PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON SOCIAL SECURITY

of the

HOUSE COMMITTEE ON WAYS AND MEANS

on

Protecting the Privacy of the Social Security Number from Identity Theft

Washington, DC

June 21, 2007

I. INTRODUCTION

Chairman McNulty, Ranking Member Johnson, and Members of the Subcommittee, I am Joel Winston, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the role of Social Security numbers ("SSNs") in identity theft and options to enhance their protection.

Identity theft is a pernicious crime and controlling it is a critical component of the Commission's consumer protection mission. This testimony describes the nature and scope of identity theft and the critical role that SSNs play both in creating and solving the problem. The testimony also summarizes the recommendations of the President's Identity Theft Task Force ("Task Force") with respect to preventing misuse of SSNs and, more broadly, combating identity theft. Finally, the testimony describes the Commission's law enforcement and education and outreach efforts on identity theft.

SSNs provide many valuable functions in our information-based economy. At the same time, they may help criminals to steal consumers' identities. The Task Force has recommended comprehensive reviews of both private and public sector usage of SSNs, which are ongoing. Ultimately, the objective of any SSN restrictions should be to reduce *unnecessary* transfer or use of SSNs, without inadvertently burdening *necessary* transfers or uses. Identity theft must be attacked on other fronts as well, from improving data security to keep sensitive information out

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any individual Commissioner.

of the hands of criminals, to educating consumers to better protect their information, to developing more effective means of authenticating consumers so that criminals who do obtain sensitive information cannot use it to open new accounts or access existing ones.

II. THE IDENTITY THEFT PROBLEM

Millions of consumers are victimized by identity thieves every year, collectively costing consumers and businesses billions of dollars and countless hours repairing the damage.[2] Beyond its direct costs, concerns about identity theft harm our economy by threatening consumers' confidence in the marketplace generally, and in electronic commerce specifically. A Wall Street Journal/Harris Interactive survey, for example, found that, as a result of fears about protecting their identities, 30 percent of consumers polled were limiting their online purchases, and 24 percent were cutting back on their online banking.[3]

There are two predominant varieties of financial identity theft: the takeover or misuse of existing credit card, debit card, or other accounts ("existing account fraud"); and the use of stolen information to open new accounts in the consumer's name ("new account fraud"). New account fraud, although less prevalent, typically causes considerably more harm to consumers.[4]

---

[2] *See, e.g.,* Javelin Strategy and Research, *2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary* (February 2007), http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf.

[3] *See* Jennifer Cummings, *Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft*, Wall St. J. Online, May 18, 2006, http://www.harrisinteractive.com/news/newsletters/WSJfinance/HI_WSJ_PersFinPoll_2006_vol2_iss05.pdf.

[4] In many cases, consumers suffer no direct monetary loss from existing account fraud. Federal law limits consumers' liability for unauthorized credit card charges to $50 per card, if the consumer notifies the credit card company within 60 days of the unauthorized charge. *See* 12 C.F.R. § 226.12(b). Many credit card companies do not require consumers to pay the $50

SSNs are valuable to identity thieves in committing both types of identity theft. Financial institutions generally require SSNs to open new accounts, either by law or because SSNs enable them to obtain creditworthiness information from consumer reporting agencies. In addition, SSNs often are used to control access to existing accounts by serving as internal identifiers to match consumers with their records, and for consumer authentication purposes.[5]

III. USES AND SOURCES OF SOCIAL SECURITY NUMBERS

SSNs play an important role in our economy. With 300 million American consumers, many of whom share the same name,[6] the unique 9-digit SSN is a key identification tool for businesses, government, and others.[7] For example, consumer reporting agencies use SSNs to ensure that the data furnished to them is placed in the correct file and that they are providing a credit report on the correct consumer.[8] Businesses and other entities use these reports in making eligibility and pricing decisions for a variety of products and services, including credit, insurance, home rentals, or employment. Additionally, SSNs are used in locator databases to find lost

---

and will not hold consumers liable for the unauthorized charges, no matter how much time has elapsed since the discovery of the loss or theft of the card. Different rules apply for debit cards and checking accounts.

