Security in Numbers

*** - ** - ****

SSNs and ID Theft

Federal Trade Commission Report

December 2008

Recommendations on Social Security Number Use in the Private Sector

I. Introduction

The President's Identity Theft Task Force ("Task Force") was established in May 2006 to develop a coordinated plan to prevent identity theft, help victims to recover, and prosecute the criminals who perpetrate it.[1] The Task Force issued its Strategic Plan, with 31 recommendations for action, in April 2007. One of those recommendations directed Task Force agencies to study the private sector uses of consumers' Social Security numbers ("SSNs"), develop a deeper understanding of the relationship between the SSN and identity theft, and explore approaches that would preserve the SSN's beneficial uses while curtailing its availability and value to identity thieves.[2]

This report answers the Task Force's mandate. Building on extensive fact-finding conducted by staff of the Federal Trade Commission ("FTC" or "Commission"), in cooperation with other Task Force agencies, the report examines the various private sector uses of the SSN and concludes with five specific FTC recommendations. These recommendations address both the supply and demand aspects of the SSN problem by proposing actions that would make SSNs less available to identity thieves, and would make it more difficult for them to misuse those SSNs they are able to obtain.

The Commission believes that the most effective course of action is to strengthen the methods by which businesses authenticate new and existing customers. Stronger authentication would make it more difficult for criminals to use stolen information, including SSNs, to impersonate consumers, thus devaluing the SSN to identity thieves and reducing the demand for it.

Limiting the supply of SSNs that are available to criminals, as a complement to improved authentication, although important, is more complex. SSNs already are available from many sources, including public records, and it may be impossible to "put the genie back in the bottle." Moreover, there is a danger that reducing the availability of SSNs would have unintended, adverse consequences. A number of important functions in our economy depend on access to SSNs. Businesses routinely rely on SSNs to ensure that the information they use or share with other organizations is matched to the right individual. Still, we believe it is feasible to reduce the availability of SSNs to identity thieves, such as by eliminating unnecessary public display, while preserving the legitimate and beneficial uses and transfers of SSNs. The Commission's five recommendations, detailed below in Section III, are:

- Improve consumer authentication;
- Restrict the public display and the transmission of SSNs;
- Establish national standards for data protection and breach notification;
- Conduct outreach to businesses and consumers; and
- Promote coordination and information sharing on use of SSNs.

II. Background

The SSN was created in 1936 for the purpose of tracking workers' earnings for benefits purposes.[3] Since that time, however, SSN usage has expanded to encompass a myriad of purposes well beyond the operation of the Social Security system. Financial institutions, insurers, universities, health care entities, government agencies, and innumerable other organizations use this nine-digit sequence as a default identifier to ensure accurate matching of consumers with their information within organizations, to facilitate matching of consumer information with other organizations, and to avoid having to establish a different identification system for each set of benefits or records. Many SSN uses have also been legally mandated. The Internal Revenue Service ("IRS"), for example, requires private sector entities, including banks, insurance companies, and employers, to collect SSNs for income and tax-related purposes. The numerous uses of the SSN reflect its considerable advantages as an identifier, because it is permanent, ubiquitous, and unique to each individual.

Many entities also use SSNs to authenticate consumers, *i.e.*, to verify that individuals are who they say they are. These entities, in effect, treat the SSN as a secret piece of information, available only to the consumer and themselves, and give access to information or benefits only when the consumer is able to supply and confirm his or her SSN.

This dual use of the SSN as identifier and authenticator has created significant identity theft concerns. SSNs often are described as the "keys to the kingdom," because an identity thief with a consumer's SSN (and perhaps other identifying information) may be able to use that information to convince a business that he is who he purports to be, allowing him to open new accounts, access existing accounts, or obtain other benefits in the consumer's name. Unfortunately, SSNs have become increasingly available to identity thieves, at least in part because they are so widely used as identifiers. Identity theft continues to be a major problem in this country, with victims numbering in the millions each year and out-of-pocket losses (primarily to businesses) in the billions of dollars.[4]

In April 2007, the FTC hosted a public workshop on consumer authentication to examine, among other things, the utility and risks of using SSNs as authenticators.[5] Following the release of the Strategic Plan that same month, the Task Force agencies launched an extensive research and outreach effort to develop a comprehensive record on the uses of SSNs by the private sector. Staff from various Task Force agencies conducted outreach to more than fifty stakeholders. In addition, the FTC received more than 300 comments after it solicited public comment on the issue.[6]

In November 2007, the FTC staff published a summary of the comments and other information it compiled through the outreach effort, entitled *Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers* (hereinafter, "FTC Staff Summary").[7] The FTC Staff Summary includes an in-depth description of the ways in which the private sector uses and collects SSNs and the role SSNs play in identity theft. Subsequently, the FTC held a second public workshop in December of 2007, which focused specifically on steps that might be taken to make the SSN less available and valuable to identity thieves.[8]

This report presents the Commission's recommendations for actions to minimize the role that SSNs play in identity theft.

A. The Role of SSNs in Identity Theft

As noted above, because private and public sector entities have used the SSN extensively as an identifier and in the authentication process, the SSN has become both available and valuable to identity thieves.[9] These criminals obtain the SSNs of the victims they impersonate and use them to facilitate the opening of new accounts, gain access to existing accounts, commit medical identity theft, seek employment, and obtain government benefits.[10] Although there is disagreement as to whether a thief can use the victim's name and SSN alone to steal her identity, it is generally understood that, at the least, the SSN facilitates identity theft, *i.e.*, that it is a *necessary*, if not necessarily *sufficient*, data element for many forms of this crime to occur.[11]

Thieves gather SSNs in many ways, from the high-tech – *e.g.*, hacking, phishing, malware, spyware, and keystroke loggers – to the low-tech – *e.g.*, dumpster diving, stealing workplace records, stealing mail or wallets, and accessing public records containing SSNs.[12] What is not known, however, is the prevalence of each of these methods. This is due in large part to the fact that victims frequently do not know how their information was compromised.[13] Moreover, even if reliable prevalence data were available, it likely would become outdated quickly as identity thieves change techniques to harvest consumers' data.

A number of commenters also addressed another form of identity theft that does not depend on illegally acquired SSNs. Some thieves fabricate SSNs that either intentionally or coincidentally correspond to SSNs that already have been issued or are about to be issued. The thieves then use these SSNs – in conjunction with other information unrelated to the individuals to whom the SSNs actually correspond – to create new identities. This is commonly referred to as synthetic identity theft.[14] The existence of synthetic identity theft demonstrates that the solution to SSN-related identity theft will require more than simply eliminating the sources of existing SSNs for identity thieves.

