PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

OHIO PRIVACY and PUBLIC RECORDS ACCESS STUDY COMMITTEE

of the

OHIO SENATE and HOUSE OF REPRESENTATIVES

on

Public Entities, Personal Information, and Identity Theft

Columbus, Ohio

May 31, 2007

I. Introduction

Senator Goodman, Representative Wolpert, and members of the Committee, I am Betsy Broder, Assistant Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission").[1] Thank you for the opportunity to speak about identity theft and the government's obligations in protecting sensitive personal information in its possession.

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 the identity theft problem, the work of the President's Identity Theft Task Force, and specific issues concerning the protection of personal information held by governmental entities.

II. The Identity Theft Problem

Identity theft has become a serious concern in our information-based economy. Millions of consumers are victimized by this crime every year.[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 recent Wall Street Journal/Harris Interactive survey, for example, found that, as a result of fears about protecting their identities,

---

[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, e.g.*, www.consumer.gov/idtheft/pdf/synovate_report.pdf.

30 percent of consumers polled were limiting their online purchases, and 24 percent were cutting back on their online banking.[3]

Generally speaking, most cases of identity theft fall into one of two broad categories: the takeover or misuse of existing credit card, debit card, or other accounts ("existing account fraud"); and the use of stolen personal 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 in out-of-pocket expenses and time necessary to repair the damage.[4]

Identity thieves obtain the information they use to commit identity theft from many sources, both private and public. They may steal wallets, rifle through trash, bribe insiders, or hack into databases. Government agencies can also be a source of consumer data that can be used to commit identity theft. Public entities, including federal, state and local governments, collect personal information about individuals for a variety of purposes, such as determining who is eligible for government programs and delivering efficient and effective services. Accordingly,

---

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

[4] Federal law limits consumers' liability for unauthorized credit card charges to $50 per card as long as the credit card company is notified 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 and will not hold the consumers liable for the unauthorized charges, no matter how much time has elapsed since the discovery of the loss or theft of the card. Consumers' liability for unauthorized debit card charges is limited to $50 in cases where the loss is reported within two business days, and to $500 if reported thereafter. *See* 15 U.S.C. § 1693g(a). In addition, if consumers do not report unauthorized use when they see it on their bank statement within 60 days of receiving the notice, they may be subject to unlimited liability for losses that occurred after that period. *Id.*

public entities play a critical role in guarding against misuse and unauthorized disclosure of the personal information they collect and maintain.

III. President's Identity Theft Task Force

On May 10, 2006, the President established an Identity Theft Task Force. Comprised of 17 federal agencies, the Task Force is chaired by Attorney General Alberto Gonzales and co-chaired by FTC Chairman Deborah Platt Majoras. The mission of the Task Force is to develop a comprehensive national strategy to combat identity theft.[5] The President specifically directed the Task Force to make recommendations on steps the federal government can take to reduce the likelihood of identity theft.

In April 2007, the Task Force published a strategic plan for combating identity theft.[6] 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 includes recommendations on how to prevent sensitive data from falling into the wrong hands, to make such data less valuable to identity thieves by improving authentication, to ease victim recovery, and to improve tools for effective criminal law enforcement. The Strategic Plan includes several specific recommendations regarding the protection of sensitive personal information collected and maintained by the Federal government.

IV. The Critical Role Of Social Security Numbers

---

[5] Exec. Order No. 13, 71 FR 27945 (May 10, 2006), available at www.idtheft.gov.

[6] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, is available at www.idtheft.gov.

Many of the Task Force recommendations focus on the security for and use of Social Security numbers ("SSNs"). The SSN is particularly valuable to identity thieves because in many cases it is the key piece of information that can enable criminals to perpetrate new account fraud. Creditors and other benefits providers often use SSNs to access information (such as a credit report) that is necessary to open an account or provide other benefits.

SSNs play a vital role in our economy, enabling both business and government to match information to the proper individual. Federal, state, and local governments rely extensively on SSNs for identifying consumers when administering programs that deliver services and benefits to the public. With 300 million Americans, many of whom share the same name, the SSN presents significant advantages as a means of identification because of its uniqueness and permanence. At the same time, however, the widespread use of SSNs makes them more readily available to identity thieves. The challenge is to find the proper balance between keeping SSNs out of the hands of thieves, while giving businesses and government sufficient means to identify individuals. Excessive restrictions on the use of SSNs could have a deleterious impact on such important purposes as public health, criminal law enforcement, and anti-fraud efforts by making it unduly difficult for government agencies to identify individuals. In addition, changes to government systems can be time-consuming and expensive, and it is important that any changes not impair the transparency of public records.