[5] For example, a financial institution may ask an account holder for his SSN to confirm his identity before providing access to his account.

[6] According to the Consumer Data Industry Association, 14 million Americans have one of ten last names, and 58 million men have one of ten first names.

[7] *See* General Accounting Office, *Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information* (GAO 04-01) (2004).

[8] *See Federal Trade Commission - Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* at 38-40 (2004), http://www.ftc.gov/reports/facta/041209factarpt.pdf.

beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments. SSN databases also are used to fight identity fraud – for example, to confirm that an SSN provided by a loan applicant does not, in fact, belong to someone who is deceased. Federal, state, and local governments rely extensively on SSNs in administering programs that provide services to consumers,[9] and businesses in many circumstances are required to collect SSNs.[10]

SSNs are available from both public and private sources. Public records in city and county government offices across the country, including birth and death records, property records, tax lien records, voter registrations, licensing records, and court records, often contain consumers' SSNs.[11] As these records are increasingly placed online, access to large stores of SSNs becomes easier and less costly. Improved access to public records has important public policy benefits, but at the same time raises significant privacy concerns. Some public records

---

[9] For example, the Federal government uses SSNs to administer the federal jury system, federal welfare and worker's compensation programs, and military draft registration. *See* Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), *available at* www.ssa.gov/history/reports/ssnreportc2.html.

[10] Employers must collect SSNs for tax reporting purposes, for example, and health care providers may need them to obtain Medicare reimbursement.

[11] As of 2004, 41 states and the District of Columbia, as well as 75 percent of U.S. counties, displayed SSNs in public records. Government Accounting Office, *Social Security Numbers: Government Could Do More to Reduce Display in Public Records and on Identity Cards,* at 2 (Nov. 2004), *available at* http://www.gao.gov/new.items/d0559.pdf. Some governmental offices have been reducing their reliance on SSNs for administrative purposes in response to identity theft concerns. For example, only a few states still use SSNs as driver's license numbers. *See* David A. Lieb, *Millions of Motorists Have Social Security Numbers on Licenses*, The Boston Globe, Feb. 6, 2006, http://www.boston.com/news/local/massachusetts/articles/2006/02/06/millions_of_motorists_have_social_security_numbers_on_licenses/. In some cases, however, governments still use SSNs as identifiers when it is not essential to do so. *See* Mark Segraves, *Registering to Vote May Lead to Identity Theft*, WTOP Radio, Mar. 22, 2006, *available at* http://www.wtop.com/?nid=428&sid=733727.

offices redact sensitive information such as SSNs, but doing so can be very costly, particularly when it involves records that already are contained within a system.

There also are a number of private sources of SSNs, including consumer reporting agencies that list name, address, and SSN as part of the "credit header" information on consumer reports. Data brokers also collect personal information, including SSNs, from a variety of sources and compile and resell that data to third parties for a variety of purposes.[12]

Although SSNs sometimes are necessary for legal compliance or business purposes, other uses are more a matter of convenience or habit. For example, some organizations use SSNs as internal identifiers or as identification numbers displayed on cards because they always have done so, even though they could generate alternate identifiers of their own. Many organizations are taking steps to switch to alternate identifiers, although changing systems and procedures entails costs.[13]

The widespread use of SSNs makes them readily available and valuable to identity thieves. The challenge is to find the proper balance between the need to keep SSNs out of the hands of identity thieves and the need to give businesses and government entities sufficient means to attribute information to the correct person.

---

[12] Some data brokers are voluntarily restricting the sale of SSNs and other sensitive information to those with a demonstrable and legitimate need. *See Social Security Numbers Are for Sale Online*, Newsmax.com, Apr. 5, 2005, *available at* http://www.newsmax.com/archives/articles/2005/4/4/155759.shtml.

[13] *See James Hilton, U.Va.'s Vice President and Chief Information Officer, Issues Message About Security*, UVa Today, Jan. 17, 2007, *available at* http://www.virginia.edu/uvatoday/newsRelease.php?id=1323. Some health insurance providers have stopped using SSNs as subscriber identification numbers. *See* www.wpsic.com/edi/comm_sub_p.shtml?mm=3.

