Prepared Statement of

The Federal Trade Commission

"Identity Theft: Victims Bill of Rights"

Before the

Subcommittee on Information Policy, Census, and National Archives
Committee on Oversight and Government Reform
United States House of Representatives

Washington, D.C.
June 17, 2009

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 represents 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.

Although identity theft often is associated with financial transactions, it can also take place in other contexts. For example, thieves can steal identities to gain employment, immigrate into this country, and evade law enforcement. Medical identity theft also has received attention in recent months.[4] It occurs when a thief uses the name or insurance information of another person to obtain medical care. As a result, not only are medical identity theft victims charged for services they did not incur, but even more importantly, their medical records may be corrupted, thus compromising their care in potentially life-threatening ways.[5]

II. The FTC's Program to Combat Identity Theft

Given the potential harms that can result from identity theft, the government and private sector must work together to combat it. The FTC has played a lead role in this effort since 1998, when Congress enacted the Identity Theft Assumption and Deterrence Act (the "Identity Theft Act"). Among other things, the Identity Theft Act required the FTC to collect consumers' identity theft complaints, provide victim assistance, and refer complaints to law enforcement.[6]

Pursuant to the Identity Theft Act, the FTC established an online portal and toll-free hotline, through which approximately 20,000 consumers contact the FTC every week for information on how to guard against identity theft or obtain assistance in recovery. In 2008, the agency received approximately 314,000 reports of actual identity theft. Consumers who report

---

[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 address it. *See* Department of Health and Human Services, ONC Commissioned Medical Identity Theft Assessment, http://healthit.hhs.gov/portal/server.pt?open=512&objID=1177&parentname=CommunityPage&parentid=9&mode=2&in_hi_userid=10741&cached=true.

[5] *See supra* note 3 at 21.

[6] 18 U.S.C. § 1028 note.

their identity theft to the FTC receive step-by-step guidance on how to minimize the harm and recover from the crime. In addition, the information they provide about their experiences is entered into the agency's Consumer Sentinel Network, a secure online resource for law enforcement. The over 1,700 investigative agencies with access to the Network can use the data to create or support ongoing investigations, enhance penalties at sentencing phase, or coordinate with other law enforcement agencies. In addition to fulfilling its responsibilities under the Identity Theft Act, the Commission has taken a broader role in combating identity theft, as described below.

A. President's Identity Theft Task Force

The Commission has played a lead role in the efforts of the President's Identity Theft Task Force ("Task Force"). In May 2006, President Bush established the Task Force, comprised of 17 federal agencies and co-chaired by the FTC's Chairman, with the mission of developing a comprehensive national strategy to combat identity theft.[7] In April 2007, the Task Force published its national strategy, which recommended 31 initiatives to reduce the incidence and impact of identity theft.[8] The recommendations focused on identity theft prevention, victim assistance, and deterrence. The FTC, along with the other Task Force agencies, have been very active in implementing the national strategy. Together, the Task Force agencies issued a report last September outlining the significant progress made to date.[9] Some highlights follow.

---

[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 Plan (2007), http://www.idtheft.gov/reports/StrategicPlan.pdf.

[9] *See* The President's Identity Theft Task Force Report (2008), http://www2.ftc.gov/os/2008/10/081021taskforcereport.pdf.

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

grants to organizations that directly help identity theft victims; developed and posted an Identity Theft Victim Statement of Rights;[10] and worked closely with the American Bar Association on a pro bono legal assistance program for identity theft victims. Task Force members also are continuing to evaluate the effectiveness of various laws and programs designed to help victims, such as state credit freeze laws and rights granted under the FACT Act.

Third, the Task Force has worked to improve law enforcement's ability to investigate, prosecute, and punish identity thieves. For instance, Task Force member agencies have provided identity theft training to over 4,600 law enforcement officers from over 1,500 agencies. Task Force members have successfully prosecuted a number of identity theft cases; partnered with foreign law enforcement agencies in identity theft investigations; and worked toward greater information sharing among and between law enforcement agencies and the private sector. To further improve law enforcement, the Task Force recommended measures to enhance the gathering of statistical data on identity theft. In response, the FTC has worked with the Bureau of Justice Statistics ("BJS") to add questions about identity theft in BJS' National Crime Victimization Survey, which reaches approximately 40,000 households. The responses will enable BJS to estimate the types of identity theft victimization as well as gather data on financial loss, emotional impact, and law enforcement response. The Commission expects that this survey, the results of which will be available later this year, will further inform its efforts to combat identity theft.