B. The SSN as Identifier

There appears to be broad consensus that the use of the SSN as an identifier – to match individuals to information about them both within an organization and between organizations – is prevalent and, in many contexts, beneficial.[15] Many organizations use SSNs as employee or customer identification numbers.[16] Some entities – including some insurers, universities, and government agencies – display the SSN on customer or employee identification cards, although this use is diminishing as noted below, while others use the SSN for data matching purposes "behind the scenes." Entities also may use their customers' SSNs to ensure that the data they share about those customers with a myriad of third parties is that of the right person. These entities share data for many legitimate, beneficial, and (in some cases) legally required purposes, such as to report earnings information to the IRS,[17] share patient records within the health care system,[18] and access consumer reports.[19]

Many businesses contend that the SSN is superior to any other item of information currently available to identify consumers and link information to them. Commenters from various sectors of the economy asserted that there are no other identifiers that are as reliable, cost-effective, and accurate for data matching as SSNs, because only the SSN is permanent, unique, ubiquitous, and common

across organizations.[20] Moreover, many have observed that consumers find it convenient to have a single identifier that can be used across applications and organizations, rather than having to memorize multiple numbers.[21]

Recognizing identity theft concerns, some organizations that use SSNs to identify their customers or members no longer print them on identification cards or otherwise publicly display them. For example, an increasing number of insurers and universities have discontinued their use of SSNs as customer, subscriber, or student identification numbers, but may still use SSNs internally.[22] In addition, some entities have stopped using SSNs as internal identifiers within their organizations, although others have resisted doing so because the change-over to another identifier can be costly and time-consuming.[23]

C. SSNs and the Authentication Process

"Authentication" is the process of verifying that someone is who he or she claims to be. It is distinguished from "identification," which simply matches an individual with his or her records, but does not prove that the individual is who he or she purports to be. Financial institutions, government agencies, and countless other organizations that enter into transactions with consumers authenticate individuals on a regular basis. It is when authentication fails – when an imposter successfully presents himself as someone else – that identity theft occurs. As the FTC Staff Summary noted, if authentication worked perfectly, identity thieves would not be able to use stolen consumer data to assume another's identity.[24]

Although there are many different kinds of authentication methods currently in use, they are not always adequate to prevent identity theft. According to the FTC Identity Theft Survey, 1.8 million consumers had new accounts opened fraudulently in their names in 2005, and another 6.5 million consumers experienced identity theft that involved exclusively existing bank account or credit account fraud.[25] These data suggest that identity thieves often are able to pass authentication screens successfully. There are different ways in which thieves might be doing so. Some thieves are able to obtain personal information about their victims beyond their SSNs that they then use to pass authentication tests. Others are able to obtain or manufacture fake drivers' licenses, similarly useful for authentication purposes. In other cases, businesses may not be requiring the right type of authentication (such as requiring only a name and SSN, or other readily available information, for account access), or their employees may not be following the company's procedures. The Commission knows of no reliable data showing the prevalence of the different methods by which criminals are passing authentication screening, but it is clear that they are able to do so in many instances.

As discussed above, there is a broad consensus that the use of the SSN as an identifier is often beneficial, but that its use as an authenticator – as proof of identity – is problematic. Identifiers are effective only when they are widely shared. One's name, for example, is widely known and generally effective as an identifier, although in many cases its lack of permanence or uniqueness prevents it from being useful as an identifier. Authenticators, on the other hand, are effective only when they are secret and thus not widely known. According to commenters and workshop participants, SSNs do not function well as authenticators because they are used commonly as identifiers and thus are widely available.[26]

Although the SSN generally is inadequate as a sole authenticator, it can be used effectively in the authentication *process*. Indeed, numerous organizations reported that they may ask a consumer to produce her SSN not because it is adequate authentication, but rather to link to other data sources that contain additional information about her that can be used to verify her identity. These data sources can take several forms. Some entities use the SSN to access databases containing information about an individual that can be used to formulate challenge questions that only the true individual should be able to answer (for example, the amount of her mortgage payment each month).[27] Other entities use the SSN to check an individual's identifying information against fraud databases (*i.e.*, databases with records of prior fraudulent transactions),[28] or as one element in their quantitative fraud prediction models, which are designed to flag suspect patterns of use of identifying information that might indicate that an application or proposed transaction is fraudulent.[29] These examples show that the SSN may not be well-suited as an authenticator itself, but can be and is used effectively to detect potential fraud by permitting access to other authentication-related information.[30]

III. Recommended Approach for Addressing the Problem

The Commission believes that the most effective approach to the problem of SSNs and identity theft will be comprehensive and multi-faceted, designed to reduce both the supply of and demand for SSNs, and carefully tailored to avoid hindering unnecessarily the beneficial transfers and uses of SSNs.

When considering ways to minimize the role the SSN plays in identity theft, commenters and participants at the SSN workshop agreed that the beneficial uses of SSNs must be weighed carefully against the harms that result when they are misused by identity thieves.[31] While these individuals acknowledged that the problems associated with SSN use must be addressed, they also cautioned that certain approaches may create unintended, negative consequences.[32]

Given that the widespread use and availability of SSNs cannot be completely reversed,[33] the Commission believes that the central component of the solution is to reduce the demand for SSNs by minimizing their value to identity thieves. This could be achieved by encouraging or requiring entities that have consumer accounts that can be targeted by identity thieves to adopt more effective authentication procedures, thereby making it more difficult for wrongdoers to use SSNs to open new accounts, access existing accounts, or otherwise impersonate a consumer.[34]

In addition, because improved authentication is not a foolproof mechanism for stopping persistent and creative thieves, it remains important to take steps to limit the supply of SSNs to criminals as part of a comprehensive approach to the identity theft problem. Therefore, the Commission recommends that measures be taken to reduce the unnecessary display and transmission of SSNs and improve data security.

With respect to its central proposals – improving authentication, reducing unnecessary SSN display and transmission, improving data security, and requiring breach notification – the Commission recommends that Congress consider establishing national standards that would be delineated further through agency rulemaking. In addition, the Commission recommends that Congress consider granting it authority to obtain civil penalties for violations of these rules.

Finally, coordination and information sharing among entities that routinely use SSNs can help facilitate the dual goals of improving authentication and protecting SSNs.[35]

A. Making It More Difficult to Use SSNs to Commit Identity Theft

The first step in minimizing the role of SSNs in identity theft is to limit the demand for SSNs by making it more difficult for thieves to use them to open new accounts, access existing accounts, or obtain other benefits or services.