IV. CURRENT LAWS RESTRICTING THE USE OR DISCLOSURE OF SOCIAL SECURITY NUMBERS

There are a variety of specific statutes and regulations that restrict disclosure of certain consumer information, including SSNs, in particular contexts. In addition, under some circumstances, entities are required to have procedures in place to ensure the security and integrity of sensitive consumer information such as SSNs. Three statutes that protect SSNs from improper access fall within the Commission's jurisdiction: Title V of the Gramm-Leach-Bliley Act ("GLBA");[14] Section 5 of the Federal Trade Commission Act ("FTC Act");[15] and the Fair Credit Reporting Act ("FCRA"),[16] as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act").[17]

A. The Gramm-Leach-Bliley Act

The GLBA imposes privacy and security obligations on "financial institutions."[18] Financial institutions are defined broadly as those entities engaged in "financial activities" such as banking, lending, insurance, loan brokering, and credit reporting.[19]

1. Privacy of Consumer Financial Information

---

[14] 15 U.S.C. §§ 6801-09.

[15] 15 U.S.C. § 45(a).

[16] 15 U.S.C. §§ 1681-1681x, as amended.

[17] Pub. L. No. 108-159, 117 Stat. 1952.

[18] 15 U.S.C. § 6809(3)(A).

[19] 12 C.F.R. §§ 225.28, 225.86.

In general, financial institutions are prohibited by Title V of the GLBA[20] from disclosing nonpublic personal information, including SSNs, to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.[21] However, the GLBA includes a number of statutory exceptions under which disclosure is permitted without notice or a right to opt-out. These exceptions include for purposes of consumer reporting (pursuant to the FCRA), fraud prevention, law enforcement and regulatory or self-regulatory purposes, compliance with judicial process, and public safety investigations.[22] Entities that receive information under an exception to the GLBA are subject to reuse and redisclosure restrictions of the GLBA Privacy Rule, even if those entities are not themselves financial institutions.[23] Specifically, the recipients may only use and disclose the information "in the ordinary course of business to carry out the activity covered by the exception under which . . . the information [was received]."[24]

2. Safeguards for Customer Information

The GLBA also requires financial institutions to implement appropriate physical,

---

[20] *See* 15 U.S.C. § 6802; Privacy of Consumer Financial Information, 16 C.F.R. Part 313 ("GLBA Privacy Rule").

[21] *See* 15 U.S.C. § 6809. The GLBA defines "nonpublic personal information" as any information that a financial institution collects about an individual in connection with providing a financial product or service to an individual, unless that information is otherwise publicly available. This includes basic identifying information about individuals, such as name, SSN, address, telephone number, mother's maiden name, and prior addresses. *See, e.g.,* Privacy of Consumer Financial Information, 16 C.F.R. Part 313 ("GLBA Privacy Rule").

[22] 15 U.S.C. § 6802(e).

[23] 16 C.F.R. § 313.11(a).

[24] *Id.*

technical, and procedural safeguards to protect the security and integrity of the information they receive from customers, whether directly or from other financial institutions.[25] The FTC's Safeguards Rule, which implements these requirements for entities under FTC jurisdiction,[26] requires financial institutions to develop a written information security plan that describes their procedures to protect customer information. Given the wide variety of entities covered, the Safeguards Rule requires that security plans account for each entity's particular circumstances - its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. It also requires covered entities to take certain procedural steps - for example, designating appropriate personnel to oversee the security plan, conducting a risk assessment, and overseeing service providers - in implementing their plans.

B. Section 5 of the FTC Act

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[27] Under the FTC Act, the Commission has broad jurisdiction over a wide variety of entities and individuals operating in commerce. Under the Commission's deception authority, it

---

[25] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule").

[26] The Federal Deposit Insurance Corporation, the National Credit Union Administration ("NCUA"), the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, and state insurance authorities have promulgated comparable information safeguards rules, as required by Section 501(b) of the GLBA. 15 U.S.C. § 6801(b); *see, e.g.*, Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616-41 (Feb. 1, 2001). The FTC has jurisdiction over entities not subject to the jurisdiction of these agencies.

