PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

IDENTITY THEFT AND SOCIAL SECURITY NUMBERS

Before the

SUBCOMMITTEE ON SOCIAL SECURITY

of the

HOUSE COMMITTEE ON WAYS AND MEANS

Washington, DC

March 30, 2006

I. INTRODUCTION

Mr. Chairman, Mr. Levin, 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 identity theft and Social Security numbers ("SSNs").

The Commission has a broad mandate to protect consumers generally and to combat identity theft specifically. Controlling identity theft is an issue of critical concern to all consumers – and to the Commission. The FTC serves a key role as the central repository for identity theft complaints, facilitates criminal law enforcement in detecting and prosecuting identity thieves, and provides extensive victim assistance and consumer education. In recognition of the need to protect sensitive consumer information and prevent identity theft, the FTC recently created a new Division of Privacy and Identity Protection. This division – which consists of staff with expertise in privacy, data security, and identity theft – addresses cutting-edge consumer privacy matters through aggressive enforcement, as well as rulemaking, policy development, and outreach to consumers and businesses.

This testimony describes the ways in which SSNs are collected and used, their relationship to identity theft, current laws that restrict the use or transfer of consumers' personal information, and the Commission's efforts to help consumers avoid identity theft or remediate its consequences.

---

[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 Commissioner.

II. THE IDENTITY THEFT PROBLEM

Identity theft is a pernicious crime that harms both consumers and businesses. Recent surveys estimate that nearly 10 million consumers are victimized by some form of identity theft each year.[2] The costs of this crime are staggering. The Commission's 2003 survey estimated that identity theft cost businesses approximately $50 billion, and cost consumers an additional $5 billion in out-of-pocket expenses, over the twelve-month period prior to the survey.[3] The 2003 survey looked at two major categories of identity theft: (1) misuse of existing accounts; and (2) the creation of new accounts in the victim's name. The 2003 survey found that the costs imposed by new account fraud were substantially higher than the misuse of existing accounts.[4]

III. USES AND SOURCES OF SOCIAL SECURITY NUMBERS

SSNs today play a vital role in our economy. With 300 million American consumers, many of whom share the same name,[5] the unique 9-digit SSN is a key identification tool for businesses, government, and others.[6] 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

---

[2] *See Federal Trade Commission - Identity Theft Survey Report* (2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf and Rubina Johannes, 2006 Identity Fraud Survey Report (2006), http://www.javelinstrategy.com/research. A free summary of the 2006 Identity Fraud Survey Report is available at http://www.bbb.org/alerts/article.asp?ID=651.

[3] *Federal Trade Commission - Identity Theft Survey Report* at 6 (2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[4] *Id.*

[5] 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.

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

credit report on the correct consumer.[7] Businesses and other entities use these reports to evaluate the risk of providing to individuals services, such as credit, insurance, home rentals, or employment. Timely access to consumer credit, as well as the overall accuracy of credit reporting files, could be compromised if SSNs could not be used to match consumers to their financial information. Additionally, SSNs are used in locator databases to find lost 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.[8] Without the ability to use SSNs as a personal identifier and fraud prevention tool, the granting of credit and the provision of other financial services would become riskier and more expensive and inconvenient for consumers.

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.[9] Increasingly, these records are being placed online where they can be

---

[7] *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.

[8] The federal government also uses the SSN as an identifier, for example, as both an individual's Medicare and taxpayer identification number. It also is used to administer the federal jury system, federal welfare and workmen's compensation programs, and military draft registration. *See* Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), www.ssa.gov/history/reports/ssnreportc2.html.

[9] Local and state governments are reducing their reliance on SSNs for many administrative purposes in response to identity theft concerns. For example, only a few states still use SSNs as drivers license numbers. *See* David A. Lieb, *Millions of Motorists Have Social*

accessed easily and anonymously.[10] There also are a number of private sources of SSNs, including consumer reporting agencies that include 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.[11]

The misuse of SSNs, however, can facilitate identity theft. For example, new account fraud - the most serious form of identity theft - is often possible only if the thief obtains the victim's SSN. The challenge is to find the proper balance between the need to keep SSNs out of the hands of identity thieves, while giving businesses and government entities sufficient means to attribute information to the correct person. Restrictions on disclosure of SSNs also could have a broad impact on such important purposes as public health, criminal law enforcement, and anti-fraud and anti-terrorism efforts. Moreover, as referenced above, regulation or restriction of the

---

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, http://www.wtop.com/?nid=428&sid=733727.