Recommendation 1: Improve Consumer Authentication

Appropriate and reasonable authentication procedures can help prevent identity thieves from consummating their fraud. Although most financial institutions are subject to some authentication requirements promulgated by the bank regulatory agencies,[36] other businesses and organizations may not be subject to any such requirements. Requiring all private sector entities that maintain consumer accounts to establish appropriate, risk-based consumer authentication programs could reduce the misuse of consumer data and the prevalence of identity theft. Many workshop participants agreed that improving consumer authentication is critical.[37]

There have been some governmental efforts to extend authentication requirements beyond the financial sector. Some states have enacted laws that prohibit businesses from requiring consumers to use SSNs to log onto or access an Internet website, unless the SSNs are used in combination with a password or other authentication device.[38] One federal legislative proposal, H.R. 3046, calls for a study on the feasibility of banning the use of SSNs as authenticators.[39]

Generally speaking, however, private sector organizations outside the financial sector currently are not subject to any specific authentication requirements. Some workshop participants observed that such organizations may not have sufficient incentives to improve their authentication systems to an optimal level, because in many cases they are spared the full cost of identity theft.[40] Businesses certainly do suffer losses when identity thieves make fraudulent charges. Consumers themselves, however, often absorb some of the damage, including both direct losses and the time and emotional costs of recovery. Several workshop participants asserted that carefully-tailored government requirements may be necessary to set the proper incentives for improving authentication,[41] much as the Fair Credit Billing Act's limitation on cardholders' liability for disputed charges spurred the creation of a market for a variety of new fraud detection tools in the credit card industry.[42]

The Commission recommends that Congress consider establishing national consumer authentication standards covering all private sector entities that maintain consumer accounts other than financial institutions subject to the jurisdiction of the bank regulatory agencies, which already are subject to such requirements. These standards, which should be consistent with those covering financial institutions, should require private sector entities to create a written program that establishes reasonable procedures to authenticate new or existing customers. This "reasonable procedures" approach, which should be fleshed out through agency rulemaking, should be technology-neutral and provide flexibility to private sector entities to implement a program that is compatible with their size, the nature of their business, and the specific authentication risks they face. The procedures also

should be adaptable to changes that may occur over time in available technologies and the nature of the risks, including the potential harm to consumers. Finally, the standard should be one of reasonableness and not perfection, acknowledging that there is no fool-proof method of authenticating consumers and no likelihood that one will be developed in the foreseeable future.[43] "Reasonable procedures" requirements have been included in several recent identity theft-related rules promulgated by the FTC and the bank regulatory agencies pursuant to the Gramm-Leach-Bliley Act and the FACT Act.[44]

In developing authentication standards, Congress should consider several factors. First, the cost of implementing new authentication procedures should be evaluated in determining what is "reasonable." Second, consumer convenience is a critical concern and also should be weighed in the reasonableness determination. Consumers are likely to resist authentication requirements that are too time-consuming or difficult, or that require the memorization or retention of too much information. Third, more robust authentication procedures that require consumers to provide additional information about themselves raise potential privacy concerns. For instance, some businesses have developed authentication methods that require consumers to provide additional personal information either at the time the account is established or when the consumer later attempts to access the account. Many businesses use knowledge-based authentication in which they ask challenge questions, the answers to which are likely to be known only by the true individual. Although this method of authentication can overcome concerns about the unreliability of documentary evidence of identity[45] and the lack of personal interaction in telephone or online transactions, challenge questions may require consumers to provide increasing amounts of information to businesses that are linked together in ways that may be unsettling to some.[46]

Some commenters and workshop participants also suggested that, even in the absence of any national standards for authentication, the FTC could spur improved authentication by challenging inadequate authentication procedures, such as using an SSN as the sole authenticator, as unfair or deceptive practices prohibited by Section 5 of the Federal Trade Commission Act.[47] The Commission has challenged businesses that failed to provide reasonable security for sensitive consumer information as deceptive (when the business misrepresented its security practices)[48] or unfair (when the business's lack of reasonable security caused or was likely to cause substantial and unavoidable consumer injury).[49] Whether the failure to conduct reasonable authentication could constitute an unfair or deceptive practice would depend on the facts of a particular case, for example, whether the company made false or misleading claims or caused substantial consumer injury by its inadequate authentication. In appropriate cases, the Commission will consider law enforcement action against businesses that fail to maintain reasonable authentication procedures.[50]

B. Curtailing the Supply of SSNs to Wrongdoers

Although decreasing the value of SSNs for identity thieves is essential to curbing their use in identity theft, limiting unnecessary SSN supply and availability remains important and would complement efforts to reduce SSN demand.

Recommendation 2: Restrict the Public Display and the Transmission of SSNs

Although SSNs are valuable as a means of linking consumers with their information, much can be done to reduce the availability of SSNs to identity thieves by eliminating the unnecessary display and transmission of SSNs by the private sector. Restricting the display of SSNs on publicly-available documents and identification cards, and limiting the circumstances and means by which they can be transmitted, would make it more difficult for thieves to obtain SSNs, without hindering their use for legitimate identification and data matching purposes.[51]

Many organizations already have discontinued using SSNs as employee or customer numbers, or have stopped printing them on identification cards or in mailings to customers.[52] Yet, some businesses, universities, and other private sector entities still include SSNs on identification cards, thereby exposing them in the event that an individual's wallet is lost or stolen.[53] Moreover, some organizations continue to display SSNs on account statements, paychecks, applications, or other documents that are sent through the mail, which puts consumers at risk for identity theft if their mail is stolen or if the documents are thrown in the trash without being shredded.[54] SSNs also can be exposed to potential identity thieves by inadvertent display, including on websites.[55]

Some states have enacted laws limiting the display and/or transmission of SSNs.[56] California was the first state to pass such a law, which prohibits the printing of SSNs on identification and membership cards and certain documents mailed to customers and bars the emailing of unencrypted SSNs.[57] Several other states have followed California's lead.[58] Workshop participants and commenters generally reported that provisions of state laws that restrict public display are not unduly burdensome.[59] They asserted that the process of removing SSNs from identification cards and public documents generally is easier than eliminating the use of SSNs for internal or external data matching, which can create inefficiencies and be expensive.[60]

Some workshop participants and commenters asserted that switching from the display of full SSNs to truncated SSNs could help reduce identity theft.[61] These observers note that partial SSNs still can be useful in identifying and authenticating consumers, although not to the extent of full SSNs.

It is true that truncated SSNs generally are less valuable to identity thieves than full SSNs, because many entities will not allow customers to open or access accounts without a full SSN. There are some situations, however, in which a thief could use a truncated SSN to steal an identity. First, some organizations may accept truncated SSNs as adequate authentication, at least in certain instances such as when a customer wishes to access his account via telephone or online. Second, inconsistencies in the means by which entities truncate could create an opening for an identity thief to obtain a full SSN. Currently, there are varying conventions for SSN truncation – some entities, for example, block the first five digits while others block the last four digits.[62] Thus, an identity thief could piece together the full SSN by obtaining different parts of the number from different sources. Third, because the Social Security Administration uses date and location of issuance to determine the first five digits of the SSN, some observers have posited that identity thieves could use a truncated SSN, augmented by other personal information that they obtain and some guess work, to determine the full SSN.[63]

The Commission recommends that Congress consider creating national standards for the public display and the transmission of SSNs.[64] Federal legislation would establish a nationwide approach to

reducing unnecessary display and transmission of SSNs, while addressing concerns about a patchwork of state laws with varying requirements. National standards should prohibit private sector entities from unnecessarily exposing SSNs. The precise standards should be developed in rulemaking by appropriate federal agencies (*i.e.*, agencies that oversee organizations that routinely transmit or display SSNs), and should include, for example, prohibitions against:

- publicly posting or displaying SSNs;
- placing SSNs on cards or documents required for an individual to access products or services provided by a covered entity, including student ID cards, employee ID cards, and insurance cards;
- transmitting (or requiring an individual to transmit) an SSN over the Internet, unless the connection is secure from unauthorized access, *e.g.*, by encryption or other technologies that render the data generally unreadable;
- printing an individual's SSN in materials mailed to the individual; and
- printing an individual's SSN on the outside of an envelope or other mailer, or in a location that is visible without opening the envelope or mailer.

