PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOUSE COMMITTEE ON THE JUDICIARY

on

Protecting Consumer Privacy and Combating Identity Theft

Washington, DC

December 18, 2007

I. INTRODUCTION

Chairman Scott, Ranking Member Gohmert 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 testimony on protecting consumer privacy and combating identity theft.

Protecting privacy is a critical component of the Commission's consumer protection mission. The explosive growth of the Internet and the development of sophisticated computer systems and databases have made it easier than ever for businesses and other organizations to gather, store, and use information about consumers.[2] These new information systems can provide tremendous benefits to consumers, such as enabling fast and convenient access to services and information. At the same time, if the sensitive information needed to enable these services is not protected adequately, or if consumers' identities are not authenticated properly, consumers can suffer harm, including identity theft. This testimony will summarize the Commission's efforts to protect privacy and fight identity theft through its law enforcement actions, its participation on the President's Identity Theft Task Force, and its extensive consumer and business education and outreach activities.

---

[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]A recent study by research firm IDC estimates that worldwide digital information will increase to 988 billion gigabytes by 2010, as compared to 161 billion gigabytes in 2006. *See* http://www.emc.com/about/destination/digital_universe/ One gigabyte equals one billion units of information.

II. THE IDENTITY THEFT PROBLEM

Identity theft is a serious concern in our information-based economy. Millions of consumers are victimized by this crime every year.[3] Identity theft takes two primary forms: 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"). The Commission's most recent national identity theft survey confirmed findings from earlier surveys that new account fraud, although less prevalent than existing account fraud, typically causes considerably more harm to consumers in out-of-pocket expenses and time necessary to repair the damage.[4] At the same time, new forms of identity theft have become more prevalent, including medical ID theft and immigration and employment fraud.

Beyond its direct costs, identity theft harms our economy by threatening consumers' confidence in the marketplace generally and in electronic commerce specifically. An April 2007 Zogby Interactive survey found that 91 percent of adult users of the Internet are concerned that their identities might be stolen (including 50 percent who are "very concerned").[5] In a May 2006 Wall Street Journal/Harris Interactive survey, as a result of fears about protecting their identities,

---

[3] The FTC recently released its second nationwide survey of the incidence and impact of identity theft ("ID Theft Survey"). The survey found that 8.3 million adults were victims of identity theft in 2005. The survey report can be found at www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

[4] The FTC survey found that 6.5 million consumers were victims of existing account fraud, and 1.8 million experienced new account frauds or other types of identity fraud. Over half of the victims of existing account fraud, and 37 percent of victims of new account fraud, suffered no out-of-pocket expenses in coping with the theft. Conversely, 25 percent of new account fraud victims incurred at least $1000 in expenses, compared to fewer than 10 percent of existing account fraud victims. New account fraud victims also spent significantly more time repairing the damage than did existing account fraud victims. ID Theft Survey, at 37-39.

[5] *See* Zogby Poll: Most Americans Worried About Identity Theft, *available at* www.zogby.com/search/ReadNews.dbm?ID=1275

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

[7]*See* Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Lim*

The FTC enforces several laws that contain data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, contains data security requirements for financial institutions.[8] The Fair Credit Reporting Act ("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,[9] and imposes safe disposal obligations on entities that maintain consumer report information.[10] In addition, the FTC has enforced the Federal Trade Commission Act's proscription against unfair or deceptive acts or practices in cases where a business made false or misleading claims about its data security procedures, or where its fai2nal Crede purpose f

[8] 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, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[9] 15 U.S.C. § 1681e.

[10] *Id. at* § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 382.

[11] 15 U.S.C. § 45(a).

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

[13] *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.*, Docket No. C-4187 (April 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 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). In its case against ChoicePoint, Inc., for example, the FTC alleged that the company inadvertently sold sensitive information on more than 160,000 consumers to a criminal gang, who used that information in some cases to commit identity theft. The company allegedly approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby commercial photocopying facilities. The Commission alleged, among other violations, that ChoicePoint misrepresented its security measures when it failed to use reasonable procedures to screen prospective purchasers of its information. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties (for alleged violations of the FCRA) and $5 million in consumer redress for identity theft

The FTC Safeguards Rule serves as a good model of this approach. Firms covered by the Rule (financial institutions) must prepare a written plan; designate an official with responsibility for the plan; identify, assess, and address foreseeable risks; oversee service providers' handling of information; monitor and evaluate the program for effectiveness; and adjust the plan as appropriate. The Rule states that what is "reasonable" will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue. This standard recognizes that there cannot be "perfect" security, and that data breaches can occur even when a company maintains reasonable precautions to prevent them. The standard also is flexible and adaptable. It acknowledges that risks, technologies, and business models change over time, and that a static technology-based standard would quickly become obsolete and could stifle innovation in security practices. The Commission will continue to apply the "reasonable procedures" principle in enforcing existing data security laws.