[10] Improved access to public records has important public policy benefits, but at the same time raises privacy concerns. Some public records offices redact sensitive information such as SSNs, but doing so can be very costly. The Commission has recognized the sensitive nature of SSNs, even when they are contained in publicly available records. For example, in response to a comment on the DSW order, the Commission stated that "[C]ertain publicly available records, such as court records, contain Social Security numbers and other highly sensitive information that can be used to perpetrate identity theft." The Commission response letter is available at http://www.ftc.gov/os/caselist/0523096/0523096DSW LettertoCommenter BankofAmerica.pdf.

[11] Some data brokers have announced that they 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, http://www.newsmax.com/archives/articles/2005/4/4/155759.shtml.

availability of SSNs in public records poses substantial policy and practical concerns.

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 certain 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");[12] Section 5 of the Federal Trade Commission Act ("FTC Act");[13] and the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"),[14] amending the Fair Credit Reporting Act ("FCRA").[15]

A. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act ("GLBA") imposes privacy and security obligations on "financial institutions."[16] Financial institutions are defined broadly as those entities engaged in "financial activities" such as banking, lending, insurance, loan brokering, and credit reporting.[17]

---

[12] 15 U.S.C. §§ 6801-09.

[13] 15 U.S.C. § 45(a).

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

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

[16] 15 U.S.C. § 6809(3)(A).

[17] 12 C.F.R. §§ 225.28, 225.86.

1. Privacy of Consumer Financial Information

In general, financial institutions are prohibited by Title V of the GLBA[18] 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.[19] However, the GLBA includes a number of statutory exceptions under which disclosure is permitted without having to provide notice and an opt-out. These exceptions include consumer reporting (pursuant to the FCRA), fraud prevention, law enforcement and regulatory or self-regulatory purposes, compliance with judicial process, and public safety investigations.[20] Entities that receive information under an exception to the GLBA are subject to the reuse and redisclosure restrictions of the GLBA Privacy Rule, even if those entities are not themselves financial institutions.[21] In particular, 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]."[22]

Entities can obtain SSNs from consumer reporting agencies, generally from the credit

---

[18] Privacy of Consumer Financial Information, 16 C.F.R. Part 313 ("GLBA Privacy Rule").

[19] 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.*, 65 Fed. Reg. 33,646, 33,680 (May 24, 2000) (the FTC's Privacy Rule).

[20] 15 U.S.C. § 6802(e).

[21] 16 C.F.R. § 313.11(a).

[22] *Id.*

header data on the credit report. However, because credit header data is typically derived from information originally provided by financial institutions, entities that receive this information generally are limited by the GLBA's reuse and redisclosure provision.

2. Required Safeguards for Customer Information

The GLBA also requires financial institutions to implement appropriate physical, technical, and procedural safeguards to protect the security and integrity of the information they receive from customers, whether directly or from other financial institutions.[23] The FTC's Safeguards Rule, which implements these requirements for entities under FTC jurisdiction,[24] 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 a plan that accounts 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

---

[23] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule").

[24] 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.

assessment, and overseeing service providers) in implementing their plans.[25]

B. Section 5 of the FTC Act

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[26] Under the FTC Act, the Commission has broad jurisdiction over a wide variety of entities and individuals operating in commerce. Prohibited practices include making deceptive claims about one's privacy procedures, including claims about the security provided for consumer information.[27]

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.[28] 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.[29]

---

[25] The Commission previously has recommended that Congress consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety. Such a requirement could extend the FTC's existing GLBA Safeguards Rule to companies that are not financial institutions. *See* Statement of Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft (June 16, 2005) at 7, http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

[26] 15 U.S.C. § 45(a).

[27] 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).

[28] 15 U.S.C. § 45(n).