Any such standards should allow for the display and transmission of SSNs when required by law and in specified circumstances where there is a substantial business need that outweighs the risks of exposure. For example, California has created exceptions for SSNs that are included in forms mailed as part of an enrollment process and for documents necessary to establish an account or contract, provided that the SSN is not visible without opening the transmitting envelope.[65] Federal agency rulemaking should similarly evaluate acceptable circumstances for display and transmission. In addition, the standards should take into account the benefits and risks of allowing the display and transmission of truncated SSNs. Finally, entities should be given a sufficient phase-in period for implementation, given the often significant cost of modifying systems to avoid displaying SSNs.

Recommendation 3: Establish National Standards for Data Protection and Breach Notification

An important step in limiting the supply of SSNs is for entities that collect and store sensitive consumer information to safeguard it against unauthorized access. Safeguards requirements currently exist with respect to certain industries, certain types of data, and in certain states. The Safeguards Rules promulgated by the FTC and the federal banking agencies pursuant to the Gramm-Leach-Bliley Act, for example, require financial institutions to establish reasonable procedures to protect consumers' personally identifiable financial information, which may include SSNs.[66] Many entities or types of data are not subject to federal data security standards, however. The Commission has previously expressed support for national data security standards that would cover SSNs in the possession of any private sector entity,[67] and numerous commenters and workshop participants voiced similar support.[68] Such standards, which would be implemented in rulemaking by federal agencies that oversee entities that routinely use and transfer sensitive consumer information, could be modeled after the Safeguards Rules and cover all entities that maintain sensitive consumer information.

The Commission also reiterates its support of its prior recommendation that Congress consider establishing national data breach notification standards requiring private sector entities to provide public notice when the entity suffers a breach of consumers' personal information and the breach creates a significant risk of identity theft or other harms.[69] These standards would also be implemented in rulemaking by appropriate federal agencies. Most states now have breach notification laws,[70] but currently there is no across-the-board federal requirement.[71] Commenters and workshop participants noted that, in addition to alerting affected consumers to protect themselves, these laws have had the indirect benefit of motivating companies to weigh their need to collect SSNs against the potential cost and liability that may ensue if the SSNs are compromised.[72] Participants also noted that many businesses have strengthened their safeguards practices to avoid data breaches, at least in part as a result of breach notification requirements.[73] The state laws differ in various respects, however, complicating compliance.[74]

Recommendation 4: Conduct Outreach to Businesses and Consumers

The Commission recommends increasing education and guidance efforts as additional steps to help reduce the role of SSNs in facilitating identity theft. Over the past several years, the Commission and other Task Force agencies (including the Social Security Administration, the Department of Health and Human Services, and the U.S. Postal Inspection Service) have conducted extensive outreach, both to businesses and consumers, on identity theft prevention and recovery, data protection, and safe computing. Many of the published materials discuss SSNs specifically, with advice to consumers on protecting their SSNs from wrongdoers.[75]

The Commission anticipates disseminating additional guidance to businesses on what they can do to reduce their use of SSNs and to safeguard SSNs when they are used. This guidance would ultimately include information regarding any national standards Congress creates for authentication, SSN display and transmission, data protection, and breach notification. This type of guidance would be especially useful to small businesses and could include the following messages:

- the importance of collecting SSNs only when necessary and storing them only as long as necessary;
- steps businesses can take to reduce the use of SSNs as internal identifiers;
- proper disposal of SSNs;
- the importance of securing SSNs (such as by encrypting them) during their transmission; and
- limiting employee access to SSNs and conducting employee screening and training.

The Commission also anticipates issuing additional guidance to consumers directed specifically at how they can protect their SSNs. This guidance will explain the various ways identity thieves obtain SSNs, from phishing to wallet theft, and how consumers can best protect their personal information. It also will address safe disposal practices and the questions consumers should ask when a business requests their SSN. Continuing and augmenting these education efforts will help maximize consumer awareness of risks and lead to decreased exposure to identity theft.

C. Improving Coordination and Information Sharing

Recommendation 5: Promote Coordination and Information Sharing on Use of SSNs

Many private sector entities, from large multi-nationals and universities to small businesses and health care systems, have described the difficulties and expense of removing SSNs from computer systems and files, as well as the challenges of keeping up with the sophisticated and changing methods of identity thieves.[76] Coordination and information sharing among private sector entities and between government and the private sector could assist entities in finding ways to reduce their uses of and better protect SSNs and improve their authentication processes. The Commission recommends that appropriate governmental entities explore helping private sector organizations establish a clearinghouse of best practices, enabling those organizations to share approaches and technologies on SSN usage and protection, fraud prevention, and consumer authentication.

IV. Conclusion

Since the creation of the SSN in 1936, the private sector increasingly has utilized it for various purposes – both as an identifier and an authenticator – because it is the only permanent, unique piece of information that most Americans have about themselves. The SSN's use has expanded as organizations have adapted their business and record-keeping systems to utilize increasingly sophisticated automated data processing. The SSN has, over time, become an integral part of our financial system.

As the private sector's use of the SSN has grown, so too has its availability and value for identity thieves. The Commission believes that a number of actions could be taken to reduce the role of SSNs in identity theft, with emphasis on reducing the demand for SSNs by minimizing their value to identity thieves through improved authentication processes. Most importantly, the Commission recommends that Congress consider establishing national authentication standards for businesses that have consumer accounts and are not already subject to authentication requirements from other federal agencies.

Because authentication can never be perfect, however, the Commission also recommends carefully targeted actions to limit the supply or availability of SSNs to identity thieves. Specifically, the Commission recommends that Congress consider prohibiting the display of SSNs on publicly-available documents, identification cards, and other materials that could potentially fall into the hands of identity thieves. The Commission also recommends that Congress set national safeguards and breach notification standards, because better-protected SSNs are less likely to fall into the hands of criminals. Finally, the Commission is committed to educating consumers on protecting their SSNs and businesses on reducing their use of SSNs, and recommends that the government and private sector entities explore information sharing and other cooperative efforts to achieve these goals.

Together, these actions could substantially reduce the misuse of SSNs by identity thieves, while at the same time preserving the beneficial uses of SSNs in our economic system.

Endnotes

1 The Task Force is comprised of 17 federal agencies and is co-chaired by the Attorney General and the Chairman of the Federal Trade Commission. *See* Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006).

