNs before making public records available on the Internet and those filing documents should be required to redact prior to filing.

- Prohibit the printing of the SSN on Medicare and other government issued cards and on government or private identification cards, including student and employee ID cards; on membership or other cards used to access goods or services; on most postal mail; and on checks and pay stubs.
- Require all businesses that hold sensitive personal information, not just financial institutions, to adopt safeguards to protect it.
- Solicitation, collection or possession of SSNs and subsequent failure to protect them should be deemed an unfair trade practice and subject to explicit and tougher civil penalties than the Federal Trade Commission is currently empowered to assess.

b. Provide Consumers with Notice of SSN Security Breach and ID Theft Prevention Tools

- Require notice to all affected consumers when a private or public entity holding sensitive personally identifiable information, including SSNs, suffers a breach of that data, without risk-based exemptions, triggers or loopholes.
- Provide consumers with a permanent, low-cost, easy to use "security freeze"—the ability to prevent others from accessing their credit report. The security freeze prevents new accounts fraud by preventing creditors from accessing the consumers' credit file unless the consumer lifts the freeze using a secure PIN. Thus, identity thieves that have duped the provider cannot secure credit in another's name—preventing the most costly and difficult to detect form of identity theft. A security freeze also limits the burden placed on consumers by lax security practices in the private and public sectors: consumers can place the freeze and leave it there with no further monitoring and know that they will be protected from new accounts fraud.

c. Provide Resources for Education Regarding the ID Theft Risks Associated with SSN Use.

While education is never a substitute for statutory and regulatory protections, the federal and state governments should invest in education of both businesses and consumers regarding the risks associated with using the SSN.

- Invest in private sector education regarding the vulnerabilities that SSN use and display creates for the business itself, as well as its customers and employees. Reliance on SSNs as identifiers and authenticators may not only expose the business to greater risk of fraud by ID thieves that buy their goods and services using another's SSN, but they risk jeopardizing consumer trust and loyalty when sensitive information is breached. Employers who unnecessarily print the full or partial SSN on pay stubs or on mail sent to employees risk exposing their own employees to ID theft.
- Though our poll results demonstrate that consumers are well aware of the risks associated with solicitation and use of their SSNs by the public and private sector,

public investment in education regarding the risks of carrying the SSN card, targeted to vulnerable low-income and elderly populations that disproportionately do so, may also help reduce ID theft risk resulting from wallet theft.

IV. CONCLUSION

The extensive record built by both federal agencies and by Congress demonstrates the strong connection between identity theft and SSN use and display. The Consumers Union poll results confirm that SSN use and solicitation is widespread and demonstrate that while consumers are well aware of the dangers of SSN use, they feel powerless to refuse the requests that are in part responsible for the extensive circulation and trade in SSNs. Consumers overwhelmingly demand stronger SSN privacy protections and remedies for data breaches. Given industry reluctance to abandon use, collection and sale of these sensitive numbers, it is time for policy makers to step in to protect consumers against risky private sector SSN practices.

Respectfully,

/s/

Jeannine Kenney
Senior Policy Analyst

/s/

Gail Hillebrand
Senior Attorney

Attachment

END NOTES

¹ Consumers Union is a non-profit membership organization chartered in 1936 under the laws of the state of New York to provide consumers with information, education and counsel about goods, services, health and personal finance, and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. To maintain our independence and impartiality, Consumers Union accepts no outside advertising, no free test samples, and has no agenda other than the interests of consumers. Consumers Union supports itself through the sale of our information products and services, individual contributions, and a few noncommercial grants. Consumer Reports, Consumer Reports Online, and our health and financial newsletters, with more than 7.4 million paid subscribers, regularly carry articles on health, product safety, financial services, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare.

² Federal Trade Commission, News Release, "FTC Seeks Comments on the Uses of Social Security Numbers in the Private Sector: Goal to Reduce ID Theft," July 30, 2007, available at <http://www.ftc.gov/opa/2007/07/ssn.shtm>.

³ See, e.g., *Protecting the Privacy of the Social Security Number from Identity Theft Before the Subcomm. on Social Security of the H. Comm. on Ways and Means*, 110th Cong. (2007) (hereinafter *2007 Social Security Subcommittee Hearing*) (statement of Daniel Bertoni, Government Accountability Office, GAO-07-1023T, at 8 – 10) (statement of Marc Rotenberg, Electronic Privacy Information Center), available at <http://waysandmeans.house.gov/hearings.asp?formmode=detail&hearing=570>; see also *Enhancing Social Security Number Privacy Before the Subcomm. on Social Security of the H. Comm. on Ways and Means*, 108th Cong. 22-33 (2004) (statement of Barbara D. Bovbjerg, General Accounting Office) available at <http://waysandmeans.house.gov/hearings.asp?formmode=detail&hearing=153>.

⁴ See *2007 Social Security Subcommittee Hearing* (statement of Daniel Bertoni, Government Accountability Office, GAO-07-1023T, at 1.)