[29] Other practices include, for example, allegations of 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),

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 NCUA, and the Commission to promulgate a coordinated rule designed to prevent unauthorized access to consumer report information by requiring all users of such information to have reasonable procedures to dispose of it properly and safely.[30] This Disposal Rule, which took effect on June 1, 2005, should help minimize 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.[31] 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 other specific classes

---

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), http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

[30] 16 C.F.R. Part 382 ("Disposal of Consumer Report Information and Record Rule").

[31] 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.

of information, including SSNs. For example, the Driver's Privacy Protection Act ("DPPA")[32] 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).[33] 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 protect the privacy of protected health information."[34]

E. FTC Enforcement Actions

Over the past year or so, reports have proliferated about information compromises at U.S. businesses, universities, government agencies, and other organizations that collect and store sensitive consumer information, including SSNs. Some of these incidents reportedly have led to identity theft, confirming that security breaches can cause real and tangible harm to consumers, businesses, and other institutions.

Since 2001, the Commission has brought twelve cases challenging businesses that have

---

[32] 18 U.S.C. §§ 2721-25.

[33] 45 C.F.R. Part 164 ("HIPAA Privacy Rule").

[34] 45 C.F.R. § 164.530(c).

failed to take reasonable steps to protect sensitive consumer information in their files.[35] Two of the Commission's most recent law enforcement actions arose from high-profile data breaches that occurred last year. In the first case, the Commission alleged that a major data broker, ChoicePoint, Inc., failed to use reasonable procedures to screen prospective subscribers and monitor their access to sensitive consumer data, in violation of the FCRA[36] and the FTC Act.[37] The Commission's complaint alleged that ChoicePoint's failures allowed identity thieves to obtain access to the personal information of over 160,000 consumers, including nearly 10,000 consumer reports. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties for the FCRA violations – the highest civil penalty ever levied in a consumer protection case – and $5 million in consumer redress for identity theft victims. The Order also requires ChoicePoint to implement a number of strong data security measures, including bi-annual audits to ensure that these security measures are in place.

In the second action, the Commission reached a settlement with CardSystems Solutions, Inc., the card processor allegedly responsible for last year's breach of credit and debit card information for Visa and MasterCard, which exposed tens of millions of consumers' credit and

---

[35] Documents related to these enforcement actions generally are available at http://www.ftc.gov/privacy/index.html.

[36] 15 U.S.C. §§ 1681-1681x, as amended. The FCRA specifies that consumer reporting agencies may only provide consumer reports for certain "permissible purposes." ChoicePoint allegedly approved as customers individuals whose applications had several indicia of fraud, including false credentials, the use of commercial mail drops as business addresses, and multiple applications faxed from the same public commercial location. The FTC's complaint alleged that ChoicePoint did not have a permissible purpose in providing consumer reports to such individuals and failed to have reasonable procedures to verify prospective subscribers.

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

debit numbers.[38] This case addresses the largest known compromise of sensitive financial data to date. As in the ChoicePoint case, the FTC alleged that CardSystems engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer data. These settlements provide important protections for consumers and also provide important lessons for industry about the need to safeguard consumer information.

V. THE COMMISSION'S EFFORTS TO COMBAT IDENTITY THEFT

In addition to our efforts to ensure that businesses take reasonable steps to safeguard sensitive consumer information, the Commission works in many other ways to address the identity theft problem. Pursuant to the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act"),[39] the Commission has implemented a program that assists consumers, businesses, and other law enforcers.

A. Working with Consumers

The Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft, for consumers concerned about identity theft. Every week, the Commission receives about 15,000 to 20,000 contacts from victims and consumers seeking information on how to avoid identity theft. The callers to the hotline receive counseling from trained personnel who provide information on steps they can

---

[38] *In the Matter of CardSystems Solutions, Inc.*, FTC File No. 052-3148 (proposed settlement posted for public comment, Feb. 23, 2006). The settlement requires CardSystems and its successor corporation to implement a comprehensive information security program and obtain audits by an independent third-party professional every other year for 20 years. As noted in the FTC's press release, CardSystems faces potential liability in the millions of dollars under bank procedures and in private litigation for losses related to the breach.