2 *See* The President's Identity Theft Task Force, *Combating Identity Theft, A Strategic Plan* (April 2007), available at http://www.idtheft.gov/reports/StrategicPlan.pdf (hereinafter "Strategic Plan"). The Task Force also made a number of recommendations regarding the public sector's use of SSNs, highlighting the importance of limiting unnecessary use of SSNs by federal departments and agencies. *See id*. at 23-27. Many of these recommendations regarding limiting use and display of SSNs have been implemented. The status of these recommendations is described in the recent *Identity Theft Task Force Report*. *See* President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), at 6-8 and 51, available at http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf.

3 Social Security Online, Social Security Number Chronology, http://www.ssa.gov/history/ssn/ssnchron.html.

4 *Federal Trade Commission – 2006 Identity Theft Survey Report* 3 & 9 (Nov. 2007), available at http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (hereinafter "FTC Identity Theft Survey").

5 Proof Positive: New Directions for ID Authentication, http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml.

6 These public comments are available at http://www.ftc.gov/os/comments/ssnprivatesector/index.shtm.

7 *Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers* (Nov. 2007), available at http://www.ftc.gov/bcp/workshops/ssn/staffsummary.pdf (hereinafter "FTC Staff Summary").

8 Security in Numbers: SSNs and Identity Theft, http://www.ftc.gov/bcp/workshops/ssn/index.shtm.

9 Transcript of Security in Numbers: SSNs and ID Theft Workshop (Dec. 10, 2007) at 184-85, (hereinafter "Transcript of SSN Workshop"), Remarks of Dr. Annie I. Anton, Associate Professor, North Carolina State University, and Director, PrivacyPlace.org (explaining that the use of the SSN for both identification and authentication makes it more valuable to an identity thief).

10 *See, e.g.*, FTC Staff Summary, at 14-18; Transcript of SSN Workshop (Dec. 10, 2007) at 62-63, Remarks of John K. Webb, Assistant U.S. Attorney, Southern District of West Virginia (discussing various ways SSNs are used to commit identity theft, including hijacking existing accounts and opening new accounts).

11 Some commenters and workshop participants asserted that identity thieves need additional information beyond a consumer's name and SSN to open a new account, while others argued the opposite, noting instances in which credit was granted based on applications full of inconsistencies and mismatched information. *See* FTC Staff Summary, at 14, 17. The FTC's latest survey found that approximately 1.8 million instances of new account identity theft occurred in 2005, the vast majority of which presumably involved the misuse of the victim's SSN. *See* FTC Identity Theft Survey, at 3. What the data do not reveal, however, is what additional information, if any, the thieves had that enabled them to open the accounts.

12 *See, e.g.*, FTC Staff Summary, at 9-14; Transcript of SSN Workshop (Dec. 10, 2007) at 26-29, Remarks of John K. Webb, Assistant U.S. Attorney, Southern District of West Virginia (discussing numerous ways identity thieves obtain SSNs, including hacking, phishing, and stealing mail or wallets).

13 The FTC's Identity Theft Survey found that 56% of the identity theft victims surveyed did not know how their personal information was obtained. See FTC Identity Theft Survey, at 30. Similarly, the 2007 Identity Fraud Survey by Javelin Strategy and Research found that 58% of identity theft victims did not know how their personal information was obtained. Javelin Strategy and Research, *2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary* 30 (Feb. 2007). Needless to say, successful thieves are unlikely to reveal their "tools of the trade."

14 *See* FTC Staff Summary, at 16-17.

15 These basic concepts are discussed in greater detail in the FTC Staff Summary.

16 *See, e.g.*, FTC Staff Summary, at 19-20.

17 *See, e.g.*, Transcript of SSN Workshop (Dec. 10, 2007) at 149-153, Remarks of Valerie Abend, Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy, U.S. Department of the Treasury (explaining the various ways the Treasury Department requires the private sector to collect and report SSNs).

18 *See, e.g.*, FTC Staff Summary, at 22; Transcript of SSN Workshop (Dec. 10, 2007) at 168, Remarks of Roberta B. Meyer, Vice President and Associate General Counsel, American Council of Life Insurers (explaining that many healthcare providers are concerned about disclosing health records without being provided an SSN).

19 *See, e.g.*, FTC Staff Summary, at 21-22; Transcript of SSN Workshop (Dec. 10, 2007) at 156-161, Remarks of Robert F. Ryan, Vice President for Government Affairs, TransUnion (describing the various ways the consumer reporting industry utilizes SSNs).

20 *See, e.g.*, FTC Staff Summary, at 19-26; Transcript of SSN Workshop (Dec. 10, 2007) at 165, Remarks of Roberta B. Meyer, Vice President and Associate General Counsel, American Council of Life Insurers (explaining that the SSN is an important identifier because it is unique and does not change over time); Transcript of SSN Workshop (Dec. 10, 2007) at 102, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles (noting the importance of the SSN as an identifier because it typically does not change); Transcript of SSN Workshop, (Dec. 10, 2007) at 175, 179-180, Remarks of Michael C. Lamb, Vice President and General Counsel, LexisNexis Risk and Information Analytics Group (stating that the SSN is the one data point that persists and is unique and that SSN use for data linking "is extremely important"); Transcript of SSN Workshop (Dec. 10, 2007) at 156, Remarks of Robert F. Ryan, Vice President for Government Affairs, TransUnion (noting that the SSN helps ensure that credit files are accurate and complete).

21 *See, e.g.*, Transcript of SSN Workshop (Dec. 10, 2007) at 39, Remarks of Lael Bellamy, Director-Legal, The Home Depot (discussing the convenience of accessing a consumer's credit account simply by punching the SSN into a key pad); Transcript of SSN Workshop (Dec. 10, 2007) at 120-21, Remarks

of Kimberly Gray, Chief Privacy Officer for Highmark, Inc. (noting that customers often ask to use their SSN for authentication purposes because they find it convenient).

22 *See, e.g.*, FTC Staff Summary, at 23-24; Transcript of SSN Workshop (Dec. 10, 2007) at 89-93, Remarks of Kimberly Gray, Chief Privacy Officer for Highmark, Inc. (describing process of removing SSNs from insurance identification cards); Transcript of SSN Workshop (Dec. 10, 2007) at 96, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles (describing process of removing SSNs from university identification cards).

23 *See, e.g.*, FTC Staff Summary, at 24; Transcript of SSN Workshop (Dec. 10, 2007) at 40-41, Remarks of Lael Bellamy, Director-Legal, The Home Depot (noting that project to remove unnecessary SSNs at The Home Depot took approximately two years).

24 FTC Staff Summary, at 26.

25 FTC Identity Theft Survey, at 3.

26 *See, e.g.*, FTC Staff Summary, at 26-27; Transcript of SSN Workshop (Dec. 10, 2007) at 184-85, Remarks of Dr. Annie I. Anton, Associate Professor, North Carolina State University, and Director of the PrivacyPlace.org (noting that use of the SSN as both an identifier and authenticator is problematic).

