PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON SOCIAL SECURITY

of the

HOUSE COMMITTEE ON WAYS AND MEANS

on

Protecting Social Security Numbers from Identity Theft

Washington, DC

April 13, 2011

I. INTRODUCTION

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, I am Maneesha Mithal, 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 how Social Security numbers ("SSNs") are used in identity theft. Protecting consumers against identity theft and its consequences is a critical component of the Commission's consumer protection mission.[2]

This testimony begins by describing the nature of identity theft and the role SSNs play in facilitating it. It then summarizes the work that federal and state agencies have done to prevent the misuse of SSNs in the public sector, as well as the recommendations of the Commission's 2008 Report on preventing the misuse of SSNs in the private sector.[3] Finally, the testimony describes the Commission's law enforcement, data collection and analysis, and education and outreach efforts on identity theft. In particular, it describes some of the 32 actions the

---

[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.

[2] *See* Identity Theft and Assumption Deterrence Act, Pub. L. 105-318, 112 Stat. 3007 (1998). Among other things, this Act directs the FTC to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. The repository of identity theft complaints, known as the "Identity Theft Clearinghouse," is discussed in greater detail below in Section IV.

[3] FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008) ("SSN Report"), *available at* www.ftc.gov/os/2008/12/P075414ssnreport.pdf.

Commission has brought since 2001 challenging businesses that failed to reasonably protect sensitive consumer information that they maintained, including SSNs.

II. THE ROLE OF SOCIAL SECURITY NUMBERS IN IDENTITY THEFT

Millions of consumers are victimized by identity thieves each year,[4] collectively costing consumers and businesses billions of dollars[5] and countless hours to repair the damage. 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").[6] SSNs are valuable to identity thieves in committing both of these types of identity theft.

SSNs are widely used throughout our economy. With 300 million American consumers, many of whom share the same name, the unique nine-digit SSN provides a key tool to identify individual consumers.[7] Financial institutions, insurers, businesses, universities, health care providers, government, and others use SSNs to ensure accurate matching of consumers with their information within organizations, to match consumers with information held by other organizations, and to avoid the costs and burdens of establishing different identification systems

---

[4] *See* Bureau of Justice Statistics, *National Crime Victimization Survey Supplement, Victims of Identity Theft, 2008* (Dec. 2010) ("BJS Supplement") at 1-2 (finding 11.7 million persons, representing 5% of all Americans age 16 or older, were victims of identity theft during a two-year period).

[5] *Id.* at 4 (finding the total financial cost of identity theft was 17.3 billion dollars over a two-year period).

[6] Although less prevalent, new account fraud typically causes considerably more harm to consumers.

[7] *See generally* General Accounting Office, *Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information* (GAO 04-01) (2004), *available at* http://www.gao.gov/new.items/d0411.pdf.

for each set of consumer records. For example, 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 authentication purposes. Consumer reporting agencies use SSNs to ensure that data furnished to them is placed in the correct consumer file and that they are providing a credit report on the correct consumer. 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. At the same time, SSN databases also are used to fight identity fraud – for example, to confirm that a SSN provided by a loan applicant does not, in fact, belong to someone who is deceased.

Additionally, federal, state, and local governments rely extensively on SSNs in administering programs and providing services to consumers.[8] For example, the Internal Revenue Service ("IRS") requires private sector entities, including banks, insurance companies, and employers, to collect SSNs for income and tax-related purposes. The federal government also uses SSNs to administer the federal jury system, as well as federal welfare and worker's compensation programs. SSNs are also used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments.

The widespread use of SSNs to identify individuals in both the private and public sectors makes them readily available and valuable to identity thieves. Thieves gather SSNs in many

---

[8] *See* Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), Chapter II, *available at* www.ssa.gov/history/reports/ssnreportc2.html.

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).[9] The challenge in combating the misuse of SSNs 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.

III. ACTIONS AND RECOMMENDATIONS TO PREVENT MISUSE OF SOCIAL SECURITY NUMBERS

Over the past several years, the federal government has taken numerous steps to prevent the misuse of SSNs in the public sector.[10] For example, the Office of Personnel Management ("OPM") has been reviewing its use of SSNs in collecting human resource data from federal agencies and on OPM forms, and taking steps to eliminate, restrict, or conceal their use whenever possible.[11] Further, OPM issued guidance to federal agencies on the appropriate and

---

[9] SSN Report, *supra* note 3, at 3.