[27] 15 U.S.C. § 45(a).

is unlawful to make false claims about one's privacy procedures or security protections.[28]

In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.[29] The Commission has used this authority to challenge a variety of injurious practices, including companies' failure to provide reasonable and appropriate security for sensitive customer data.[30] The Commission can obtain injunctive relief for violations of Section 5, as well as consumer redress or disgorgement in appropriate cases.

C. The Fair and Accurate Credit Transactions Act of 2003

The FACT Act amended the FCRA to include a number of provisions designed to increase the protection of sensitive consumer information, including SSNs. One such provision required the banking regulatory agencies, the National Credit Union Administration ("NCUA"), and the Commission to promulgate a coordinated rule, requiring all users of consumer report information to have reasonable procedures to dispose of it properly and safely.[31] This Disposal

---

[28] Deceptive practices are defined as material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances. *Cliffdale Associates, Inc.*, 103 F.T.C. 110 (1984).

[29] 15 U.S.C. § 45(n).

[30] The Commission also has challenged as unfair the practice of imposing unauthorized charges in connection with "phishing," high-tech scams that use spam or pop-up messages to deceive consumers into disclosing credit card numbers, bank account information, SSNs, passwords, or other sensitive information. *See FTC v. Hill*, No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003), *available at* http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm; *FTC v. C.J.*, No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), *available at* http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

[31] 16 C.F.R. Part 382 ("Disposal Rule").

Rule, which took effect on June 1, 2005, helps reduce the risk of improper disclosure of SSNs. In addition, the FACT Act requires consumer reporting agencies to truncate the SSN on consumer reports at the consumer's request when providing the reports to the consumer.[32] Eliminating the unnecessary display of this information could lessen the risk of it getting into the wrong hands.

D. Other Laws

Other federal laws not enforced by the Commission regulate certain specific classes of information, including SSNs. For example, the Driver's Privacy Protection Act ("DPPA")[33] prohibits state motor vehicle departments from disclosing personal information in motor vehicle records, subject to fourteen "permissible uses," including law enforcement, motor vehicle safety, and insurance. The Health Information Portability and Accountability Act ("HIPAA") and its implementing privacy rule prohibit the disclosure to third parties of a consumer's medical information without prior consent, subject to a number of exceptions (such as, for the disclosure of patient records between entities for purposes of routine treatment, insurance, or payment).[34] Like the GLBA Safeguards Rule, the HIPAA Privacy Rule also requires entities under its jurisdiction to have in place "appropriate administrative, technical, and physical safeguards to

---

[32] 15 U.S.C. § 1681g(a)(1)(A). The FTC advises consumers of this right through its consumer outreach initiatives. *See, e.g.,* the FTC's identity theft prevention and victim recovery guide, *Take Charge: Fighting Back Against Identity Theft* at 5 (2005), *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf.

[33] 18 U.S.C. §§ 2721-25.

[34] 45 C.F.R. Part 164 ("HIPAA Privacy Rule").

protect the privacy of protected health information."[35]

V. TASK FORCE RECOMMENDATIONS REGARDING THE USE OF SSNS

On May 10, 2006, the President established an Identity Theft Task Force. Comprised of 17 federal agencies, including the FTC, the mission of the Task Force is to develop a comprehensive national strategy to combat identity theft.[36] The President specifically directed the Task Force to make recommendations on ways to improve the effectiveness and efficiency of the Federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution.

In April 2007, the Task Force published a strategic plan for combating identity theft.[37] Broadly, the plan is organized around the life cycle of identity theft – from the thieves' attempts to obtain sensitive information to its impact on victims – and identifies roles for consumers, the private sector, government agencies, and law enforcement.

The strategic plan also describes how identity thieves come into possession of consumers' SSNs and how they use them to steal identities. It concludes that "[m]ore must be done to eliminate unnecessary uses of SSNs."[38] Accordingly, several of the Task Force recommendations focus on SSNs and their use in the public and private sectors. With respect to the public sector, the Task Force recommended that:

---

[35] *Id.* at § 164.530(c).

[36] Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

[37] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("strategic plan") is available at www.idtheft.gov.