[39] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

take both to prevent identity theft and to resolve problems resulting from the misuse of their identities. Victims are advised to: (1) obtain copies of their credit reports and have a fraud alert placed on them;[40] (2) contact each of the creditors or service providers with which the thief has established or accessed an account to request that the account be closed and to dispute any associated charges; and (3) report the theft to the police and, if possible, obtain a police report. The police report is useful in demonstrating to purported creditors and debt collectors that the consumer is a victim of identity theft, and serves as an "identity theft report" that can be used for exercising various victims' rights granted by the FACT Act.[41] The Commission's identity theft website, www.consumer.gov/idtheft, has an online complaint form where victims can enter their complaints into the Clearinghouse.

The Commission also has taken the lead in developing and disseminating identity theft-related consumer education materials, including an identity theft primer, *ID Theft: What It's All About*, and a victim recovery guide, *Take Charge: Fighting Back Against Identity Theft.* The Commission alone has distributed more than 2.1 million copies of the *Take Charge* booklet (formerly known as *ID Theft: When Bad Things Happen To Your Good Name*) since its release in

---

[40] The FACT Act added a requirement that consumer reporting agencies, at the request of a consumer, place a fraud alert on the consumer's credit report. Consumers may obtain an initial alert if they have a good faith suspicion that they have been or are about to become an identity theft victim. The initial alert must stay on the file for at least 90 days. Actual victims who submit an identity theft report can obtain an extended alert, which remains in effect for up to seven years. Fraud alerts require users of consumer reports who are extending credit or related services to take certain steps to verify the consumer's identity. *See* 15 U.S.C. § 1681c-1.

[41] These include the right to an extended fraud alert, the right to block fraudulent trade lines on credit reports and to prevent such trade lines from being furnished to a consumer reporting agency, and the ability to obtain copies of fraudulent applications and transaction reports. *See* 15 U.S.C. § 1681 *et seq.*, as amended.

February 2000 and has recorded more than 2.4 million visits to the Web version. The Commission also maintains the identity theft website, www.consumer.gov/idtheft, which provides publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

Last fall, the Commission, together with partners from law enforcement, the technology industry, and nonprofits, launched OnGuard Online, an interactive, multi-media resource for information and up-to-the minute tools on how to recognize Internet fraud, avoid hackers and viruses, shop securely online, and deal with identity theft, spam, phishing, and file-sharing.[42]

In addition, the Commission will launch this spring a major new identity theft education campaign. The campaign will encourage consumers to guard against identity theft by taking steps to reduce their risk, keep a close eye on their personal information, and move quickly to minimize the damage if identity theft occurs. The centerpiece of the campaign will be a turnkey toolkit – a comprehensive how-to guide that will help promote grassroots education about identity theft.

The Commission also has developed ways to simplify the recovery process. One example is the ID Theft Affidavit, included in the *Take Charge* booklet and on the website. This standard form was developed in partnership with industry and consumer advocates for victims to use in resolving identity theft debts. To date, the Commission has distributed more than 293,000 print copies of the Affidavit and has recorded more than 1.1 million hits to the Web version.

---

[42] *See* www.onguardonline.gov. OnGuard Online is also available in Spanish. *See* www.AlertaEnLinea.gov.

B. Working with Industry

The private sector can play a key role in combating identity theft by reducing its incidence through better security and authentication. The Commission works with institutions to promote a "culture of security" by identifying ways to spot risks to the information they maintain and keep it safe.

Among other things, the Commission has disseminated advice for businesses on reducing risks to their computer systems[43] and on compliance with the Safeguards Rule.[44] Our emphasis is on preventing breaches before they happen by encouraging businesses to make security part of their regular operations and corporate culture. The Commission also has published *Information Compromise and the Risk of Identity Theft: Guidance for Your Business,* a booklet on managing data compromises.[45] This publication provides guidance on when it would be appropriate for an entity to notify law enforcement and consumers in the event of a breach of personal information.

In 2003, the Commission held a workshop that explored the challenges consumers and industry face in securing their computers. Titled "Technologies for Protecting Personal Information: The Consumer and Business Experiences," the workshop also examined the role of technology in meeting these challenges.[46] Workshop participants, including industry leaders,

---

[43] *Security Check: Reducing Risks to Your Computer Systems, available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

[44] *Financial Institutions and Customer Data: Complying with the Safeguards Rule, available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

[45] *Information Compromise and the Risk of Identity Theft: Guidance for Your Business, available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.pdf.