---

[10] *See* Federal Trade Commission, Fighting Back Against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/rights.html.

B. Law Enforcement on Data Security

One important way to keep sensitive information out of the hands of identity thieves is to ensure that those who maintain such information adequately protect it. The Commission plays a central role in furthering this goal by bringing law enforcement actions against businesses that fail to implement reasonable security measures to protect sensitive consumer data.

The FTC enforces several laws that contain data security requirements applicable to the private sector. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, contains data security requirements for financial institutions.[11] 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,[12] and imposes safe disposal obligations on entities that maintain consumer report information.[13] In addition, the FTC enforces the Federal Trade Commission Act's proscription against unfair or deceptive acts or practices 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.[14]

---

[11] 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 the Secretary of the Treasury have promulgated comparable safeguards requirements for the entities they regulate.

[12] 15 U.S.C. § 1681e.

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

[14] 15 U.S.C. § 45(a).

Since 2001, the Commission has used its authority under these laws to bring 26 cases against businesses that allegedly failed to protect consumers' personal information.[15] These cases, including cases against such well-known companies as Microsoft, Choicepoint, TJX, Lexis Nexis, and CVS, have alleged such practices as the failure to (1) comply with posted privacy policies;[16] (2) take even the most basic steps to protect against common technology threats;[17] (3) dispose of data properly;[18] and (4) take reasonable steps to ensure that they do not share customer data with unauthorized third parties.[19]

Some of these cases involved unfair or deceptive practices under the FTC Act, while others were brought under the Commission's Safeguards Rule or the FCRA. Although the Commission has brought its cases under different laws, all of the cases stand for the principle that companies must maintain reasonable and appropriate measures to protect sensitive consumer information. What is "reasonable" will depend on the size and complexity of the business, the

---

[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 of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No.C-4110 (May 28, 2004); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002);.

[17] *See, e.g., In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008); *In the Matter of Reed Elsevier, Inc.*, FTC Docket No. C-4226 (July 29, 2008).

[18] *See, e.g.*, *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); *In the Matter of CVS Caremark Corp.*, File No. 072 3119 (Feb. 19, 2009) (accepted for public comment).

[19] *See, e.g., United States v. Rental Research Svcs.,* No. 09 CV 524 (D. Minn. Mar. 5, 2009); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006).

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 two publications, and recorded over 4.5 million visits to the Web versions.

The Commission recognizes that its consumer education efforts can be even more effective if it partners with local businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. For example, the Commission has launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend," which contains a consumer education kit that includes direct-to-consumer brochures, training materials, presentation slides, and videos for use by such groups. The Commission has

[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.

D. Implementation of the FACT Act

The Commission also has worked to implement the identity theft protections of the FACT Act. That Act amended the FCRA by, among other things, adding several provisions designed to reduce the incidence of identity theft or minimize the injury to victims. First, it sought to limit opportunities for identity thieves to access consumer report information. For example, the FACT Act mandated that businesses dispose of consumer report information in a safe manner.[22] The Commission has promulgated the Disposal Rule to implement this requirement for entities within its jurisdiction, and has sued entities that failed to comply.[23]

Second, the FACT Act provided consumers new opportunities to review their credit records and spot incipient signs of identity theft. Under the FACT Act, consumers have the right to receive a free credit report every twelve months from each of the nationwide consumer reporting agencies ("CRAs"), as well as from nationwide "specialty" CRAs.[24] The Commission has acted aggressively to uphold the integrity of the free report program; for example, it has brought two actions against companies offering "free" credit reports tied to the purchase of a credit monitoring service.[25] To provide further clarity to consumers, Congress recently enacted

---

[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 records databases, and check verification services.