[38] Strategic Plan, at 25.

- the Office of Personnel Management ("OPM") review its use of SSNs in collecting human resource data from federal agencies and on OPM forms, and take steps to eliminate, restrict, or conceal their use wherever possible (including assigning employee identification numbers where practicable).[39]

- OPM issue guidance to federal agencies on how to restrict, conceal, or mask SSNs in employee records.

- The Social Security Administration develop a clearinghouse of agency "best practices" for minimizing the use and display of SSNs.

- The Office of Management and Budget complete its analysis of responses to its survey on agency uses of SSNs.

- The Task Force work with state and local governments to explore ways to eliminate unnecessary use and display of SSNs.

The Task Force also recommended an analysis of private sector reliance on SSNs. As discussed in Section III, it is well-understood that the private sector uses SSNs in a many ways to match information with individuals. What is less clear is the extent to which such uses are driven by business necessity, as opposed to convenience or habit, and what direct and indirect costs would be entailed in requiring businesses to use alternate identifiers. Therefore, the strategic plan recommends that the Task Force develop a comprehensive record on the uses of the SSN in the private sector and evaluate their necessity. By the first quarter of 2008, the Task Force will make recommendations to the President on whether additional steps should be taken regarding the use of SSNs.

VI. COMMISSION ACTIVITIES TO COMBAT IDENTITY THEFT

As described earlier, to successfully combat identity theft, it must be attacked at several different points in its life cycle. First, SSNs and other sensitive data must be kept out of the

---

[39] *Id.* The OPM review has been completed.

hands of data thieves by, among other things, limiting the availability of such data and improving the manner in which those who collect such data safeguard it.[40] Second, it must be made more difficult for thieves to use data they steal to open or access accounts in the victims' names by, among other ways, improving methods to authenticate consumers.[41] Third, identity theft must be deterred through more effective prosecution of criminals responsible for these acts.[42]

Through its longstanding efforts to combat identity theft through law enforcement and consumer and business education, and its recent implementation of the Task Force recommendations, the Commission has and is continuing to act aggressively on each of these fronts.

A. Data Security

Public awareness of, and concerns about, data security have reached new heights as reports about breaches of sensitive personal information continue to proliferate. Recent breaches have touched both the public and private sectors. Of course, not all data breaches result in identity theft and, in fact, many may lead to no harm whatsoever. Nonetheless, some breaches - especially those that result from deliberate actions, such as hacking, by criminals - have led to fraud.

A number of bills have been introduced in the past two sessions of Congress that would require businesses that maintain sensitive consumer information to have reasonable protections in place to prevent unauthorized access, as well as to require companies that suffer a data breach

---

[40] *Id.* at 22-42.

[41] *Id.* at 42-45.

[42] *Id.* at 52-71.

to provide notice to affected consumers. At the same time, well over half of the states have enacted data security and/or breach notification laws. The Commission and the Task Force have recommended that Congress establish national standards for data security and breach notification.[43]

1. Law Enforcement

Pending the enactment of national standards, the FTC enforces several existing laws and regulations that, explicitly or implicitly, contain data security requirements, including the GLBA Safeguards Rule, the FCRA's "know your customer" requirements,[44] and the FTC Act. Since 2001, the Commission has brought fourteen cases challenging businesses that failed to reasonably protect sensitive consumer information that they maintained.[45] In a number of these cases, the Commission alleged that the company had misrepresented the nature or extent of its security procedures in violation of the FTC Act's prohibition on deceptive practices.[46] In some

---

[43] *See* Statement of Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft, at 7 (June 16, 2005) *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf; Strategic Plan, at 34-37.

[44] 15 U.S.C. § 1681 *et seq*. The FCRA specifies that consumer reporting agencies may provide consumer reports only for enumerated "permissible purposes," and requires that they have reasonable procedures to verify the identity and permissible purposes of prospective recipients of their reports.

[45] *See generally* http://www.ftc.gov/privacy/index.html.