[46] *See* workshop agenda and transcripts *available at* www.ftc.gov/bcp/workshops/technology. *See* Staff Report *available at*

technologists, researchers on human behavior, and representatives from consumer and privacy groups, identified a range of challenges in safeguarding information and proposed possible solutions.

C. Working with Law Enforcement

A primary purpose of the Identity Theft Act was to provide law enforcement with access to a centralized repository of identity theft victim data to support their investigations. The Commission operates this database as a national clearinghouse for complaints received directly from consumers and through numerous state and federal agencies, including the Social Security Administration's Office of Inspector General.

With over 1,060,000 complaints, the Clearinghouse provides a detailed snapshot of current identity theft trends as reported by the victims themselves. The Commission publishes data annually showing the prevalence of complaints broken out by state and city.[47] Since its inception, nearly 1,400 law enforcement agencies have registered for access to the Clearinghouse database. Individual investigators within those agencies can access the system from their desktop computers 24 hours a day, seven days a week. The Clearinghouse also gives access to training resources, and enables users to coordinate their investigations.

---

http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf.

[47] *See Federal Trade Commission - National and State Trends in Fraud & Identity Theft* (Jan. 2006), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf. The Commission also conducts national surveys to learn how identity theft impacts the general public. The FTC conducted the first survey in 2003 and is conducting a second survey this spring. *See Federal Trade Commission – Identity Theft Survey Report* (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

The Commission also encourages use of the Clearinghouse through training seminars offered to law enforcement. In cooperation with the Department of Justice, the U.S. Postal Inspection Service, the U.S. Secret Service, and the American Association of Motor Vehicle Administrators, the Commission began organizing full-day identity theft training seminars for state and local law enforcement officers in 2002. To date, this group has held 20 seminars across the country. More than 2,880 officers have attended these seminars, representing over 1,000 different agencies. Future seminars are being planned for additional cities.

To further assist law enforcers, the Commission staff developed an identity theft case referral program. The staff creates preliminary investigative reports by examining patterns of identity theft activity in the Clearinghouse, and refers the reports to financial crimes task forces and others for further investigation and possible prosecution. In addition, analysts from the FBI, U.S. Secret Service, and Postal Inspection Service work on-site at the FTC, developing leads and supporting ongoing investigations for their agencies.

VI. CONCLUSION

The crime of identity theft is a scourge, causing enormous damage to businesses and consumers. The unauthorized use of consumers' SSNs is an important tool of identity thieves, especially those seeking to create new accounts in the victim's name. Although current laws place some restrictions on the use or disclosure of SSNs by certain entities under certain circumstances, this information is still otherwise available from both public and private sources, thereby enabling identity thieves to obtain SSNs through legal means as well as illegal means.

At the same time, SSNs are an important driver of our market system. Businesses and others rely on SSNs to provide many important benefits for consumers and to fight identity theft.

There are a number of things that government, industry, and consumers can do to help stem the tide of identity theft. First, both government and industry need to consider what information they collect and maintain from or about consumers and whether they need to do so. Entities that possess sensitive consumer information should continue to enhance their procedures to protect it. The Commission will continue its law enforcement and outreach efforts to encourage and, when necessary, require better protections.

Second, industry should continue the development of improved fraud prevention methods to stop identity thieves from misusing the consumer information they have managed to obtain. In this regard, the FACT Act should prove instrumental by requiring the bank regulatory agencies, the NCUA, and the FTC to develop jointly regulations and guidelines for financial institutions and creditors to identify possible risks of identity theft.[48]

Third, the Commission will continue and strengthen its efforts to empower consumers by providing them with the knowledge and tools to protect themselves from identity fraud and to deal with the consequences when it does occur. As discussed above, new consumer rights granted by the FACT Act should help consumers minimize the damage.

Finally, the Commission will continue to assist criminal law enforcement in detecting and prosecuting identity thieves. The prospect of serious jail time hopefully will discourage those considering identity theft from perpetrating this crime.

The Commission looks forward to continuing to work with Congress to address ways to reduce identity theft.

---

[48] 15 U.S.C. § 1681m(e).