⁵ Jonathan Krim, *Net Aids Access to Sensitive ID Data*, WASH. POST, Apr. 4, 2005, at A1, available at www.washingtonpost.com/ac2/wp-dyn/A23686-2005Apr3?language=printer (George Washington University law school professor Daniel Solove called SSNs the "magic key" for identity thieves. He noted, "Anyone can easily find it [the Social Security number] out...It's used everywhere, and it's really hard to change if it falls in the wrong hands. How could you come up with a worse system?").

⁶ See, e.g., *2007 Social Security Subcommittee Hearing*, unofficial transcript, at 34, 36-37. Subcommittee Chairman McNulty noted that a merchant requested his social security number when the Chairman was merely purchasing an appliance with a personal check and provided other forms of identification. In that same hearing, Cong. Joe Barton noted that when he purchased a cell phone, he was required to provide his SSN to three different parties over a 30 minute period; see also, *2007 Social Security Subcommittee Hearing* (statement of Patrick O'Carroll, Inspector General, Social Security Administration), available at <http://waysandmeans.house.gov/hearings.asp?formmode=view&id=6145> ("...[S]chools, businesses, and State and local governments request SSNs for a multitude of purposes—very few of which are required by law. Rather, many of these organizations use the SSN as an identifier simply because it is convenient. For example, our auditors have looked at the use of SSNs by universities and hospitals as student and patient identifiers, respectively. While both of these types of organizations may have had some reason for collecting SSNs, such as financial aid or Medicare coverage, we found that once collected, the number was used too frequently for other purposes and not always given the level of protection necessary.")

⁷ See *2007 Social Security Subcommittee Hearing* (O'Carroll statement) *supra* note 6.

⁸ See, e.g., *2007 Social Security Subcommittee Hearing* (statement of Stuart Pratt, Computer Data Industry Association) available at <http://waysandmeans.house.gov/hearings.asp?formmode=view&id=6149>.

⁹ See, e.g., *2007 Social Security Subcommittee Hearing* (Rotenberg statement) *supra* note 4, at n.7 (citing cases of identity theft in which thieves obtained credit when credit issuers used the SSN for authentication despite discrepancies in the name, telephone number or address); see also, Aleksandra Todorova, *The Secret Life of Your Social Security Number*, SMARTMONEY.COM, July 8, 2004, <http://www.smartmoney.com/debt/advice/index.cfm?story=ssn2004> (recounting the case of a consumer whose SSN was used by another, under their own name, to take out several mortgages and car loans, creating two separate identities from a single SSN. Unfortunately, the debt collectors pursued the rightful card number holder owner); see also Beth Healy, *Credit Agencies Lag on Errors, Fraud* BOSTON GLOBE, Dec. 28, 2006, available at

http://www.boston.com/news/local/massachusetts/articles/2006/12/28/credit_agencies_lag_on_errors_fraud (recounting the issuance of credit to an individual applying under his own name but using another's SSN.).

¹⁰ For a summary of reports analyzing errors found in consumer credit files, *see generally*, FAIR CREDIT REPORTING (NAT'L CONSUMER LAW CENTER (2006)) at 88 - 90. One report found that persons with common last names experienced a 90 percent error rate in their reports, suggesting that the asserted existing use of social security numbers to properly match data does not prevent consumer reporting errors.

¹¹ *See* "Account Numbers Are Coming in October," <http://www.tsp.gov/curinfo/login/accountnumber.html>

¹² Social Security Administration, <http://www.ssa.gov/pubs/10002.html#protect>.

¹³ 15 U.S.C. §§ 6801-6809 (2000) (requiring financial institutions to adopt safeguards to protect customer information).

¹⁴ *See 2007 Social Security Subcommittee Hearing* (Bertoni statement) *supra* note 3, at 12-13.

¹⁵ Notice, Enhancing the Efficiency of SSA's SSN Assignment, 72 Fed. Reg. 36540 (Jul. 3, 2007).

¹⁶ *See, e.g.*, Krim *supra* note 5.

¹⁷ *See id.* ("Yet with only scant checks to verify whether someone requesting data is legitimate, several sites sell full Social Security numbers, potentially contributing to an epidemic of identity theft or fraud that touched about 10 million Americans in the past year.")

¹⁸ *See, e.g.*, *2007 Social Security Subcommittee Hearing* (Bertoni statement) *supra* note 3, (O'Carroll statement) *supra* note 6.

¹⁹ Congress has conducted 16 hearings in the past seven years on the issue of social security number privacy. *See 2007 Social Security Subcommittee Hearing* (statement of Rep. Michael R. McNulty, Chairman, H. Subcommittee on Social Security), *available at* <http://waysandmeans.house.gov/hearings.asp?formmode=view&id=6161>

²⁰ *See generally*, "Memo to State Legislators," Consumers Union, Aug. 6, 2007, http://www.consumersunion.org/pub/core_financial_services/004801.html (regarding state measures to protect SSNs). While the states have made a useful start, many state laws contain significant loopholes that reduce their effectiveness in protecting consumers from identity theft.