[46] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 23, 2007); *In the Matter of Nations Title Agency, Inc*., FTC Docket No. C-4161 (June 19, 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 (March 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); *In the Matter of*

cases, the alleged security inadequacies led to breaches that caused substantial consumer injury and were challenged as unfair practices under the FTC Act.[47] Several cases involved alleged violations of the Safeguards Rule or the FCRA.[48]

Probably the best-known FTC data security case was its 2006 action against ChoicePoint, Inc., a data broker that allegedly sold sensitive information (including credit reports in some instances) on more than 160,000 consumers to data thieves posing as ChoicePoint clients. In turn, the thieves used that information in many instances to steal the consumers' identities. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of its information and ignored obvious red flags. For example, the company allegedly approved as purchasers individuals who lied about their credentials, used commercial mail drops and business addresses, and faxed multiple applications from nearby commercial photocopying facilities. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties for violations of the FCRA and $5 million in consumer redress for identity theft victims, and agreed

---

Microsoft Corp., FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.,* FTC Docket No. C-4047 (May 8, 2002).

[47] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *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 (March 7, 2006); *In the Matter of BJ's Wholesale Club, Inc.,* FTC Docket No. C-4148 (Sept. 20, 2005).

[48] *E.g., United States v. ChoicePoint, Inc*., No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Nations Title Agency, Inc*., FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.,* FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Nationwide Mortgage Group Inc.*, FTC Docket No. 9319 (April 15, 2005); *In the Matter of Sunbelt Lending Services,* FTC Docket No. C-4129 (Jan. 3, 2005). In the *Nations Title, Nationwide Mortgage Group,* and *Sunbelt Lending Services* cases, the Commission also alleged that the companies violated the GLBA's privacy provisions and the FTC's implementing Privacy Rule, which, among other things, require financial institutions to provide notices to their customers describing their information-sharing policies.

to undertake substantial new data security measures.[49]

The Commission's most recent data security enforcement action involved Guidance Software, Inc., a marketer of software and related services for investigating and responding to computer breaches and other security incidents. According to the FTC complaint, Guidance, contrary to its claims, failed to implement simple, inexpensive, and readily available security measures to protect consumers' data, for example, by failing to defend against commonly-known or reasonably foreseeable web attacks, and by permanently storing credit card information in clear, readable text rather than encrypting or otherwise protecting it.[50]

Although the Commission's data security cases have been brought under different laws, they share common elements: the vulnerabilities were multiple and systemic, and readily-available and often inexpensive measures were available to prevent them. Together, the cases stand for the proposition that companies should maintain reasonable and appropriate measures to protect sensitive consumer information. The Commission will continue to apply these principles in enforcing existing data security laws.

2. Consumer and Business Education

The Commission has made substantial efforts to increase consumer and business awareness of the importance of protecting data and taking other steps to prevent identity theft.

---

[49] *See* FTC Press Release, *ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.html. The Commission has mailed more than 5,000 claims forms to possible victims and has created a website at which consumers can download the forms and obtain information about the claims process.

[50] *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 3, 2007).

The Commission works to empower consumers by providing them with the knowledge and tools to protect themselves from identity theft and to deal with the consequences when it does occur. The Commission receives about 15,000 to 20,000 contacts each week through its toll-free hotline and dedicated website regarding identity theft recovery, or how to avoid becoming a victim in the first place. Callers to the hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft. The FTC's identity theft primer[51] and victim recovery guide[52] are widely available in print and online. The Commission has distributed over 2 million copies of the primer and has recorded over 2.4 million visits to the Web version.

Last year, the Commission launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend."[53] It includes direct-to-consumer brochures, as well as training kits and ready-made materials (including presentation slides and a video) for use by businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. The Commission has distributed over 3.5 million brochures and 40,000 kits to date. The Commission also has partnered with other organizations to broaden its reach. As just one example, the U.S. Postal Inspection Service recently initiated an outreach campaign to place FTC educational materials on subway cars in New York, Chicago, San Francisco, and Washington D.C.

---

[51] *Avoid ID Theft: Deter, Detect, Defend, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm.

[52] *Take Charge: Fighting Back Against Identity Theft, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm.

[53] *See* http://www.ftc.gov/bcp/edu/microsites/idtheft.