[10] In May 2006, President Bush established an Identity Theft Task Force, comprised of 17 federal agencies, and co-chaired by the FTC's Chairman. The Task Force's mission was to develop a comprehensive national strategy to combat identity theft. *See* The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (April 2007), *available at* www.identitytheft.gov/reports/StrategicPlan.pdf. In September 2008, the Task Force published its recommendations. *See* The President's Identity Theft Task Force, *Task Force Report* (Sept. 2008) ("Task Force Report"), *available at* www.idtheft.gov/reports/IDTReport2008.pdf. A number of the activities described in this section are the result of these recommendations. Federal agencies continue to implement the Task Force recommendations. For example, the Department of Defense recently announced the discontinuance of SSNs on identification cards beginning June 1, 2011. A news release explaining this policy is available at www.defense.gov/news/newsarticle.aspx?id=63409.

[11] Task Force Report, *supra* note 10, at 6-7.

inappropriate use of SSNs in federal employee records.[12] Additionally, the FTC, Social Security Administration ("SSA"), and IRS have coordinated with states and local governments to encourage: (1) a reduction in the need for, and display of, SSNs on public documents, especially online documents, (2) the improvement of data security, and (3) the protection of tax payer information.[13]

With respect to private sector uses of SSNs, the FTC hosted a two-day workshop in December 2007 to examine ways to make SSNs less valuable and less accessible to identity thieves. In December 2008, the Commission issued a report, containing four legislative recommendations in this area.[14] The Commission continues to believe that these recommendations are still needed.

First, the Commission recognized that because there has been widespread use and availability of SSNs, any solution to the misuse of SSNs must include reducing their value to identity thieves through improved consumer authentication.[15] As detailed in the report, this can be achieved by encouraging or requiring all private sector businesses and organizations that have

---

[12] Task Force Report, *supra* note 10, at 7. On June 18, 2007, OPM issued "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft" to the Chief Human Capital Officers of all federal departments and agencies, *available at* www.chcoc.gov/Transmittals/Attachments/trans847.pdf. That Guidance has two goals: (1) to eliminate the unnecessary use of SSNs in federal personnel records; and (2) to strengthen the protection of employees' sensitive information from theft or loss.

[13] Task Force Report, *supra* note 10, at 9-10.

[14] *See generally* SSN Report, *supra* note 3.

[15] *Id.* at 6-7. "Authentication" is the process of verifying that someone is who he or she claims 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. Good authentication reduces the likelihood that identity thieves can use stolen data to assume another's identity.

consumer accounts to adopt appropriate, risk-based consumer authentication programs that do not rely on SSNs alone to authenticate consumers. This approach would make it more difficult for thieves to use SSNs to open new accounts or access existing accounts.[16] To that end, the Commission recommended that Congress consider establishing national consumer authentication standards to verify that consumers are who they purport to be.[17]

Second, the Commission recommended that Congress consider creating national standards to reduce the public display and transmission of SSNs, such as by eliminating their unnecessary display on publicly-available documents and identification cards and limiting how they can be transmitted.[18] Such steps would reduce the availability of SSNs to thieves, without hindering the use of SSNs for legitimate identification and data-matching purposes.

Third, the Commission recognized that an important step in limiting identity thieves' access to SSNs is for entities that collect and store them to maintain reasonable safeguards against unauthorized access. Thus, the Commission expressed support for national data security standards that would cover SSNs in the possession of any private sector entity.

Finally, the Commission supported national data breach notification standards requiring private sector entities to provide public notice when they suffer a breach of consumers' personal

---

[16] Congress directed the Commission and banking regulatory agencies to promulgate a rule requiring certain covered entities to be on guard against "red flags" of possible identity theft in their day-to-day operations. The resulting Red Flags Rule suggests that one way to detect the red flags of identity theft is to have in place procedures for authenticating customers. *See* 16 C.F.R. Part 681.

[17] The SSN report recommended that an authentication requirement cover all private sector entities that maintain consumer accounts, other than financial institutions already subject to authentication requirements promulgated by bank regulatory agencies. SSN Report, *supra* note 3, at 6.

[18] *Id*. at 8-9.

information.[19] In addition to alerting affected consumers to protect themselves, such a law would have the indirect benefit of motivating companies to weigh their need to collect SSNs against the potential cost and liability that may ensue if collected SSNs are compromised.[20]

IV. COMMISSION ACTIVITIES TO COMBAT IDENTITY THEFT

In addition to making these recommendations, the Commission has used its existing authority and resources to implement a longstanding and comprehensive program to combat identity theft, acting aggressively on three fronts: law enforcement, data collection, and consumer and business education.

A. Law Enforcement

The Commission enforces a variety of specific statutes and regulations that restrict disclosure of SSNs in particular contexts. For example, the Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to truncate the SSN on consumer reports at the consumer's request when providing the reports to the consumer.[21] Eliminating the unnecessary display of this information could lessen the risk of it getting into the wrong hands.