27 *See, e.g.*, FTC Staff Summary, at 29; Transcript of SSN Workshop (Dec. 10, 2007) at 162-63, Remarks of Stan Szwalbenest, Remote Channel Risk Director, JPMorgan Chase Consumer and Retail Franchise (describing the process of using SSNs to obtain knowledge-based authentication questions from consumer reporting agencies).

28 *See, e.g.*, FTC Staff Summary, at 30.

29 *See, e.g.*, FTC Staff Summary, at 30-31; Transcript of SSN Workshop (Dec. 10, 2007) at 240-45, Remarks of Thomas Oscherwitz, Vice President of Government Affairs and Chief Privacy Officer, ID Analytics (describing how ID Analytics uses the SSN in its quantitative fraud prediction model).

30 *See, e.g.*, FTC Staff Summary, at 26-31; Transcript of SSN Workshop (Dec. 10, 2007) at 237, 240, Remarks of Jennifer Barrett, Global Privacy Officer, Acxiom Corporation (stating that without use of the SSN, Acxiom's ability to validate an individual's information would decrease significantly, and noting that she does not know of an equivalent substitute for the SSN for linking data for authentication).

31 *See* FTC Staff Summary, at 19-26, 43; *see also* Strategic Plan, at 26-27.

32 *See, e.g.*, Transcript of SSN Workshop (Dec. 11, 2007) at 59, Remarks of Jim McCartney (noting the inevitability of unintended consequences from making changes to SSN usage); Transcript of SSN Workshop (Dec. 11, 2007) at 95, Remarks of Fred Cate, Distinguished Professor and Director for Applied Cybersecurity Research, Indiana University, and Senior Policy Advisor, Center for Information Policy Leadership, Hunton & Williams (commenting on the potential for increased fraud if access to data useful for fraud detection purposes is restricted; also noting the potential for increased consumer inconvenience if data uses are restricted); FTC Staff Summary, at 31-32 (reviewing commenters' concerns that restrictions on SSN usage would make fraud detection and employee and volunteer screening more difficult).

33 Many workshop participants and commenters noted that SSNs already are widely available, and any attempt now to "put the genie back in the bottle" likely would be of limited value. Transcript of SSN

Workshop (Dec. 10, 2007) at 254-55 and Transcript of SSN Workshop (Dec. 11, 2007) at 126-27, Remarks of Tom Oscherwitz, Vice President of Government Affairs and Chief Privacy Officer, ID Analytics; Transcript of SSN Workshop (Dec. 11, 2007) at 155, Remarks of Fred Cate, Distinguished Professor and Director for Applied Cybersecurity Research, Indiana University, and Senior Policy Advisor, Center for Information Policy Leadership, Hunton & Williams.

34 Some suggested approaches to the problem of SSNs and identity theft focus on restricting the sale or transfer of SSNs to prevent thieves from obtaining them in the first instance, rather than reducing the value of SSNs to identity thieves once obtained. *See* FTC Staff Summary, at 38-39. These approaches also seek to preserve beneficial uses of SSNs. For example, some proposals would allow specified beneficial transfers (*e.g.*, for credit reporting or fraud prevention purposes), and some would authorize the FTC or other agencies to create additional exemptions. The Commission believes that it would be extremely difficult, however, to craft the exemptions with sufficient precision so as to eliminate harmful transfers while permitting beneficial ones. If drafted too broadly, the exemptions could "swallow" the rule, so that virtually any type of transfer could fit within one or more exemptions. *See generally* Transcript of SSN Workshop (Dec. 11, 2007) at 156, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies. Conversely, if the exemptions were drafted too narrowly, the rules could inadvertently prohibit beneficial transfers. Further complicating this task is the fact that some transfers of SSNs could serve both a beneficial purpose *and* raise risks of harm. For example, SSNs often are used for locating individuals, which could be for beneficial purposes (*e.g.*, finding witnesses or beneficiaries) or harmful purposes (*e.g.*, stalking).

35 This report focuses on recommendations to minimize the role of SSNs in identity theft, and does not address whether additional criminal penalties related to other types of misuse of SSNs are appropriate. For example, there have been reports of stalkers and other criminals obtaining and using SSNs to locate their victims. *Protecting the Social Security Number from Identity Theft: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways and Means*, 110th Cong. (June 21, 2007) (statement of Rep. Ed Markey).

36 For example, the guidance on authentication released by the Federal Financial Institutions Examination Council ("FFIEC") advises companies of the risk management controls they should adopt to authenticate the identity of customers in the electronic banking context. *See* FFIEC, *Authentication in an Internet Banking Environment*, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. In addition, the Customer Identification Program ("CIP") rule, promulgated by the federal banking agencies (the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation) and the National Credit Union Administration ("NCUA") under the USA PATRIOT Act, although not designed to prevent identity theft, mandates that, before opening a new consumer account, a financial institution or other covered entity must "form a reasonable belief that it knows the true identity of each customer." 31 C.F.R. §§ 103.121(b)(2), 103.122(b)(2), 103.123(b)(2) & 103.131(b)(2). Finally, the Identity Theft Red Flags rules, recently promulgated by the FTC, the federal banking agencies, and the NCUA pursuant to the FACT Act of 2003, require most financial institutions and creditors to develop and implement an Identity Theft Prevention Program that includes reasonable policies and procedures for detecting, preventing, and mitigating identity theft in connection with existing accounts or the opening of new accounts. 16 C.F.R. § 681.2. These procedures may include enhanced customer authentication.

37 For example, workshop participants highlighted the importance of avoiding the use of the SSN as the sole authenticator. *See* Transcript of SSN Workshop (Dec. 10, 2007) at 185, Remarks of Dr. Annie I. Anton, Associate Professor, North Carolina State University, and Director, PrivacyPlace.org; Transcript of SSN Workshop (Dec. 10, 2007) at 218, Remarks of Beth Givens, Director, Privacy Rights Clearinghouse; Transcript of SSN Workshop (Dec. 10, 2007) at 254 and (Dec. 11, 2007) at 127, Remarks of Tom Oscherwitz, Vice President of Government Affairs and Chief Privacy Officer, ID Analytics; Transcript of SSN Workshop (Dec. 11, 2007) at 93-94, 155, Remarks of Fred Cate, Distinguished Professor and Director for Applied Cybersecurity Research, Indiana University, and Senior Policy Advisor, Center for Information Policy Leadership, Hunton & Williams; Transcript of SSN Workshop (Dec. 11, 2007) at 131, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies; Transcript of SSN Workshop (Dec. 11, 2007) at 25, Remarks of Stuart Pratt, President and CEO, Consumer Data Industry Association; Transcript of SSN Workshop (Dec. 11, 2007) at 46, Remarks of Bob Blakley, Principal Analyst, Burton Group; Transcript of SSN Workshop (Dec. 11, 2007) at 154-55, Remarks of Chris Jay Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology and Public Policy Clinic, UC Berkeley School of Law.