[25] *FTC v. Consumerinfo.com, Inc.*, SACV05-801AHS(MLGx) (C.D. Cal. Aug. 15, 2005); *FTC v. Consumerinfo.com, Inc.,* SACV05-801AHS(MLGx) (C.D. Cal. Jan. 8, 2007). In the original case in 2005, the Commission charged, among other things, that defendant Consumerinfo.com, an affiliate of the nationwide CRA Experian, had deceptively mimicked the FACT Act free report program. The stipulated order required the defendant to make prominent

legislation requiring entities that advertise "free" credit reports to disclose that such reports are available under federal law at annualcreditreport.com.[26] The FTC is promulgating a rule to implement this requirement. Third, the FACT Act empowered consumers to take steps to limit the damage from identity theft once they become victims. For example, consumers who have a good faith suspicion that they have been or are about to become victims of fraud or related crimes such as identity theft may place an initial, 90-day fraud alert on their credit files, alerting potential users of their reports to exercise special vigilance in opening accounts in the consumers' names. Actual victims may request an extended, seven-year alert if they provide a police report to the CRA.[27] In addition, victims may obtain from creditors the underlying documentation associated with transactions that may have been fraudulent,[28] block fraudulent information on their credit files,[29] and prohibit creditors from reporting fraudulent information to CRAs.[30]

Fourth, the FACT Act required businesses and organizations to detect and respond to "red flags," or signs of identity theft.[31] To implement this requirement, the Commission and

---

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 refunds to dissatisfied past customers. In the 2007 case, the Commission alleged that Consumerinfo.com had violated the 2005 order. The new order includes a $300,000 judgment for consumer redress.

[26] *See* Pub. L. 111-24; 15 U.S.C. § 1681j(g).

[27] 15 U.S.C. § 1681c-1.

[28] 15 U.S.C. § 1681g

[29] 15 U.S.C. § 1681c-2.

[30] 15 U.S.C. § 1861s-2(a)(6).

[31] 15 U.S.C. § 1681m(e).

other federal financial regulators promulgated the Red Flags Rule, which seeks to ensure that financial institutions and creditors are on the lookout for signs of identity theft or attempted identity theft.[32] The Red Flags Rule and accompanying guidelines require financial institutions and creditors that hold certain consumer accounts or other accounts for which there is a reasonable risk of identity theft, to develop and implement a written "Identity Theft Program" to help spot identity theft. In recent months, the FTC staff has undertaken substantial outreach efforts to educate financial institutions and creditors about the Rule. This outreach has included developing a compliance guide for businesses,[33] distributing general and industry-specific articles, speaking before numerous audiences, responding to individual inquiries by telephone and e-mail, and working with a number of trade associations that are developing model policies or specialized guidance for their members.[34]

Finally, the FACT Act included provisions to improve consumers' rights to dispute inaccuracies in their credit reports. Because businesses and other entities use consumer reports to grant credit, employment, insurance, and other benefits, it is critical that the information in the reports be as accurate as possible and that consumers have effective ways to dispute any inaccuracies. This is even more important for victims of identity theft, so that fraudulent information does not corrupt their credit reports. Previously, consumers could dispute

---

[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 Creditors and Financial Institutions to Adopt Identity Theft Prevention Programs (Apr. 30, 2009), http://ftc.gov/opa/2009/04/redflagsrule.shtm.

inaccuracies in their credit reports only with CRAs; the FACT Act granted consumers the right to file disputes directly with the furnisher of the disputed information.[35] The FTC and other financial regulators have completed drafting regulations to implement this provision.

In addition to implementing the specific identity theft protections of the FACT Act, the Commission is seeking to assess the effectiveness of these provisions by conducting a survey of identity theft victims that have filed complaints with the FTC.[36] The survey will provide information on victims' understanding of the remedies available to them under the FACT Act, as well as the effectiveness of these remedies. The results will help guide the FTC's efforts to enforce the law and educate consumers and the consumer reporting industry about their rights and duties.

III. Legislative Recommendations

The Commission has supported and continues to support additional legislation to improve its ability to fight identity theft. For example, the Commission has recommended that Congress enact federal legislation to establish data security standards across the private sector that would require all organizations that hold sensitive consumer data to take reasonable measures to safeguard it, and to notify consumers when the security of their information is breached.[37] In addition, the Commission has recommended that Congress provide it with

---

[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.

[37] *See* Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, United States Senate, 109th Cong. (Jun. 16, 2005), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf. Such legislation should be crafted carefully to avoid duplicate regulation of financial institutions and other entities covered by already-existing, comparable data security and breach notice obligations.

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.