---

[19] Congress enacted a federal breach notification law in the health area, enforced by the Department of Health and Human Services and the FTC. *See* American Recovery and Reinvestment Act of 2008, Pub. L. 111-5, 123 Stat. 155 (2009). To implement this law, the Commission promulgated the Health Breach Notification Rule, 16 C.F.R. Part 318, which requires certain entities within the Commission's jurisdiction that offer personal health records and related services to provide consumers with notification in the event of a security breach.

[20] *See also* FTC Staff, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* www.ftc.gov/os/2010/12/101201privacyreport.pdf (recommending that companies should protect consumers by not collecting information they do not need, securing information they do collect, and not retaining information they no longer need).

[21] 15 U.S.C. § 1681(g).

In addition, the Commission enforces a variety of laws requiring entities, in some circumstances, to have reasonable procedures in place to secure consumer information, such as SSNs. For example, the Commission's Safeguards Rule under the Gramm-Leach-Bliley Act contains data security requirements for financial institutions.[22] The FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[23] and imposes safe disposal obligations on entities that maintain consumer report information.[24] In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices[25] in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.

Since 2001, the Commission has brought 32 law enforcement actions challenging businesses that failed to reasonably protect sensitive consumer information that they maintained. Several Commission cases have involved breaches of SSNs. One of the best-known FTC data security cases is the 2006 action against ChoicePoint, Inc., a data broker that allegedly sold sensitive information (including SSNs in some instances) concerning more than 160,000

---

[22] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[23] 15 U.S.C. § 1681e.

[24] *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[25] 15 U.S.C. § 45(a).

consumers to data thieves posing as ChoicePoint clients.[26] In many instances, the thieves used that information 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 security red flags. For example, the FTC alleged that the company approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from public 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 to undertake new data security measures.[27]

More recently, the Commission reached settlements with two pharmacy chains – CVS Caremark[28] and Rite Aid[29] – alleging that both companies failed to take reasonable and appropriate security measures to protect sensitive financial and medical information concerning customers and employees. As a result, information such as employment records and pharmacy labels were found in open trash dumpsters. Settlements with the two companies require them to establish comprehensive information security programs.

---

[26] *United States v. ChoicePoint, Inc.,* No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006).

[27] In 2009, the Commission charged that the company violated the earlier court order and obtained a stipulated modified order under which ChoicePoint agreed to expand its data security obligations and pay monetary relief in the amount of $275,000. *United States v. ChoicePoint, Inc.,* No. 1:06-CV-0198-JTC (N.D. Ga. (settlement entered on Oct. 14, 2009). In bringing cases under section 5, Commission staff routinely collaborate with state Attorneys General and other federal and state authorities, as it did in *Choicepoint*.

[28] *CVS Caremark Corp.*, FTC No. C-4259 (June 18, 2009).

[29] *Rite Aid Corporation.*, FTC No. C-4308 (Nov. 12, 2010).

Finally, earlier this year, the Commission settled actions against three credit report resellers,[30] alleging violations of the FCRA, the FTC Act, and the Safeguards Rule. Due to their lack of information security policies and procedures, these companies allegedly allowed clients without basic security measures, such as firewalls and updated antivirus software, to access sensitive consumer reports through an online portal. By failing to ensure that their clients maintained basic security protections when accessing the portal, the companies enabled hackers to access more than 1,800 credit reports without authorization. The settlements require each company, among other things, to have comprehensive information security programs in place to protect the security, confidentiality, and integrity of consumers' personal information.

B. Data Collection and Analysis

In addition to law enforcement, the Commission collects and analyzes identity theft complaint data in order to target its education efforts and assist criminal law enforcement authorities. The Commission manages the Identity Theft Clearinghouse, a secure online database of identity theft-related complaints. Identity theft victims can enter complaint information directly into the database via an online complaint form or by calling a toll-free identity theft hotline and speaking with a trained counselor. The Commission makes the Clearinghouse data available to over 2,000 American and Canadian federal, state, and local law enforcement agencies who have signed confidentiality and data security agreements.[31] Through

---

[30] *SettlementOne Credit Corp.,* FTC File No. 082 3208; *ACRAnet, Inc.,* FTC File No. 092 3088; *Fajilan and Assoc., Inc.*, FTC File No. 092 3089 (Feb. 3, 2011) (consent orders accepted for public comment). A news release and links to these cases is available at http://www.ftc.gov/opa/2011/02/settlement.shtm.