SSNs are widely available in public records held by federal agencies, states, local jurisdictions, and courts. As of 2004, 41 states and the District of Columbia, as well as 75

percent of U.S. counties, displayed SSNs in public records.[7] Although the number and type of records in which SSNs are displayed vary greatly across states and counties, SSNs are often found in death records, voter registration records, property records, and court documents.[8] In addition, the increasing online availability of public records may make it easier for thieves to obtain SSNs from those records. Although steps are being taken to reduce the widespread availability of SSNs through publicly available documents -- such as the 2003 change in Bankruptcy Court rules that requires that truncated versions of SSNs be used in most documents filed with the court[9] -- SSNs remain one of the most widely used individual identifiers. Decisions and policies regarding public display of SSNs and other consumer data must rely on a careful balancing of the need for public access to records with the concerns for privacy and security, along with the costs of limiting access.

The Identity Theft Task Force made several recommendations with respect to the issue of government use of SSNs. Based on an Office of Personnel Management ("OPM") review of the use of SSNs by federal agencies for human resource purposes, the Task Force recommended that OPM take steps to eliminate, restrict, or conceal the use of SSNs wherever possible (including assigning employee identification numbers where practicable). The Task Force expressly

---

[7] Government Accounting Office, *Social Security Numbers: Government Could Do More to Reduce Display in Public Records and On Identity Cards* (November 2004), at 2, available at www.gao.gov/new.items/d0559.pdf.

[8] In the past, many states used SSNs as driver's license identification numbers. Many states voluntarily changed this practice to reduce the unnecessary use of SSNs. The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, now prohibits the display of SSNs on driver's licenses, vehicle registrations, or other identification documents issued by state departments of motor vehicles. *See* 42 U.S.C. 405(c)(2)(C)(vi).

[9] *See, e.g.*, Federal Rule of Bankruptcy Procedure 1005.

recognized that SSNs must continue to be used for certain purposes, such as income and tax records, and recommended that OPM issue guidance to federal agencies on how to restrict, conceal, or mask SSNs in those records. The Task Force also recommended that the Social Security Administration develop a clearinghouse for agency practices that minimize use and display of SSNs in order to facilitate the sharing of best practices.

In addition, the Task Force recommended that its agencies work with state and local governments -- through organizations such as the National Governors Association, the National Association of Attorneys General, the National League of Cities, and the National Association for Public Health Statistics and Information Systems -- to discuss the use of SSNs and to explore ways to eliminate unnecessary use and display of SSNs. Many of the recommendations to federal agencies can be applied equally to government agencies at all levels.

V. Data Security in the Public Sector

Governments collect sensitive personal information that can be misused by identity thieves, and must therefore take appropriate steps to ensure that the information is properly protected. Just as private entities need to develop and strengthen their security programs, government agencies need to carefully examine their methods of protecting the privacy of individuals whose information they collect and store. Certain of these obligations are imposed by law,[10] while others are simply a function of proper oversight and management.

Federal agencies currently are taking steps to strengthen their information security. The Federal Information Security Management Act (FISMA), the primary governing statute for the

---

[10] *See, e.g.,* The Privacy Act, 5 U.S.C. § 552a; The E-Government Act of 2002, 44 U.S.C. § 3501 note.

federal government's information technology security program, establishes a comprehensive framework for ensuring the effectiveness of information security controls over federal information resources. It also provides for the development and maintenance of minimum controls required to protect federal information and information systems.[11] FISMA requires the head of each federal agency to implement cost-effective policies and procedures to reduce information technology security risks to an acceptable level. It also requires agency officials to conduct annual reviews of agency information security programs and report the results to the Office of Management and Budget (OMB). OMB issued several guidance memoranda last year on how agencies should safeguard sensitive information. For example, OMB published a checklist for protecting remotely accessed information, including a recommendation that agencies encrypt all data on mobile devices and use a "time-out" function for remote access and mobile devices.[12]

In addition, OMB and the Department of Homeland Security ("DHS") lead an interagency Information Systems Security Line of Business working group on government data security practices. This working group has identified key steps for improving the government's security procedures. Employee training is one essential part of ensuring the effectiveness of such procedures. Training programs must be reviewed continuously and updated to reflect the most recent changes, issues, and trends in information security. This effort includes the development of annual security training for all government employees, particularized security training

---

[11] 44 U.S.C. §§ 3541, *et seq.*

[12] *See Protection of Sensitive Agency Information*, Memorandum from Clay Johnson III, Deputy Director for Management, OMB, to Heads of Departments and Agencies, M-06-16 (June 23, 2006).

curricula for all employees with significant security responsibilities, a repository of training programs, and conferences and seminars organized to share knowledge. Each of these components contributes to greater security awareness within agencies, leading to enhanced protection of sensitive data.[13]

The Task Force issued several recommendations aimed at ensuring that government agencies take concrete steps to improve their data security measures. First, the Task Force recommended that OMB and DHS outline best practices in the arena of automated tools, training processes, and standards that would enable agencies to improve their security and privacy programs. The Task Force also recommended the development of a list of the most common mistakes to avoid in protecting personal information held by the government.

