Prepared Statement of

The Federal Trade Commission

“I deP Tf(P)Tj29.0.8400 0.0000 TD ft:deP

Chairman Clay, Ranking Member McHenry, and members of the Subcommittee, I am Betsy Broder, Assistant Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on its activities to protect consumers from identity theft.[1] Although identity theft continues to be a serious concern in our information-based economy, the Commission is working to reduce its incidence and impact on consumers. This testimony will summarize the Commission's efforts to fight identity theft through (1) participation on the President's Identity Theft Task Force; (2) law enforcement on data security; (3) consumer and business education; and (4) implementation of the identity theft-related provisions of the Fair and Accurate Credit Transactions Act ("FACT Act").[2] It will also describe the Commission's legislative recommendations in this area.

I. The Profile of Identity Theft

Millions of consumers are victimized by identity theft every year. According to the Commission's most recent identity theft survey, approximately 8.3 million American adults – 3.7 percent of all American adults – discovered that they were victims of identity theft in 2005.[3] Beyond its direct costs, identity theft harms our economy by threatening consumers' confidence in the marketplace.

---

[1] This written statement presents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

[2] Pub. L. 108-159 (2003)

[3] See Federal Trade Commission, Identity Theft Survey Report, Prepared by Synovate 3 (2006), www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[4] In October 2008, the Department of Health and Human Services hosted a Town Hall meeting on the subject, and in January 2009, it released a report containing a list of potential action items to addre

[7] Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 15, 2006).

[8] See The President's Identity Theft Task Force, Combating Identity Theft: A Strategic

First, with respect to prevention, the Task Force promoted an enhanced culture of data security in the public and private sectors. For the public sector, the Task Force member agencies launched a variety of initiatives aimed at making the federal government a better custodian of sensitive personal information. For example, the Office of Management and Budget issued data security and breach management guidance for government agencies; the Social Security Administration removed Social Security numbers ("SSNs"), a key item of information for identity thieves, almost entirely from its internal human resources forms; and the Department of Defense is working toward removal of SSNs from military identification cards. The recent breach of sensitive records maintained by the National Archives highlights the need for continued vigilance on data security in the public sector.

The Task Force is encouraging similar data security efforts in the private sector. These efforts, some of which are described in other parts of this testimony, include business education and outreach, law enforcement actions against companies that fail to maintain reasonable security, and proposed legislation on data security. At the same time, the Commission and other agencies are educating consumers on how to avoid becoming victims of identity theft. In one important example, the U.S. Postal Service delivered a mailing in early 2008 to 146 million U.S. residences and businesses with advice on how consumers can protect themselves against identity theft.

Second, the Task Force launched a number of initiatives to assist identity theft victims when they begin the sometimes arduous task of repairing their credit and restoring their good names. For example, the FTC has developed a training CD and publications on victim assistance to help law enforcement offices direct identity theft victims to the resources they need for recovery. In addition, Task Force members have trained victim assistance counselors; provided

See Federal Trade Com

[15] See Federal Trade Commission, Privacy Initiatives, Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[16] See, e.g., In the Matter of Premier Capital Lending, Inc., FTC Docket No. C-4241 (Dec. 10, 2008); In the Matter of Life is good, Inc., FTC Docket No. C-4218 (Apr. 16, 2008); In the Matter of Petco Animal Supplies, Inc., FTC Docket No. C-4133 (Mar. 4, 2005); In the Matter

nature and scope of its activities, and the sensitivity of the information at issue. The principle recognizes that there cannot be "perfect" security, and that data breaches can occur even when a company maintains reasonable precautions to prevent them. At the same time, companies that put consumer data at risk can be liable even in the absence of a known breach. The Commission believes that its aggressive law enforcement has helped sensitize businesses to the importance of data security and motivated them to devote more attention and resources to the protection of sensitive data.

C. Consumer and Business Education

Both independently and pursuant to the Identity Theft Task Force recommendations, the Commission has undertaken substantial efforts to increase consumer and business awareness about how to prevent identity theft and how to minimize the damage when a theft does occur. For example, the FTC's identity theft primer and victim recovery guide are widely available in print and online in English and Spanish.[20] Since 2000, the Commission has distributed more than 9 million copies of the

[20] See Federal Trade Commission, Fighting Back Against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/deter-detect-defend.html

developed a second consumer education toolkit with everything an organization needs to host a "Protect Your Identity Day." Since the campaign launch in 2006, the FTC has distributed nearly 100,000 consumer education kits and over 47,000 Protect Your Identity Day kits.

The Commission also sponsors a multimedia website, OnGuard Online, and a Spanish-language counterpart, Alerta En Linea, designed to educate consumers about basic computer security, including the importance of not disclosing personal information to possible fraudsters. OnGuard Online was developed in partnership with other government agencies and the technology sector, and since its launch in 2005, has attracted more than 9.5 million visits. The site allows users to download educational games and videos, search for specific topics such as phishing or social networking, and obtain useful tips and information in an interactive format.