38 *See, e.g.*, Tenn. Code Ann. § 47-18-2110 (2008).

39 Social Security Number Privacy and Identity Theft Protection Act of 2007, H.R. 3046, 110th Cong. § 14 (2007).

40 *See* Transcript of SSN Workshop (Dec. 11, 2007) at 33, Remarks of Jeanine Kenney, Senior Policy Analyst, Consumers Union; Transcript of SSN Workshop (Dec. 11, 2007) at 19-20, Remarks of Bob Blakley, Principal Analyst, Burton Group.

41 *See* Transcript of SSN Workshop (Dec. 11, 2007) at 46-47, Remarks of Bob Blakley, Principal Analyst, Burton Group; Transcript of SSN Workshop (Dec. 11, 2007) at 107-108, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies.

42 15 U.S.C. § 1666-1666j. Workshop participants discussed a number of innovative authentication techniques or programs, such as the use of third-party identity providers. To date, these innovations have not flourished for reasons that may include the lack of market incentives. *See* Transcript of Proof Positive: New Directions in ID Authentication Workshop (Apr. 23-24, 2007), Panel 7, at 26-27, (hereinafter "Transcript of Authentication Workshop"), Remarks of Fred Schneider, Professor, Computer Science Department, Cornell University (explaining that regulations may be needed to "fix the market" and create incentives for better authentication); Transcript of SSN Workshop (Dec. 11, 2007) at 19-21, Remarks of Bob Blakley, Principal Analyst, Burton Group (stating that externalities could be addressed by third-party identity providers, or "identity oracles"). Workshop participants also noted the importance of consumer convenience in any authentication system. *See* Transcript of Authentication Workshop, Panel 5, at 11, Remarks of Cynthia Bohman, Manager, Cyber Fraud Risk, Discover Financial Services (discussing the importance of consumer convenience to an authentication system). Creating appropriate incentives is likely to encourage the development of authentication techniques that are both effective and convenient.

43 In some cases, even using multiple authenticators will not prevent identity theft, if the thief has sufficient information about his victim. Some organizations match identifying information provided by an applicant to that found in a third-party database, such as that of a consumer reporting agency, but this

process only detects mismatched information and would not detect an identity thief who has provided sufficient, accurate identifying information. Other companies may rely on checking a driver's license to authenticate an individual, but identity thieves can obtain falsified licenses. FTC Staff Summary, at 27.

44 These include: (1) the Safeguards Rules, which require financial institutions to have a written data security program with reasonable procedures to identify and address risks to customers' personally identifiable financial information, 16 C.F.R. Part 314; (2) the Disposal Rules, which require that businesses implement reasonable procedures to ensure that certain sensitive information is disposed of in a safe manner, 16 C.F.R. Part 682; and (3) the Identity Theft Red Flags Rules, which require most financial institutions and creditors to develop and implement a written Identity Theft Prevention Program that includes reasonable policies and procedures for detecting, preventing, and mitigating identity theft in connection with existing accounts or the opening of new accounts, 16 C.F.R. Part 681.

45 Participants at both the authentication and SSN workshops noted that documents frequently used for authentication when creating an account, such as driver's licenses, Social Security cards, and birth certificates, can easily be forged. *See* Transcript of Authentication Workshop, Panel 3, at 2-4, Remarks of Garland Land, Executive Director, National Association for Public Health Statistics and Information Systems (explaining weaknesses in birth certificate issuance process); Transcript of Authentication Workshop, Panel 3, at 19, Remarks of Ari Schwartz, Deputy Director, Center for Democracy and Technology (discussing the need for strengthening the driver's license issuance process); Transcript of SSN Workshop (Dec. 10, 2007) at 26, Remarks of John K. Webb, Assistant United States Attorney, Southern District of West Virginia (addressing ease of forging SSN cards).

46 *See* Transcript of SSN Workshop (Dec. 11, 2007) at 49, Remarks of Stuart Pratt, President and CEO, Consumer Data Industry Association. In some cases, challenge questions may be based on information the business already has or is able to obtain from outside data sources, *e.g.*, what financial institution holds the consumer's mortgage. *See* Transcript of Authentication Workshop, Panel 4, at 14-16, 19, Remarks of Micheline Casey, Senior Director, Identity Management, Choicepoint Government Services (explaining the process used to create knowledge-based authentication questions). In other cases, businesses may ask the consumer to establish questions and answers at the time of account enrollment, known as shared secrets, to be used for subsequent account access. Such questions and answers may be about a customer's pets, previous vehicles owned, family members, etc. *See* Transcript of Authentication Workshop, Panel 7, at 29, Remarks of Thomas Oscherwitz, Chief Privacy Officer, ID Analytics (noting that in an environment where information is available, for example, through social networking sites, shared secrets must become more and more personal in order to defeat the fraudsters). In either event, the business is compiling and maintaining additional information about the consumer. Because there currently are no broad-based restrictions on using this information for other purposes, or sharing it with third parties, some participants at the authentication workshop suggested that the government should enact broader privacy rules so that consumers will willingly participate in systems requiring stronger authentication. *See* Transcript of Authentication Workshop, Panel 7, at 4, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies; Transcript of Authentication Workshop, Panel 7, at 27, Remarks of Jeffrey Friedberg, Chief Privacy Architect, Microsoft (discussing privacy concerns raised by authentication technologies that allow the linking of personal data).

47 *See, e.g.*, Transcript of SSN Workshop (Dec. 11, 2007) at 88-89, Remarks of Chris Jay Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology and Public Policy Clinic, UC Berkeley School of Law; Comment of Center for Information Policy Leadership at Hunton & Williams, at 5. A deceptive

practice, pursuant to 15 U.S.C. § 45, "is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." FTC Policy Statement on Deception, Oct. 14, 1983, available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm. An unfair practice is an "act or practice [that] causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

48 *United States v. ValueClick, Inc.*, No. CV08-01711 (C.D. Cal. Mar. 13, 2008); *In the Matter of Goal Financial, LLC*, FTC Docket No. C-4216 (April 15, 2008); *In the Matter of Life is Good, Inc.*, FTC Docket No. C-4218 (Apr. 18, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 3, 2007); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *and In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

49 *In the Matter of The TJX Companies*, FTC Docket No. C-4227 (Aug. 1, 2008); *In the Matter of Reed Elsevier Inc. and Seisint Inc.*, FTC Docket No. C-4226 (Aug. 1, 2008); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); and *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

50 Inadequate authentication could violate other existing laws or regulations as well. The Safeguards Rules, for example, require financial institutions to maintain reasonable protections for personally identifiable financial information, which could include SSNs. The duty to protect this information could include, in appropriate cases, the duty to employ reasonable authentication procedures to prevent unauthorized persons from gaining access to consumers' accounts and records. Similarly, the Identity Theft Red Flags Rules require covered entities to detect signs of identity theft, which might be addressed by improving authentication procedures for both account opening and account access requests. *See* 16 C.F.R. § 681.2.