Because several highly-publicized government data breaches involved the loss of laptops, the Task Force also recommended that Chief Information Officers of federal agencies remind the agencies of their responsibilities to protect laptops and other portable data storage and communication devices, such as PDAs and thumb drives.

For example, the FTC itself has instituted an extensive and active program to instill and support a culture of privacy throughout the agency. The FTC maintains a Privacy Steering Committee ("the Committee") and created the position of Chief Privacy Officer. The Chief

---

[13] The Commission has published a guide, entitled *Protecting Personal Information*, available at http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html, which includes guidelines for improving information security. Although directed at businesses, it includes a five-step process that applies equally well to government entities: (1) entities should take stock of the information in their possession; (2) efforts should be made to collect only necessary information; (3) information that is retained must be sufficiently protected and employees should receive training in information security; (4) information that is not needed should be disposed of properly; and (5) entities should make plans to respond to any security breaches that may occur.

Privacy Officer is responsible for overseeing the FTC's internal privacy policies and procedures and reports directly to the agency's Chief of Staff.

In 2006, the Committee undertook a comprehensive and systematic review of the FTC's collection, use, sharing, retention, storage, and disposal of personally identifiable information and sensitive health information. The Committee then developed detailed FAQs that provide practical advice regarding situations that staff is likely to encounter when handling personally identifiable information during agency activities. Employees and contractors undergo mandatory data security training, and electronic access to data is secured through multi-layered security. The FTC also is developing a formal incident response plan setting forth how it should respond in the event of a data breach. All of these efforts are directed at raising awareness throughout the agency of each person's responsibility to ensure the security of personal identifying information. From processing employment records to collecting documents in litigation, agency employees are charged with using appropriate care, forethought, and attention to the data within their control.

VI. Data Breach Responses in the Public Sector

Just as with private-sector breaches, the loss or compromise of personal data by the government exposes individuals to identity theft. In addition to taking steps to avoid such breaches, government agencies also should have response plans in place should a breach occur. Government agencies should be prepared to determine (1) whether a particular breach warrants notice to consumers, (2) the content of the notice, (3) which third parties, if any, should be notified, and (4) whether to offer affected individuals credit monitoring or other prophylactic or remedial services.

The Task Force developed guidelines that set forth the factors that should be considered in deciding how to respond to a breach, and recommended that OMB issue them as a guidance to all federal agencies and departments.[14] OMB issued the guidance on September 20, 2006. The guidelines contain three core recommendations: (1) agencies should identify a core response group that can be convened in the event of a breach; (2) if a breach occurs, the core response group should engage in a risk analysis to determine whether the incident poses risks of identity theft; and (3) if it is determined that an identity theft risk is present, the agency should tailor its response to the nature and scope of the risk presented. This risk-based approach allows an agency to assess a situation and take appropriate steps to minimize consumer harm.

In determining whether a breach creates a risk of identity theft, the guidelines suggest that agencies consider: (1) how difficult it would be for an unauthorized person to access the personal information; (2) whether the breach was likely the result of criminal activity; (3) the ability of the agency to mitigate the identity theft; and (4) any evidence that the compromised information is actually being used to commit identity theft.

The guidelines also provide recommendations for issuing notices to affected consumers, when appropriate, including the timing, content, and methods of notification. In addition, the guidelines discuss two other possible actions that agencies can take when the risk of identity theft appears to be high. First, agencies can perform an analysis to determine whether the data breach appears actually to be resulting in identity theft. This can allow agencies to evaluate the severity of a breach and determine whether some action other than a notice to consumers is warranted.

---

[14] *See* President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, Appendix A, pages 73-82.

Second, agencies can provide credit monitoring to affected individuals, a service that advises consumers of material changes to their credit report, thereby assisting them in early detection of identity theft and allowing them to take steps to minimize the impact. Although credit monitoring can be costly when it involves large numbers of consumers, it may be justified in cases where, because of the nature of the breach, risk of identity theft is high.

While each security breach must be evaluated individually, establishing a set of guidelines for assessing the situation can improve a government entity's ability to respond to a security incident in a timely and reasonable fashion.

VII. Conclusion

Identity theft remains a serious problem in our economy, causing enormous harm to consumers and businesses and threatening consumer confidence in the marketplace and, at times, in government agencies. To succeed in the battle against identity theft, governments, together with the private sector, must make it more difficult for thieves to obtain the information they need to steal identities and respond appropriately to data breaches if they occur. To prevent thieves from obtaining sensitive information, government must consider what information it collects and maintains from or about consumers and must better protect the data it does collect. In this regard, eliminating unnecessary collection, use, and disclosure of Social Security numbers -- an important tool of identity thieves -- can play a key role.

From county clerks and town halls to federal departments, public agencies play a key role in reducing the incidence and impact of identity theft. Minimizing collection of data, restricting its availability to those who have a legitimate need for it, and implementing appropriate response systems for breaches all can contribute to the efforts to reduce identity theft.