[31] For example, each of the 50 Offices of the Attorney General have access to the Clearinghouse data.

the Clearinghouse, law enforcers can search identity theft complaints submitted by victims, law enforcement organizations, and the Identity Theft Assistance Center, a not-for-profit coalition of financial services companies. To assist law enforcement and policy makers, the FTC also routinely issues reports on the number and nature of identity theft complaints received by the FTC.[32]

C. Consumer and Business Education

Consumer and business education is another important part of the Commission's mission. 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. Callers to the hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft.

Further, the FTC makes available a wide variety of consumer educational materials, including many in Spanish, to help consumers deter, detect, and defend against identity theft. For example, the FTC publishes a victim recovery guide – *Take Charge: Fighting Back Against Identity Theft*[33] – that explains the immediate steps identity theft victims should take to address the crime; how to obtain a credit report and correct fraudulent information in credit reports; how

---

[32] *See*, *e.g.,* FTC, *Consumer Sentinel Network Data Book for January - December, 2010* (Feb. 2011), *available at* http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf. The 2010 Data Book shows that over 250,000 consumers reported some form of identity theft, which represents 19% of the total number of complaints submitted to the Commission. This makes identity theft the most frequently reported category of consumer complaints, continuing a pattern that started over a decade ago.

[33] *Available at* www.ftc.gov/bcp/ed/pubs/consumers/idtheft/idt04.pdf.

to file a police report;[34] and how to protect personal information. The Commission has distributed over 3.8 million copies of the recovery guide and has recorded over 3.5 million visits to the Web version.

The Commission also sponsors a multimedia website, OnGuard Online,[35] designed to educate consumers about basic computer security, including the importance of not disclosing personal information such as SSNs to possible fraudulent operators. OnGuard Online was developed in partnership with other government agencies and technology companies. Visitors to the site can download educational games and videos, learn more about specific topics, including phishing and social networking, and obtain useful tips and information in an interactive format.

The Commission directs its outreach to businesses as well.[36] It has developed a brochure and an online tutorial[37] that set out the key components of a sound data security plan. These materials alert businesses to the importance of data security and give them a solid foundation on how to address those issues. In addition, the FTC creates business educational materials to

---

[34] The FCRA also provides identity theft victims with additional tools to recover from identity theft. For example, identity theft victims who provide police reports to a consumer reporting agency may obtain a seven-year fraud alert on their credit files, alerting potential users of their reports to exercise special vigilance in opening accounts in the consumers' names. In addition, victims may block fraudulent information on their credit files, obtain from creditors the underlying documentation associated with transactions that may have been fraudulent, and prohibit creditors from reporting fraudulent information to the consumer reporting agencies. *See* FCRA, 15 U.S.C. §§ 605A, 605B, 609(e), and 611.

[35] *Available at* www.onguardonline.gov. A Spanish-language counterpart, Alerta En Linea, is available at www.alertaenlinea.gov.

[36] *See* FTC, *Protecting Personal Information: A Guide for Business;* and FTC, *Information Compromise and Risk of Identity Theft: Guidance for Your Business.* Both publications are available at http://business.ftc.gov.

[37] The tutorial is available at www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html.

address particular risks. For example, the Commission developed a new business education brochure – *Peer-to-Peer File Sharing: A Guide for Business*[38] – to educate businesses about the risks associated with P2P file sharing programs and advise them about ways to address these risks.

Finally, the Commission leverages its resources by providing educational and training materials to "first responders." For example, because victims often report identity theft to state and local law enforcement agencies, the FTC informs law enforcers on how to talk to victims about identity theft.[39] The Commission also distributes a law enforcement resource CD Rom that includes information about how to assist victims, how to partner with other law enforcement agencies, how to work with businesses, and how to access the Identity Theft Clearinghouse. In addition, the FTC and its partners have provided identity theft training to over 5,400 state and local law enforcement officers from over 1,770 agencies.

Similarly, the FTC has encouraged the development of a nationwide network of *pro bono* clinics to assist low-income identity theft victims. As part of this initiative, the FTC has created a comprehensive guide for advocates providing legal assistance to identity theft victims. The Guide for Assisting Identity Theft Victims (*Pro Bono Guide)*[40] describes how advocates can intervene with creditors, credit reporting agencies, debt collectors, and others, and it provides self-help measures that victims can take to address their problems. Step-by-step instructions

---

[38] *Available at* www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm. Peer-to-Peer (P2P) technology enables companies to form a network in order to share documents and to facilitate online telephone conversations.

[39] Resources for law enforcement are available at www.ftc.gov/idtheft.

[40] The *Pro Bono Guide* is available at www.idtheft.gov/probono.

provide best practices for recovering from identity theft.

V. CONCLUSION

Identity theft remains a serious problem in this country, causing enormous harm to consumers, businesses, and ultimately our economy. The Commission will continue to play a central role in the battle against identity theft and looks forward to working with this Subcommittee on this important issue.