The Commission directs its outreach to businesses as well. The FTC widely disseminates its business guide on data security, along with an online tutorial based on the guide.[21] These resources are designed to provide diverse businesses – especially small businesses – with practical, concrete advice as they develop data security programs and plans. In addition, the FTC has held regional data security workshops for businesses in locations around the country, including Chicago, Los Angeles, Dallas and New York. It also has released nine articles for businesses relating to basic data security issues for a non-legal audience. The articles have been reprinted in both English and Spanish language newsletters for local Chambers of Commerce and other business organizations.

[21] See Federal Trade Commission, Protecting Personal Information: A Guide for Business, www.ftc.gov/infosecurity.

[22] 15 U.S.C. § 1681w.

[23] 16 C.F.R. Part 682. See Federal Trade Commission v. Navone, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008); United States v. American United Mortgage, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007.)

[24] 15 U.S.C. § 1681j(a)(1). Specialty CRAs include tenant and employment screening services, medical recor

disclosures that its program is not associated with the free annual report program and provide a link to the official web site for that program, www.annualcreditreport.com. The defendants also agreed to pay $950,000 in disgorgement, and to provide re

[32] 16 C.F.R. § 681.1.

[33] See Federal Trade Commission, Fighting Fraud with the Red Flags Rule, http://www.ftc.gov/redflagsrule.

[34] Enforcement of the Red Flags Rule will begin after August 1, 2009. See Press Release, Federal Trade Commission, FTC Will Grant Three-Month Delay of Enforcement of "Red Flags" Rule Requiring

[35] 15 U.S.C. § 1681s-2(a)(8).

[36] The FTC is conducting the survey pursuant to a recommendation of the President's Identity Theft Task Force.

authority to seek civil penalties in data security cases.[38] In most of the 26 data security cases described above, the Commission did not have the authority to obtain monetary penalties for data security violations, and the Commission believes that such authority would serve as an additional incentive for businesses to maintain reasonable data security measures.

The Commission also has recommended legislation that would help reduce the unnecessary use and display of Social Security numbers ("SSN"), which are a particularly valuable tool for identity thieves. In its April 2007 strategic plan, the President's Identity Theft Task Force called on agencies to build a comprehensive record on the uses of SSNs in the private sector and evaluate their necessity. Accordingly, the Commission issued a report last December examining myriad private sector uses of SSNs.[39] In the report, the Commission made

---

Congress is considering legislation that contains these requirements. See, e.g., H.R. 2221, 111th Cong. (2009). In addition, the American Recovery and Reinvestment Act, Pub. L. No. 111-5 (2009) (the "Recovery Act"), requires entities that collect certain individually identifiable health information to notify individuals when the security of such information has been breached. The Recovery Act charges the Department of Health and Human Services and the FTC with issuing rules to implement these requirements. In response, the FTC issued a Notice of Proposed Rulemaking in April 2009, 74 Fed. Reg. 17,914 (Apr. 20, 2009), and is considering comments received. The FTC plans to issue a final rule in August 2009.

[38] Id. See also See Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sept. 12, 2007), available at http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (Apr. 10, 2007), available at http://www.ftc.gov/os/testimony/P040101FY2008BudgetandOngoingConsumerProtectionandCompetitionProgramsTestimonySenate04102007.pdf. These recommendations also were made in the President's Identity Theft Task Force strategic plan. See The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Apr. 2007, available at http://www.idtheft.gov/reports/StrategicPlan.pdf.

[39] See FTC Report, "Recommendations on Social Security Number Use in the Private Sector," (Dec. 2008), available at http://www2.ftc.gov/opa/2008/12/ssnreport.shtm.

two new legislative recommendations. First, it recommended that Congress consider establishing national consumer authentication standards. This recommendation recognizes that the first step to minimizing the role of SSNs in identity theft is to make it more difficult for thieves to use them to open new accounts, access existing accounts, or obtain other benefits or services. Thus, the report stated that Congress should require private sector entities to establish reasonable procedures to authenticate new or existing customers to ensure that they are who they say they are.[40] Second, the report recommended that Congress consider creating national standards to reduce the public display and transmission of SSNs. Implementing these recommendations would make SSNs less available to identity thieves, and would make it more difficult for them to misuse those SSNs they are able to obtain.

IV. Conclusion

As explained in this testimony, the Commission has used multiple tools in its arsenal to fight identity theft, and is committed to continuing its work in this area. We appreciate the opportunity to testify, and look forward to working with you on this important issue.

[40] The report recommended that this requirement cover all private sector entities that maintain consumer accounts, other than financial institutions already subject to authentication requirements promulgated by bank regulatory agencies.