B. Participation in the Identity Theft Task Force

On May 10, 2006, President Bush established an Identity Theft Task Force, comprised of 17 federal agencies and co-chaired by FTC Chairman Deborah Platt Majoras, with the mission of developing a comprehensive national strategy to combat identity theft.[16] 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.

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

In April 2007, the Task Force published its strategic plan for combating identity theft.[17] Broadly, the plan is organized around the life cycle of identity theft – from the thieves' attempts to obtain sensitive information to the impact of the crime on victims – and identifies roles for consumers, the private sector, government agencies, and law enforcement.

The Task Force Strategic Plan recommends 31 initiatives directed at reducing the incidence and impact of identity theft. The recommendations focus on *prevention* through improvements in data security and more effective customer authentication procedures, *victim assistance* by ensuring victims have the means and support to restore their identities, and *deterrence* through stronger tools to punish the criminals who perpetrate this crime.

1. Prevention

The Task Force recognized that both the public and private sectors must develop better protections for sensitive consumer data. For the public sector, the Plan recommended that federal agencies and departments improve their internal data security processes; develop breach notification systems; and reduce unnecessary uses of Social Security numbers, which are often the key item of information that identity thieves need.

For the private sector, the Task Force proposed that Congress establish national standards for data security and breach notification that would preempt the numerous state laws on these issues. The data security standards would follow the Safeguards Rule model, requiring covered entities to implement reasonable administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive consumer information, protect against anticipated threats, and prevent unauthorized access. The proposed breach notification standards would

[17]The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("Strategic Plan"), *available at* http.//www.idtheft.gov.

require entities to provide notice to consumers when they experience a breach that creates a significant risk of identity theft.

In addition, the Plan recommended:

- the dissemination of additional guidance to the private sector for safeguarding sensitive consumer data,
- continued law enforcement against entities that fail to implement appropriate security,
- a multi-year consumer awareness campaign to encourage consumers to take steps to safeguard their personal information and minimize their risk of identity theft,
- a comprehensive assessment of the private sector's usage of Social Security numbers, and
- holding workshops on developing more reliable methods of authenticating the identities of individuals to prevent thieves who obtain consumer information from using it to open accounts in the consumer's name.

2. Victim recovery

Once consumers have been victimized, it is critical that they have the ability to minimize and reverse the damage to their credit records and other aspects of their identities. The Strategic Plan recommended a number of steps to aid those who assist victims, as well as the victims themselves. These include:

- development of easy-to-use reference materials for law enforcement, often the first responders to identity theft,
- implementation of a standard police report, a key document for victim recovery,
- nationwide training for victim assistance counselors,

[21]*See*

To ensure that law enforcement agencies are aware of these resources and are equipped to respond to identity theft, the FTC has partnered with the Department of Justice, the U.S. Postal Inspection Service, the U.S. Secret Service, the F.B.I., and the American Association of Motor Vehicle Administrators to provide on site training to local law enforcement around the country. Since the first training in 2002, these agencies have conducted more than 26 training sessions for over 3,300 law enforcement officers from more than 1000 agencies. This critical outreach will continue with training sessions planned for North and South Carolina, Minnesota, and the New England states in the coming months.

Because law enforcement officials often are the first responders for identity theft victims, the FTC also has developed a training CD and publications on victim assistance to help law enforcement offices direct ID theft victims to the resources they need for recovery, including the FTC.[23]

D. Implementation of the FACT Act

The FACT Act extensively amended the Fair Credit Reporting Act, including the addition of a number of new provisions intended to reduce the incidence of identity theft or minimize the injury to victims. The FACT Act assigned to the Commission, alone or in coordination with one or more other federal agencies, the task of promulgating approximately twenty implementing rules, guidelines, compliance forms, and notices, and conducting nine studies with reports to Congress.

[23] *See* http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/helping-victims.html.

The FACT Act added a number of new provisions to limit the opportunities for wrongdoers to obtain unauthorized access to sensitive information, and to assist consumers in avoiding and remediating identity theft. With respect to prevention, the FACT Act requires merchants to truncate the account number and redact the expiration date on consumers' copies of electronic credit card receipts.[24] In addition, the FTC and bank regulatory agencies recently

[24]15 U.S.C. § 1681c(g).

[25]*See* http://www.ftc.gov/opa/2007/10/redflag.shtm and accompanying regulatory text. The agencies also recently issued the final Affiliate Marketing Rules intended to enhance consumer privacy. The rules prohibit a person from using information obtained by an affiliate for marketing purposes unless the consumer has been given notice and has had an opportunity to opt out of the marketing. *See* http://www.ftc.gov/opa/2007/10/affiliate.shtm, and accompanying regulatory text.