51 *See* FTC Staff Summary, at 23 ("Not displaying SSNs on cards, which are frequently carried by the holder, decreases the risk of identity theft through loss, theft, or duplication of the card."); Transcript of SSN Workshop (Dec. 10, 2007) at 107, Remarks of Kim Duncan, Vice President of Enterprise Fraud Management at SunTrust Bank; Transcript of SSN Workshop (Dec. 11, 2007) at 170-71, Remarks of Joel Winston, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission.

52 FTC Staff Summary, at 20, 23-25.

53 *See* FTC Staff Summary, at 12. Five percent of all identity theft victims point to a stolen wallet as the source of information used to commit the identity theft against them. Notably, 56 percent of all victims do not know how their information was obtained by the thief. *See* FTC Identity Theft Survey, at 30.

54 FTC Staff Summary, at 12.

55 *See, e.g.*, Lena H. Sun, *Posting of Social Security Numbers Results in Suspension of Three Workers*, Washington Post, June 15, 2008, available at http://www.washingtonpost.com/wp-dyn/content/article/2008/07/14/AR2008071402245.html (reporting that the Social Security numbers of nearly 4,700 current and former District of Columbia Metro employees were mistakenly posted on the transit agency's website).

56 FTC Staff Summary, at 40; Transcript of SSN Workshop (Dec. 10, 2007) at 96, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles; Transcript of SSN Workshop (Dec. 10, 2007) at 88-89, Remarks of Kimberly Gray, Chief Privacy Officer for Highmark, Inc.

57 *See* Cal. Civ. Code § 1798.85.

58 *See* Government Accountability Office, GAO-08-1009R, *Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring*, 4 (Sept. 2008) (approximately 25 states have passed laws limiting the public display and/or use of SSNs); Transcript of SSN Workshop (Dec. 10, 2007) at 83-85, Remarks of Steven Sakamoto-Wendel, Assistant Attorney General, State of Maryland.

59 FTC Staff Summary, at 40-41; Transcript of SSN Workshop (Dec. 10, 2007) at 85-86, Remarks of Steven Sakamoto-Wendel, Assistant Attorney General, State of Maryland. Some workshop participants and commenters were concerned that certain states are beginning to move beyond public display restrictions. *See* Transcript of SSN Workshop (Dec. 10, 2007) at 160, Remarks of Robert F. Ryan, Vice President for Government Affairs, TransUnion; Transcript of SSN Workshop (Dec. 10, 2007) at 181-82, Remarks of Michael Lamb, Vice President and General Counsel, LexisNexis Risk and Information Analytics Group (commenting on a recent Minnesota law mandating fairly broad sale and use restrictions in addition to restrictions on display of full SSNs).

60 FTC Staff Summary, at 23-26; Transcript of SSN Workshop (Dec. 10, 2007) at 93-95, Remarks of Kimberly Gray, Chief Privacy Officer for Highmark, Inc. (discussing the removal of SSNs from Highmark, Inc. identification cards and the various ways Highmark, Inc. continues to use SSNs for data matching); Transcript of SSN Workshop (Dec. 10, 2007) at 103-104, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles (explaining that although the university has removed SSNs from its identification cards and dramatically reduced their use, there are some instances where SSNs remain necessary for data matching).

61 *See, e.g.*, Comment of Mortgage Bankers Assoc., at 4 (recommending the use of truncated SSNs as a way to limit identity theft exposure); Comment of New York State Consumer Protection Board, at 2 (recommending the use of truncated SSNs on all documents as a way of preventing identity theft); Transcript of SSN Workshop (Dec. 10, 2007) at 107, Remarks of Kim Duncan, Vice President of Enterprise Fraud Management, SunTrust Bank (discussing the use of SSN truncation by financial institutions).

62 *See* Government Accountability Office, GAO-06-495, *Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs*, 12-14 (May 2006).

63 *See, e.g.*, Comment of Consumers Union, at 3.

64 Many of the current congressional proposals addressing SSNs include display restrictions. *See, e.g.*, Social Security Number Misuse Prevention Act, S. 238, 110th Cong. § 3 (2007); Social Security Number Privacy and Identity Theft Protection Act of 2007, H.R. 3046, 110th Cong. §§ 2 & 8 (2007).

65 *See* Cal. Civ. Code § 1798.85.

66 *See* 16 C.F.R. Part 314; 17 C.F.R. § 248.30; Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616 (Feb. 1, 2001).

67 *See Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (June 16, 2005) (written statement of Federal Trade Commission) at 7. The Task Force similarly recommended such standards. *See* Strategic Plan, at 35.

68 FTC Staff Summary, at 42; Transcript of SSN Workshop (Dec. 10, 2007) at 186, Remarks of Dr. Annie I. Anton, Associate Professor, North Carolina State University, and Director, PrivacyPlace.org; Transcript of SSN Workshop (Dec. 11, 2007) at 51, Remarks of Stuart Pratt, President and CEO, Consumer Data Industry Association.

69 *See Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (June 16, 2005) (written statement of Federal Trade Commission) at 7. The Task Force also supported this recommendation, as well as civil penalty authority to enforce such standards. *See* Strategic Plan, at 34-35, 37.

70 Strategic Plan, at 34-35; FTC Staff Summary, at 41-42.

71 The federal banking agencies and the NCUA have issued guidance to their regulated entities regarding breach response and notification procedures. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005).

72 Transcript of SSN Workshop (Dec. 11, 2007) at 106, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies; Transcript of SSN Workshop (Dec. 10, 2007) at 226, Remarks of Emily Mossburg, Senior Manager, Security and Privacy Services, Deloitte & Touche; Transcript of SSN Workshop (Dec. 10, 2008) at 96-97, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles; Transcript of SSN Workshop (Dec. 11, 2007) at 51, Remarks of Stuart Pratt, President and CEO, Consumer Data Industry Association.

73 Transcript of SSN Workshop (Dec. 11, 2007) at 106, Remarks of James Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies; Transcript of SSN Workshop (Dec. 10, 2007) at 143, Remarks of Jim Davis, Associate Vice Chancellor for Information Technology & CIO, University of California-Los Angeles; Transcript of SSN Workshop (Dec. 10, 2007) at 46-47 and (Dec. 11, 2007) at 110-12, Remarks of Chris Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology and Public Policy Clinic, UC Berkeley School of Law.

74 FTC Staff Summary, at 41; Strategic Plan, at 34-35.

75 *See, e.g.*, "Deter, Detect, Defend: Avoid ID Theft," Federal Trade Commission, available at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.pdf.

76 *See, e.g.*, FTC Staff Summary, at 23-26; Transcript of SSN Workshop (Dec. 10, 2007) at 111-13, 117-18, Remarks of Bill Schaumann, Senior Manager, Ernst & Young.