The Commission also sponsors a multimedia website, OnGuard Online,[54] designed to educate consumers about basic computer security, including the importance of not disclosing personal information such as SSNs to possible fraudsters. OnGuard Online was developed in partnership with other government agencies and the technology sector, and since its launch has attracted more than 3.5 million visits.

The Commission directs its outreach to businesses as well. Recently, the FTC released a new business education guide related to data security.[55] Most companies have some information in their files - names, SSNs, credit card numbers - that identifies their customers and employees. The Commission has heard from some businesses, particularly smaller businesses, that they were not sure what data security measures they should take to protect such sensitive information from falling into the wrong hands. The Commission, therefore, developed a brochure that articulates the key steps that are part of a sound data security plan. The Commission anticipates that the brochure will be a useful tool in alerting businesses to the importance of data security issues and give them a solid foundation on how to address those issues.

B. Limiting Unnecessary Uses of SSNs

As described earlier, the Task Force recommended that agencies undertake a comprehensive review of the public and private sector uses of SSNs, with the goal of identifying unnecessary uses that could be eliminated. Efforts to evaluate and limit government collection,

---

[54] *See* http://www.onguardonline.gov/index.html.

[55] *Protecting Personal Information: A Guide for Business, available at* http://www.ftc.gov/infosecurity.htm. Other business publications on data security and responding to data breaches are available at http://www.ftc.gov/bcp/edu/microsites/idtheft.htm.

use, and disclosure through the OPM and OMB are well underway. At the same time, the Commission, assisted by other Task Force agencies, has begun implementing the review of private sector uses. Commission staff is developing a number of outreach opportunities to learn from stakeholders on this issue.

C. Authentication

Restricting unnecessary uses of SSNs and better data security are not the only means of preventing SSN misuse. Even the most effective efforts cannot prevent thieves from obtaining sensitive information in all cases. For that reason, it is important to make this information less useful to thieves by making it more difficult for them to use it to steal an identity. To accomplish this goal, better methods of authenticating consumers - for example, proving that the individual is who she purports to be - must be developed.

To that end, the Task Force recommended holding a workshop on improving authentication methods, which the Commission hosted on April 23 and 24, 2007. The workshop was designed to facilitate discussions about the technological and policy issues surrounding the development of improved authentication procedures.[56] A number of themes emerged during the course of the two days of discussions. First, there is no single "right" way to authenticate individuals, but rather there are a number of promising techniques being developed and implemented that use multiple layers of security, including biometrics and smart cards. Identity thieves are increasingly sophisticated and adept at defeating authentication efforts, so that it is critical that new techniques continue to be developed to stay "a step ahead" of the thieves.

---

[56] *See Proof Positive: New Directions for ID Authentication* at http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml.

Participants also agreed that consumer convenience and usability are critical - consumers will reject authentication procedures that are too burdensome. And, there was general agreement that the government can play an important role in this area by encouraging and facilitating the development of better authentication. Commission staff currently is drafting a summary report of the workshop proceedings.

D. Criminal Prosecution

The Task Force strategic plan contains a detailed discussion of how identity thieves currently are investigated and prosecuted. The plan recommends numerous actions - from strengthening criminal statutes, to better coordinating domestic and international efforts, to more training of law enforcement investigators and prosecutors, to the establishment of an interagency National Identity Theft Law Enforcement Center to enhance information sharing among law enforcers. Although the Commission lacks criminal jurisdiction itself, it will play an active role in implementing these recommendations.

VII. CONCLUSION

Identity theft remains a serious problem in this country, causing enormous harm to consumers, businesses and ultimately our economy. Succeeding in the battle against identity theft will require the public and private sectors, working together, to make it more difficult for thieves both to obtain sensitive information and to use the information they are able to procure to steal identities. To prevent thieves from obtaining sensitive information, government and the business community should, first, limit the information they collect and maintain from or about consumers - including SSNs - to that necessary to meet clear legal or business needs, and,

second, to better protect the data they do collect. In addition, to keep thieves from using the information they do procure to steal identities, consumer authentication techniques must be improved. The Task Force's strategic plan provides a blueprint for achieving these goals, and the Commission will continue to play a central role in the battle against identity theft.