[26]15 U.S.C. § 1681j(a)(1)(c). The FTC regulations implementing this program are at 16 C.F.R. Part 610. The Commission has taken action to uphold the integrity of the free report program, including two cases against a company that offered "free" credit reports tied to the purchase of a credit monitoring service, through the web site "freecreditreport.com." *FTC v. Consumerinfo.com, Inc.*, No. SACV05-801AHS(MLGx) (C.D. Cal. Aug. 15, 2005); *FTC v. Consumerinfo.com, Inc.*, No. SACV05-801AHS(MLGx) (C.D. Cal. Jan. 8, 2007). In the first case, the Commission charged, among other things, that the defendants, affiliates of the nationwide consumer reporting agency Experian, had deceptively

their credit file. The reports also ensure that identity theft complaints flow into the FTC's ID Theft Data Clearinghouse for the use of law enforcement officers.

E. Consumer and Business Education

Both independently and pursuant to the Identity Theft Task Force Strategic Plan, the Commission had undertaken substantial efforts to increase consumer and business awareness of the importance of protecting data and taking other steps to prevent identity theft, as well as steps that can be taken to minimize the damage when a theft does occur. As noted earlier, the Commission receives approximately 15,000 to 20,000 contacts each week through its toll-free hotline and online complaint form from consumers who are seeking advice on how to recover from identity theft or how to avoid becoming a victim in the first place. The FTC's identity theft primer[32] and victim recovery guide[33] are widely available in print and online. Since 2000, the Commission has distributed more than 9.7 million copies of the two publications, and recorded over 4.5 million visits to the Web versions.

Last year, the Commission launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend." 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 2.6 million brochures and 60,000 kits to date, and has recorded more than 4.8 million visits to the education program's

---

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

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

Web site this year alone. The Commission also has partnered with other organizations to broaden its reach. As just one example, the U.S. Postal Inspection Service initiated an outreach campaign to place FTC educational materials on subway cars in New York, Chicago, San Francisco, and Washington D.C.

[34] *See* www.onguardonline.gov/index.html.

[35] *E.g., FTC v. Action Research Group,*

ads back to them.[36] Since 1997, the Commission has brought 92 law enforcement actions involving spam, 29 of which were filed after Congress enacted the CAN-SPAM Act.

With respect to telemarketing, the National Do Not Call Registry currently includes more than 145 million telephone numbers, and this program has been tremendously successful in protecting consumers' privacy from unwanted telemarketing calls. Although the Commission appreciates the high rate of compliance with its Do-Not-Call Rule, it vigorously enforces the requirements of the Registry to ensure its ongoing effectiveness. Violations of the Do-Not-Call rule subject telemarketers to civil penalties of up to $11,000 per violation. Thirty-four FTC telemarketing cases have alleged Do-Not-Call and/or Abandoned Call violations, resulting in $16.4 million in civil penalties and $8.2 million in consumer redress or disgorgement ordered. Last month, the Commission announced its latest crackdown on Do-Not-Call violations, including six settlements and a seventh lawsuit against companies and individuals alleged to have violated the Rule. The settlements, which involved such prominent companies as Craftmatic Industries, ADT Security Services, and Ameriquest Mortgage Company, resulted in total fines of nearly $7.7 million.[37]

C. Children's Online Privacy Protection Rule

The Commission also enforces the Children's Online Privacy Protection Rule ("COPPA"), which prohibits the collection, use, or disclosure of personal information from

---

[36] *In the Matter of DirectRevenue, LLC*, FTC Docket No. C-4194 (June 29, 2007), *available at* http://www.ftc.gov/opa/2007/06/fyi07258.shtm.

[37] *See* http://www.ftc.gov/opa/2007/11/dncpress.shtm.

[38]16 C.F.R. Part 312.

sophisticated technology to analyze consumers' online activities and provide advertising identified as relevant to their interests. This November, the Commission held a follow-up "town hall" public meeting to examine the privacy implications of behavioral advertising in more depth.[41] Participants at this town hall discussed and debated the various costs and benefits of behavioral advertising to consumers and the business community, as well as possible government or private sector responses to the burgeoning of this type of advertising.

V. CONCLUSION

Maintaining the privacy and security of sensitive consumer data is one of the highest priorities for the Commission. In particular, identity theft remains a serious problem in our society, causing enormous harm to consumers and businesses and threatening consumer confidence in the marketplace. As new information technologies and privacy threats emerge, the Commission, through its own efforts and its participation on the Identity Theft Task Force, works to educate itself and the public about these new developments, advise businesses on their legal obligations, educate consumers to help them better protect themselves, train state and local law enforcement, assist identity theft victims, and take action against businesses that violate the law.

To succeed in the battle against identity theft, government and the private sector, working together, must make it more difficult for thieves to obtain the information they need to steal identities, and make it more difficult to misuse that information if they do obtain it. The Commission will continue and strengthen its efforts to combat identity theft and protect consumer privacy.

---

[41] *See* http://www.ftc.gov/opa/2007/10/thma.shtm